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

Estimaciones y resultados de existencia de puntos racionales de variedades singulares sobre cuerpos finitos y aplicaciones

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Melina L. Privitelli

Director: Guillermo Matera
Consejero de estudios: Pablo Solernó

Buenos Aires, 15 de julio de 2014

Estimaciones y resultados de existencia de puntos racionales de variedades singulares sobre cuerpos finitos y aplicaciones

Resumen

El primer objetivo de esta tesis es proporcionar estimaciones y resultados de existencia de puntos racionales de intersecciones completas singulares definidas sobre el cuerpo finito $\mathbb{F}_q$. Nuestros resultados se basan en la obtención de nuevas versiones efectivas del segundo teorema de Bertini que garantizan la existencia de secciones lineales no singulares de una variedad singular, definidas sobre $\mathbb{F}_q$. Así, aplicando la conocida estimación de P. Deligne para variedades no singulares, obtenemos estimaciones y resultados de existencia para intersecciones completas cuyo lugar singular tiene codimensión al menos dos o tres. Dichas estimaciones se expresan en términos de la dimensión del lugar singular, el grado y la dimensión de la variedad. Además, proporcionamos una versión explícita de la estimación de Hooley para variedades singulares.

En la segunda parte de este trabajo aplicamos nuestras estimaciones a dos problemas concretos de teoría de códigos y combinatoria. En ambos casos las variedades involucradas son intersecciones completas simétricas, es decir, están definidas por polinomios invariantes bajo la acción del grupo de permutaciones de sus coordenadas. Es por esto que, en primer lugar, estudiamos las propiedades geométricas de dichas variedades, más concretamente la dimensión del lugar singular de las mismas. El problema de teoría de códigos que abordamos es el de determinar la existencia de *deep holes* en un código de Reed-Solomon estándar. En lo que respecta a problemas de combinatoria, analizamos el comportamiento del valor promedio del conjunto de valores (o "value set") de ciertas familias de polinomios definidas sobre $\mathbb{F}_q[T]$. En ambos casos, mejoramos los resultados existentes en la literatura.

Palabras clave. intersecciones completas singulares sobre cuerpos finitos, puntos racionales, segundo teorema de Bertini, variedades definidas por polinomios simétricos, código de Reed-Solomon estándar, *deep holes*, conjunto de valores promedio de polinomios univariados sobre cuerpos finitos.

Estimates and existence results for rational points of singular varieties over a finite field and applications

Abstract

The first aim of this thesis is to obtain estimates and existence results for rational points of singular complete intersections defined over a finite field $\mathbb{F}_q$. Our results rely on obtaining new effective versions of the second Bertini theorem. This theorem asserts that there exists a nonsingular linear section defined over $\mathbb{F}_q$ of a singular variety defined over $\mathbb{F}_q$. Thus, by applying the well known Deligne estimate, we provide estimates and existence results for rational points of singular complete intersections for which the singular locus has codimension at least two or three. Our estimates are expressed in terms of the dimension of the singular locus, the degree and the dimension of the variety. Furthermore, we obtain an explicit version of the Hooley estimate for singular complete intersections.

In the second part of this thesis we apply our estimates to concrete problems of coding theory and combinatorics. In both cases, the varieties under consideration are symmetric complete intersections, namely, they are defined by polynomials which are invariant under the action of the group of permutations of their coordinates. Hence, we first study some geometric properties of symmetric complete intersections; more precisely, we obtain information about the dimension of the singular locus of these varieties. Concerning coding theory, we study the existence of deep holes of the standard Reed-Solomon code. With respect to combinatorics, we analyze the average value set of families of univariate polynomials with coefficients in $\mathbb{F}_q$. In both cases, we improve the existing results in the literature.

Key words. singular complete intersections defined over a finite field, rational points, second Bertini's theorem, varieties defined by symmetric polynomials, standard Reed-Solomon code, deep holes, average value set of univariate polynomials.

Agradecimientos.

A Guillermo, por su compromiso, su dedicación, su paciencia, por acompañarme a lo largo de mi carrera, por todo lo que me enseñó y porque gracias a él pude llegar a este momento.

A Pablo, por aceptar ser mi consejero de estudios y por darme una mano siempre que la necesité.

A Teresa Krick, Daniel Panario y Juan Pablo Rossetti, por aceptar ser jurado de mi tesis y hacer el esfuerzo de acomodarse a mis tiempos y por la dedicación con la que leyeron este trabajo.

A mi amiga Mariana, por su infinita generosidad, por recorrer juntas parte de este camino y por acompañarme y ayudarme a seguir adelante en los momentos difíciles.

A dos amigas que conocí a lo largo de esta carrera. Euge, por estar siempre y porque la paso muy bien en nuestras salidas y largas charlas telefónicas. Isa, por su compañía, sus consejos y por saber que siempre puedo contar con ella.

A Xime, Isa y Mer, por los momentos compartidos en nuestras meriendas que hicieron más lindos estos años.

A mis compañeros del ICI: Ana, Ezequiel, Luciano y Martín, por los almuerzos, las charlas en la oficina y porque me encanta estar en el ICI trabajando con ellos.

A Nardo, por todos estos años compartidos.

A Eda, por sus consejos y por todo lo que aprendí trabajando con ella.

A Deby, por la buena onda de siempre y por ayudarme con los trámites para la presentación. A Martín, por ayudarme con algunas cosas del latex.

A mi mamá, mi tía Alicia y mis primos José y Patricia, por su ayuda incondicional, por el apoyo a lo largo de estos años y por alegrarse con mis logros.

A Nico, por su amor, por confiar en mi, por acompañarme en todo momento, por estos ocho años que fueron los mejores años de mi vida y por Agustín que es lo más lindo que nos pudo pasar.

Índice general

Capítulo 1

Introducción

El estudio del conjunto de soluciones racionales de sistemas de ecuaciones polinomiales sobre cuerpos finitos es un tema clásico, con importantes aplicaciones en áreas diversas de la matemática. En particular, cabe mencionar problemas concretos de teoría de códigos, criptografía y combinatoria, entre otras aplicaciones, donde éstos juegan un papel fundamental. Por ejemplo, en teoría de códigos, el estudio de las propiedades de polinomios sobre cuerpos finitos permite diseñar códigos detectores y correctores de errores, como los códigos de Reed-Solomon, Goppa, BCH y Reed-Muller (ver, por ejemplo, [HP03]). Por otro lado, en criptografía, las soluciones q-racionales, esto es, las soluciones cuyas coordenadas pertenecen al cuerpo finito $\mathbb{F}_q$, de ciertos sistemas de ecuaciones polinomiales son utilizadas a fin de codificar mensajes en los denominados "esquemas criptográficos multivariados"(ver, por ejemplo, [DGS06]). Asimismo, otros problemas centrales en criptografía, como el del logaritmo discreto, pueden ser expresados en términos de problemas vinculados al estudio de polinomios sobre cuerpos finitos. A su vez, los sistemas de ecuaciones polinomiales sobre cuerpos finitos aparecen naturalmente en muchas áreas de la combinatoria. Un problema clásico consiste en determinar el cardinal de clases de polinomios definidos sobre un cuerpo finito que poseen ciertas propiedades o características (ver, por ejemplo, [GHP99] o [vzGVZ13]). Por ejemplo, se trata de determinar la cantidad de polinomios de permutación, de polinomios irreducibles o más generalmente la cantidad de polinomios con cierto patrón de factorización, polinomios ralos, etc., en ciertas familias de polinomios (por ejemplo, el conjunto de polinomios univariados de grado dado cuyos coeficientes satisfacen ciertas condiciones).

Una estrategia para abordar estos problemas utiliza métodos típicos de la combinatoria analítica, es decir, se consideran funciones generatrices cuyos coeficientes expresan las propiedades en cuestión. Cuando no es posible calcular con exactitud dichos coeficientes se recurre al análisis asintótico para obtener una estimación de los mismos (ver, por ejemplo, [FS09]). Desafortunadamente cuando hay restricciones sobre el tipo de familias de polinomios en consideración (por ejemplo, restricciones sobre los coeficientes de los mismos) o sobre la característica del cuerpo finito en consideración, estos métodos no pueden ser aplicados. Es en este punto en el que cobra importancia la geometría, ya que a veces es posible reducir los problemas al de estimar o garantizar la existencia de puntos q-racionales de una cierta variedad

algebraica. Un ejemplo concreto de este fenómeno es el estudio del cardinal de la imagen (o "conjunto de valores") de familias de polinomios univariados sobre un cuerpo finito. Los resultados que se conocen cuando se considera el conjunto de polinomios univariados de grado dado en los cuales algunos coeficientes están prefijados son poco precisos y se basan en el estudio de ciertas sumas exponenciales.

En esta tesis vamos a obtener estimaciones que mejoran significativamente los resultados existentes sobre el cardinal del conjunto de valores de tales familias de polinomios por medio de un enfoque "geométrico", es decir, expresando las cantidades en consideración en términos de la cantidad de puntos q-racionales de ciertas variedades algebraicas que asociamos al problema. Estas variedades poseen características geométricas (por ejemplo, son intersecciones completas cuyo lugar singular tiene codimensión al menos 2 o 3) que tienen consecuencias importantes en lo que respecta al conjunto de puntos q-racionales de las mismas. De hecho, la primera mitad de esta tesis se dedica a obtener estimaciones sobre la cantidad de puntos q-racionales de tales variedades.

En resumen, vamos a considerar los siguientes problemas:

1. Obtener estimaciones y resultados de existencia sobre la cantidad de puntos q-racionales de una intersección completa singular (es decir cuyo lugar singular tiene dimensión mayor o igual a cero) definida sobre $\mathbb{F}_q$, en términos de invariantes geométricos tales como su dimensión, su grado, la dimensión del lugar singular, etc.

2. Aplicar las estimaciones y resultados de existencia obtenidos a dos problemas concretos:

   i) La existencia de *deep holes* en un código de Reed-Solomon estándar.

   ii) El comportamiento promedio del cardinal del conjunto de valores de ciertas familias de polinomios en $\mathbb{F}_q[T]$.

Salvo mención explícita en contrario, los resultados de esta tesis son originales y se encuentran en los siguientes artículos: [CMP12], [CMPP14] y [CMP14]. Los dos primeros ya están publicados, en tanto que el último ha sido sometido a publicación. Por otro lado, los resultados de las Secciones 3.4, 4.2.3 y 7.5 no se encuentran todavía publicados.

1.1. Antecedentes

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos, $\overline{\mathbb{F}}_q$ su clausura algebraica y sean $f_1, \ldots, f_m$ polinomios en $\mathbb{F}_q[X_1, \ldots, X_n]$. Consideremos el conjunto de soluciones en el espacio afín n-dimensional $\mathbb{A}^n := \mathbb{A}^n(\overline{\mathbb{F}}_q) := \overline{\mathbb{F}}_q^n$ sobre $\overline{\mathbb{F}}_q$ del sistema que estos polinomios definen, es decir,

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

Decimos entonces que V es una $\mathbb{F}_q$-variedad afín. Cuando $f_1, \ldots, f_m$ son polinomios homogéneos en $\mathbb{F}_q[X_0, \ldots, X_n]$ y se considera el conjunto de ceros comunes de ellos

en el espacio proyectivo n-dimensional $\mathbb{P}^n := \mathbb{P}^n(\overline{\mathbb{F}}_q)$ sobre $\overline{\mathbb{F}}_q$, entonces decimos que V es una $\mathbb{F}_q$-variedad proyectiva. El conjunto de puntos de V cuyas coordenadas pertenecen a $\mathbb{F}_q$, es decir, el conjunto de soluciones en $\mathbb{F}_q^n$ en el caso afín, o $\mathbb{P}^n(\mathbb{F}_q)$ en el caso proyectivo, de dicho sistema, se denomina el conjunto de puntos q-racionales de V.

Se conocen pocos resultados sobre la cantidad exacta de puntos q-racionales de $\mathbb{F}_q$-variedades. Básicamente los resultados existentes se refieren a variedades particulares, como por ejemplo variedades definidas por ecuaciones diagonales o ecuaciones cuadráticas. Por lo tanto, teniendo en cuenta estas limitaciones y, como mencionamos anteriormente, en vistas a las diversas aplicaciones de la cuestión, muchas veces es necesario disponer de estimaciones y resultados de existencia.

Los primeros en proporcionar una estimación de tipo general fueron A. Weil y S. Lang, quienes en [LW54] establecen un "prototipo" de estimación sobre el número de puntos q-racionales de una $\mathbb{F}_q$-variedad absolutamente irreducible. Ellos demuestran que, si $V \subset \mathbb{P}^n$ es una $\mathbb{F}_q$-variedad proyectiva absolutamente irreducible de dimensión r y grado δ, el número de puntos q-racionales $|V(\mathbb{F}_q)|$ satisface la siguiente estimación:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta-1)(\delta-2)q^{r-1/2} + C(n,r,\delta)q^{r-1},$$

donde $p_r := q^r + \cdots + q + 1$ y $C(n,r,\delta)$ es una constante que depende de n, r y δ, pero no de q. Cabe destacar que Lang y Weil no proporcionan ninguna expresión explícita sobre dicha constante, sólo se limitan a probar su existencia. Interpretando esta estimación en términos afines obtenemos que, si $V \subset \mathbb{A}^n$ es una $\mathbb{F}_q$-variedad absolutamente irreducible de dimensión r y grado δ, el número de puntos q-racionales $|V(\mathbb{F}_q)|$ satisface la siguiente estimación:

$$\big||V(\mathbb{F}_q)| - q^r\big| \leq (\delta-1)(\delta-2)q^{r-1/2} + C(n,r,\delta)q^{r-1}.$$

Hacia comienzos de los años 70 no se disponían de versiones explícitas o cotas superiores para la constante $C(n,r,\delta)$. En 1974, W. Schmidt [Sch74] proporciona una cota inferior no trivial y, por lo tanto, un resultado de existencia sobre el número de puntos q-racionales $|H(\mathbb{F}_q)|$ de una hipersuperficie absolutamente irreducible de grado δ:

$$|H(\mathbb{F}_q)| \geq q^{n-1} - (\delta-1)(\delta-2)q^{n-3/2} - (5\delta^2+\delta+1)q^{n-2},$$

bajo la condición $q > 10^4 n^3 \delta^5 P^3([4\log\delta])$, donde $P(u)$ es el u-ésimo número primo. Posteriormente, Schmidt es el primero en dar la siguiente estimación explícita para una $\mathbb{F}_q$-hipersuperficie absolutamente irreducible (ver [Sch76]):

$$\big||H(\mathbb{F}_q)| - q^{n-1}\big| \leq (\delta-1)(\delta-2)q^{n-3/2} + 6\delta^2\theta^{2^\theta}q^{n-2}, \tag{1.1}$$

donde $\theta := (\delta+1)\,\delta/2$.

En 2002, S. Ghorpade y G. Lachaud [GL02a, GL02b], utilizando herramientas de cohomología, encuentran una versión explícita para la constante $C(n,r,\delta)$. Más precisamente, obtienen la siguiente estimación:

$$\big||V(\mathbb{F}_q)| - q^r\big| \leq (\delta-1)(\delta-2)q^{r-1/2} + 6\cdot 2^s(sd+3)^{n+1}q^{r-1},$$

donde s es el número de ecuaciones que definen a V y d es el grado máximo de las mismas. Por otro lado, A. Cafure y G. Matera obtienen en [CM06] nuevas estimaciones para la constante $C(n, r, \delta)$ que mejoran la estimación de Ghorpade y Lachaud en algunos casos de interés. Más precisamente, utilizando herramientas de eliminación efectiva los autores prueban que, si $V \subset \mathbb{A}^n$ es una $\mathbb{F}_q$-variedad absolutamente irreducible de dimensión $r > 0$ y grado δ, y se satisface la condición $q > 2(r+1)\delta^2$, entonces

$$\big||V(\mathbb{F}_q)| - q^r\big| \leq (\delta - 1)(\delta - 2)q^{r-1/2} + 5\,\delta^{13/3}q^{r-1}. \tag{1.2}$$

Además, los autores proporcionan resultados de existencia de puntos q-racionales de $\mathbb{F}_q$-hipersuperficies que mejoran significativamente el mejor resultado existente al respecto, que se deduce de (1.1). Cabe destacar que este resultado es casi óptimo, en un sentido que vamos a explicar en el Capítulo 2.

Teniendo en cuenta la casi optimalidad de los resultados de existencia mencionados, una posible alternativa es la de obtener resultados de existencia y estimaciones para variedades que poseen ciertas características geométricas, tales como la no singularidad, normalidad o el hecho de ser intersección completa, entre otras. Un resultado conocido en este sentido es la estimación de P. Deligne para intersecciones completas proyectivas no singulares definidas sobre $\mathbb{F}_q$ (ver [Del74]). En efecto, sea $V \subset \mathbb{P}^n$ una intersección completa no singular definida sobre $\mathbb{F}_q$, de dimensión r y multigrado $\boldsymbol{d} = (d_1, \ldots, d_{n-r})$, donde $d_1 \geq \cdots \geq d_{n-r}$ representan los grados de cualquier sistema de polinomios homogéneos que generan el ideal de V. Entonces se satisface la siguiente estimación:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_r(n, \boldsymbol{d})q^{r/2}, \tag{1.3}$$

donde $b'_r(n, \boldsymbol{d})$ es el r-ésimo número de Betti primitivo de V.

Posteriormente, en 1991, C. Hooley [Hoo91] extiende la estimación de Deligne a intersecciones completas arbitrarias. Si $V \subset \mathbb{P}^n$ es una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r y multigrado $\boldsymbol{d}$, cuyo lugar singular tiene dimensión singular $s \geq 0$, entonces la cantidad de puntos q-racionales de V verifica:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq C(r, s, \boldsymbol{d})q^{(r+s+1)/2}. \tag{1.4}$$

Hooley no provee una expresión explícita de la constante involucrada en esta estimación, sólo establece su independencia respecto de q.

Ghorpade y Lachaud, utilizando las herramientas de cohomología ya mencionadas, dan la siguiente expresión explícita de la constante $C(r, s, \boldsymbol{d})$ (ver [GL02a, GL02b]). Si $V \subset \mathbb{P}^n$ es una intersección completa definida sobre $\mathbb{F}_q$ de dimensión r y multigrado $\boldsymbol{d}$, cuyo lugar singular tiene dimensión a lo sumo $0 \leq s \leq r-2$, entonces

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_{r-s-1}(n - s - 1, \boldsymbol{d})q^{(r+s+1)/2} + C_s(V)q^{(r+s)/2}, \tag{1.5}$$

donde $C_s(V)$ es una constante independiente de q que se puede acotar por

$$C_s(V) \leq 9\,.\,2^{n-r}((n-r)d + 3)^{n+1},$$

siendo $d := \text{máx}\{d_1, \ldots, d_{n-r}\}$ si $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$.

Para completar el panorama de las estimaciones sobre intersecciones completas singulares, cabe mencionar que, en 2007, Cafure y Matera proporcionan una estimación y mejores resultados de existencia para una intersección completa proyectiva normal definida sobre $\mathbb{F}_q$, basándose en una versión efectiva del segundo teorema de Bertini para variedades normales (ver [CM07a]). Más precisamente, en dicho trabajo se demuestra que, si $V \subset \mathbb{P}^n$ es una intersección completa normal de dimensión r y multigrado $\boldsymbol{d}$, definida sobre $\mathbb{F}_q$, y q satisface la condición $q > 2(n-r)d\delta + 1$, entonces

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b_1'(n-r+1, \boldsymbol{d})q^{r-1/2} + 2\big((n-r)d\delta\big)^2 q^{r-1}. \tag{1.6}$$

1.2. Resultados obtenidos y organización del trabajo

El Capítulo 2 está dedicado a introducir los preliminares geométricos y fijar notaciones. También hacemos una revisión de los resultados clásicos sobre cotas superiores y resultados de existencia de puntos q-racionales. Dado que muchas condiciones genéricas con las que tratamos en el Capítulo 3 se expresan en términos de hipersuperficies multiproyectivas, dedicamos la última sección a recopilar las definiciones básicas y propiedades del espacio multiproyectivo $\mathbb{P}^{\boldsymbol{n}} := \mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_m}$. Asimismo, obtenemos una nueva cota superior para la cantidad de puntos q-racionales de hipersuperficies multiproyectivas (Proposición 2.3.12), que enunciamos a continuación.

Teorema 1.2.1. *Sea $F \in \overline{\mathbb{F}}_q[\boldsymbol{X}_1, \ldots, \boldsymbol{X}_m]$ un polinomio multihomogéneo (es decir, homogéneo en cada grupo de variables $\boldsymbol{X}_i$) de multigrado $\boldsymbol{d} := (d_1, \ldots, d_m)$ con $\max_{1\leq i\leq m} d_i < q$ y sea N la cantidad de ceros q-racionales de F en $\mathbb{P}^{\boldsymbol{n}}$. Entonces*

$$N \leq \eta_m(\boldsymbol{d}, \boldsymbol{n}) := \sum_{\boldsymbol{\varepsilon}\in\{0,1\}^m\setminus\{\boldsymbol{0}\}} (-1)^{|\boldsymbol{\varepsilon}|+1} \boldsymbol{d}^{\boldsymbol{\varepsilon}} p_{\boldsymbol{n}-\boldsymbol{\varepsilon}},$$

donde $p_{\boldsymbol{n}}$ denota la cantidad de puntos q racionales del espacio multiproyectivo $\mathbb{P}^{\boldsymbol{n}}$.

Con el objetivo de obtener nuevas estimaciones y resultados de existencia, en el Capítulo 3 obtenemos una versión efectiva del segundo teorema de Bertini. El segundo teorema de Bertini establece que, si $V \subset \mathbb{P}^n$ es una intersección completa de dimensión r, multigrado $\boldsymbol{d}$ y lugar singular de dimensión s, entonces existe una sección lineal genérica de V de dimensión $r-s-1$ que es no singular. Una versión efectiva de este resultado proporciona una constante $C(n, r, s, \boldsymbol{d})$ tal que, si $q > C(n, r, s, \boldsymbol{d})$ y V está definida sobre $\mathbb{F}_q$, entonces existe una sección lineal no singular de V de dimensión $r-s-1$ definida sobre $\mathbb{F}_q$.

Para esto seguimos el enfoque de [CM07a], donde dichas secciones lineales se obtienen como la clausura Zariski de las fibras de una proyección genérica $\pi : V \to \mathbb{P}^{s+1}$. En esta tesis mejoramos y generalizamos el resultado de [CM07a], estudiando el conjunto S de puntos excepcionales de dicha proyección. Esto lo hacemos, mediante un enfoque novedoso, identificando a S con una cierta variedad polar. Las variedades

polares constituyen un concepto clásico de la geometría proyectiva introducido por F. Severi y J. Todd en los años 30 y fuertemente impulsado por los trabajos de R. Piene [Pie78] y B. Teissier [Tei82] en los años 70. Nuestro resultado principal en relación con las variedades polares establece condiciones sobre π bajo las cuales la correspondiente variedad polar tiene la dimensión esperada (Teorema 3.1.6). A partir de este resultado obtenemos la siguiente versión efectiva del segundo teorema de Bertini (ver Teorema 3.3.4 y Corolario 3.3.6).

Teorema 1.2.2. *Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$ de dimensión r, grado δ, multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ y lugar singular de dimensión a lo sumo $s \geq 0$. Sea $D := \sum_{i=1}^{n-r}(d_i - 1)$. Si $q > (n+1)^2 D^{r-s-1}\delta$, entonces existe una sección lineal de V no singular de dimensión $r-s-1$ definida sobre $\mathbb{F}_q$.*

Cabe destacar que esta versión del segundo teorema de Bertini mejora exponencialmente la versión dada en [Bal03] para hipersuperficies.

En el Capítulo 4 proporcionamos resultados de existencia de puntos q-racionales regulares de intersecciones completas singulares. Un problema clásico es determinar condiciones sobre q de forma tal que una cierta variedad tenga al menos un punto q-racional. Sin embargo, en muchas aplicaciones resulta necesario probar la existencia de un punto q-racional regular (ver, por ejemplo, [Woo08] y [Zah10]). En esta tesis obtenemos resultados de este tipo como consecuencia de nuestra versión efectiva del segundo teorema de Bertini. Más precisamente, si V es una $\mathbb{F}_q$-variedad proyectiva de dimensión r y lugar singular de dimensión a lo sumo s, establecemos una condición sobre q que implica que existe una sección no singular S de dimensión $r-s-1$ de V definida sobre $\mathbb{F}_q$. El resultado se sigue de aplicar la estimación de Deligne (1.3) a dicha sección y de observar que S está contenida en el conjunto de puntos regulares de V. Más precisamente, obtenemos el siguiente teorema (ver Corolarios 4.1.3 y 4.1.4).

Teorema 1.2.3. *Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r, grado δ, multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ y lugar singular de dimensión a lo sumo $s \geq 0$. Sea $D := \sum_{i=1}^{n-r}(d_i - 1)$. Si $s = r-2$ y $q > 2(D+2)^2\delta^2$, o $s = r-3$ y $q > 3D(D+2)^2\delta$, entonces V tiene al menos un punto q-racional regular.*

Por otro lado, en ese capítulo obtenemos estimaciones sobre la cantidad de puntos q-racionales regulares de intersecciones completas para las cuales el lugar singular tiene dimensión $r-2$ o $r-3$. Para ello consideramos el morfismo lineal genérico $\pi : V \to \mathbb{P}^{s+1}$ que mencionamos anteriormente y expresamos a V como una unión finita de secciones lineales de V de dimensión $r-s-1$. Recordemos que cada una de estas secciones se obtiene como la clausura Zariski de una fibra de π definida sobre $\mathbb{F}_q$. Observamos que los puntos q-racionales de V que pertenecen a fibras singulares no hacen un aporte significativo a la estimación. Por lo tanto, aplicando (1.3) a aquellas fibras que resultan no singulares podemos estimar satisfactoriamente la cantidad de puntos q-racionales de V. En resumen, tenemos el siguiente teorema (ver Corolarios 4.2.3 y 4.2.4).

Teorema 1.2.4. *Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r, grado δ, multigrado $\boldsymbol{d}$ y lugar singular de dimensión $s \in \{r-3, r-2\}$. Sea V_{sm} el conjunto de puntos regulares de V. Sea $D := \sum_{i=1}^{n-r}(d_i - 1)$. Entonces, para $s \leq r-2$, se tiene:*

$$\begin{aligned} \big||V(\mathbb{F}_q)| - p_r\big| &\leq (\delta(D-2)+2)q^{r-1/2} + 14D^2\delta^2 q^{r-1}, \\ \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| &\leq (\delta(D-2)+2)q^{r-1/2} + 8(r+1)D^2\delta^2 q^{r-1}. \end{aligned}$$

Por otro lado, si $s \leq r-3$,

$$\begin{aligned} \big||V(\mathbb{F}_q)| - p_r\big| &\leq 14D^3\delta^2 q^{r-1}, \\ \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| &\leq (34r-20)D^3\delta^2 q^{r-1}. \end{aligned}$$

Este teorema mejora la estimación (1.5) en los casos $s = r-2$ y $s = r-3$ para variedades de dimensión grande ($r > (n-1)/2$) o grado pequeño ($\delta \leq (2(n-r))^{n-r}$). Por otro lado, (1.5) puede resultar conveniente en el caso en que la variedad sea de dimensión baja y grado alto. En tal sentido, podemos decir que nuestro resultado complementa la estimación (1.5). En el Capítulo 7 nos encontramos con el problema de estimar la cantidad de puntos q-racionales de una intersección completa de grado bajo cuyo lugar singular tiene codimensión al menos 3. Este es un ejemplo concreto en el cual, de nuestra estimación para el caso $s = r-3$, se desprenden mejores resultados que si aplicáramos (1.5). Por último, mejoramos (1.6) para variedades normales ya que no imponemos condiciones sobre q, mientras que allí se pide $q > 2(n-r)d\delta + 1$.

Finalmente, obtenemos la siguiente versión explícita de la estimación de Hooley (1.4), que vale bajo una cierta condición sobre q (Teorema 4.2.8). Cuando se satisface esta condición, nuestra estimación mejora exponencialmente la mejor estimación explícita que se conoce, debida a Ghorpade y Lachaud (ver [GL02a, Theorem 6.1]).

Teorema 1.2.5. *Sea $q > 2(s+1)\delta D^{r-s-1}(D+r-s+1)$ y $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r, grado δ, multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ y lugar singular de dimensión a lo sumo $s \geq 0$. Tenemos entonces la siguiente estimación:*

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \left(b'_{r-s-1}(n-s-1, \boldsymbol{d}) + 2\sqrt{\delta} + 1\right) q^{\frac{r+s+1}{2}}.$$

Ciertas cuestiones de teoría de códigos, criptografía y combinatoria requieren estudiar $\mathbb{F}_q$-variedades en las que actúa un grupo finito de invariantes. Este es el caso de la existencia de "deep holes" en códigos de Reed-Solomon estándar [CM07b], el reconocimiento de funciones de tipo "almost perfect nonlinear" en el ámbito del cripto-análisis diferencial [Nyb94] y, como es presentado de manera original en esta tesis, el estudio del conjunto de valores de polinomios sobre cuerpos finitos (Capítulo 7). En todos estos casos, se trata de estimar el cardinal del conjunto de puntos q-racionales de una intersección completa singular "simétrica", es decir, una intersección completa cuyo conjunto de soluciones resulta invariante bajo la acción del grupo simétrico de sus coordenadas. En el Capítulo 5 estudiamos las propiedades geométricas de intersecciones completas simétricas. El resultado principal de dicho

capítulo establece una cota superior no trivial para la dimensión del lugar singular de las mismas. Finalmente, en los últimos dos capítulos aplicamos nuestras estimaciones y resultados geométricos sobre intersecciones completas simétricas a un problema de teoría de códigos y otro de combinatoria.

En el Capítulo 6 consideramos el primero de ellos, es decir, un problema concreto de la teoría de códigos de Reed-Solomon. Los códigos de Reed-Solomon fueron introducidos en los años 60 y son comúnmente utilizados en diversas cuestiones de índole tecnológico. Su excelente capacidad de detectar y corregir errores, sumada a la existencia de buenos algoritmos de decodificación, los convierten en un tipo de códigos muy usado en la práctica.

Dado un conjunto de evaluación $\mathsf{D} := \{x_1, \ldots, x_n\} \subset \mathbb{F}_q$ y un entero positivo $k \leq n$, el código de Reed-Solomon de longitud n y dimensión k sobre $\mathbb{F}_q$ es el siguiente subespacio de $\mathbb{F}_q^n$:

$$C(\mathsf{D}, k) := \{(f(x_1), \ldots, f(x_n)) : f \in \mathbb{F}_q[T], \deg(f) \leq k-1\}.$$

Los elementos de $C(\mathsf{D}, k)$ se llaman palabras del código. Cuando $\mathsf{D} = \mathbb{F}_q^*$, decimos que $C(\mathsf{D}, k)$ es el código de Reed-Solomon estándar. La distancia de Hamming entre dos vectores de $\mathbb{F}_q^n$ es la cantidad de coordenadas en las que ellos difieren y el radio de recubrimiento del código es la máxima distancia posible de un elemento cualquiera de $\mathbb{F}_q^n$ al código. Un deep hole es un elemento de $\mathbb{F}_q^n$ en donde se alcanza esta distancia. En tal sentido, podemos decir que los deep holes son las palabras más difíciles de decodificar, dado que son aquellas en cuya transmisión se han cometido la mayor cantidad de errores.

Si bien los deep holes han sido caracterizados en varios tipos de códigos, dicha caracterización no es conocida (ni trivial) en el caso de los códigos de Reed-Solomon. En 2007, Q. Cheng y E. Murray abordaron este problema desde un punto de vista geométrico, reduciendo el problema de determinar si una palabra recibida es un deep hole al de decidir cuando una $\mathbb{F}_q$-hipersuperficie absolutamente irreducible posee un punto q-racional con coordenadas distintas y no nulas. Para ello aplicaron la estimación (1.2) a fin de obtener condiciones que garantizan la inexistencia de deep holes en códigos de Reed-Solomon estándar. Más precisamente, si asociamos a una palabra recibida $\mathbf{w} := (w_1, \ldots, w_n) \in \mathbb{F}_q^n$ el único polinomio $f_{\mathbf{w}} \in \mathbb{F}_q[T]$ de grado a lo sumo $n-1$ tal que $f_w(x_i) = w_i$ para $1 \leq i \leq n$ (en cuyo caso decimos que la palabra $\mathbf{w}$ está generada por el polinomio $f_{\mathbf{w}}$), Cheng y Murray obtienen el siguiente resultado.

Teorema 1.2.6 ([CM07b, Theorem 1]). *Sean k, d enteros positivos, q un número primo y ϵ una constante positiva. Si $q > \max\{k^{4+\epsilon}, d^{13/3+\epsilon}\}$ entonces una palabra $\mathbf{w}_f$ generada por un polinomio $f \in \mathbb{F}_q[T]$ de grado $k+d < q-1$ no es un deep hole del código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$.*

Más aún, en dicho trabajo los autores conjeturan que los únicos deep holes son los generados por polinomios de grado k, lo que permitiría clasificarlos completamente. En 2008, Y. Li y D. Wan [LW08b] mejoran el resultado de Cheng y Murray utilizando la cota de Weil para ciertas sumas exponenciales. Más precisamente, los autores obtienen la siguiente caracterización.

Teorema 1.2.7 ([LW08b, Theorem 1.4]). *Sean k, d enteros positivos, q es una potencia de un primo y ϵ una constante positiva. Si $q > \max\{d^{2+\epsilon}, (k+1)^2\}$ y se verifica que $k > (\frac{2}{\epsilon}+1)d+\frac{8}{\epsilon}+2$, entonces una palabra $\mathbf{w}_f$ generada por un polinomio $f \in \mathbb{F}_q[T]$ de grado $k+d < q-1$ no es un deep hole en el código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$.*

Utilizando nuestros resultados sobre intersecciones completas simétricas y la estimación (1.5) mejoramos la caracterización de los deep holes dada por Li y Wan. En efecto, obtenemos el siguiente resultado (Teorema 6.5.1).

Teorema 1.2.8. *Sean k y d enteros con $k > d \geq 3$ y ϵ una constante positiva. Sea $\mathbf{w}_f$ la palabra generada por un polinomio $f \in \mathbb{F}_q[T]$ de grado $k+d < q-1$. Si $q > \max\{(k+1)^2, 14\,d^{2+\epsilon}\}$ y $\quad k \geq d\Big(\frac{2}{\epsilon}+1\Big)$, entonces $\mathbf{w}_f$ no es un deep hole del código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$.*

Cabe mencionar que la conjetura de Cheng y Murray fue resuelta por la negativa en el año 2012 (ver [WH12]). Sin embargo, continúa pendiente la cuestión de determinar cuáles polinomios generan deep holes, cuestión para la cual el Teorema 1.2.8 constituye un avance.

En el Capítulo 7 estudiamos el "conjunto de valores" (value set) de polinomios definidos sobre un cuerpo finito. Dado un polinomio $f \in \mathbb{F}_q[T]$, se define el conjunto de valores de f sobre $\mathbb{F}_q$ como el conjunto imagen de la función polinomial de $\mathbb{F}_q$ en $\mathbb{F}_q$ que define f. Denotamos por $\mathcal{V}(f)$ al cardinal de dicho conjunto. Birch y Swinnerton–Dyer [BSD59] demostraron que, si f es un polinomio de grado $d \geq 1$, entonces

$$\mathcal{V}(f) = \mu_d\, q + \mathcal{O}(q^{1/2}),$$

donde $\mu_d := \sum_{r=1}^{d} (-1)^{r-1}/r!$ y la constante que subyace a la notación $\mathcal{O}$ depende sólo de d.

En los años 50, L. Carlitz y S. Uchiyama, utilizando técnicas de análisis combinatorio, estudiaron el comportamiento del valor promedio $\mathcal{V}(d,0)$ de $\mathcal{V}(f)$ cuando f recorre los polinomios mónicos en $\mathbb{F}_q[T]$, de grado fijo y que verifican que $f(0) = 0$ (ver [CU57], [Car55], [Uch55a] y [Uch56]). Sus resultados fueron mejorados por S. Cohen ([Coh73, §2]), quien demuestra el siguiente resultado:

$$\mathcal{V}(d,0) = \sum_{r=1}^{d} (-1)^{r-1} \binom{q}{r} q^{1-r} = \mu_d\, q + \mathcal{O}(1).$$

Una variante de este problema fue considerada por Uchiyama [Uch55b] y Cohen [Coh72, Coh73], los cuales, estudiando ciertas sumas exponenciales, determinan el comportamiento promedio de $\mathcal{V}(f)$ en el caso especial en el que algunos coeficientes se encuentran fijos. En este caso, los resultados que obtienen son menos precisos. En concreto, si s es un entero con $1 \leq s \leq d-2$ y $\boldsymbol{a} := (a_{d-1}, \ldots, a_{d-s}) \in \mathbb{F}_q^s$, definimos para cada $\boldsymbol{b} := (b_{d-s-1}, \ldots, b_1)$ el polinomio

$$f_{\boldsymbol{b}} := f_{\boldsymbol{b}}^{\boldsymbol{a}} := T^d + \sum_{i=1}^{s} a_{d-i} T^{d-i} + \sum_{i=s+1}^{d-1} b_{d-i} T^{d-i}.$$

Si $p := \mathrm{char}(\mathbb{F}_q) > d$, entonces, por ejemplo, Cohen demuestra que

$$\mathcal{V}(d,s,\boldsymbol{a}) := \frac{1}{q^{d-s-1}} \sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}}) = \mu_d\, q + \mathcal{O}(q^{1/2}), \tag{1.7}$$

donde la constante que subyace a la notación $\mathcal{O}$ depende sólo de d y s. Cabe mencionar que ni Cohen ni Uchiyama dan una expresión explícita del término de error en sus estimaciones.

En esta tesis mejoramos significativamente estos resultados. Para ello, expresamos a $\mathcal{V}(d,s,\boldsymbol{a})$ en términos del número $\chi_r^{\boldsymbol{a}}$ de ciertos "conjuntos interpolantes" para $d-s-1 \le r \le d$ (ver Teorema 7.2.1). Más precisamente, definimos $\chi_r^{\boldsymbol{a}}$ como el número de subconjuntos de r elementos de $\mathbb{F}_q$ para los cuales $f_{\boldsymbol{a}}$ puede ser interpolado por un polinomio de grado a lo sumo $d-s-1$. Se tiene que el número $\chi_r^{\boldsymbol{a}}$ está relacionado con la cantidad de puntos q-racionales de una cierta variedad $V_r^{\boldsymbol{a}}$. Dicha variedad resulta ser una intersección completa simétrica (ver Proposición 7.2.4), con lo cual podemos aplicar los resultados geométricos del Capítulo 5. Finalmente, combinando esto con la estimación (4.17) para intersecciones completas cuyo lugar singular tiene codimensión al menos 3, obtenemos el siguiente teorema (ver Teorema 7.4.4).

Teorema 1.2.9. *Sean $\boldsymbol{a} \in \mathbb{F}_q^s$, d, r y s enteros positivos con $d < q$ y $2(s+1) \le d$. Para $d-s+1 \le r \le d$, se verifica que*

$$\left|\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d\, q - \frac{1}{2e}\right| \le \frac{(d-2)^5 e^{2\sqrt{d}}}{2^{d-2}} + \frac{7}{q}.$$

Si bien nuestra estimación vale para $s \le d/2-1$, mientras que (1.7) es válido para $s \le d-2$, mejoramos (1.7) en diversos aspectos. En primer lugar, no imponemos condiciones sobre la característica p de $\mathbb{F}_q$, en tanto que en (1.7) se pide que $p > d$. Por otro lado, en (1.7) se prueba que $\mathcal{V}(d,s,\boldsymbol{a}) = \mu_d\, q + \mathcal{O}(q^{1/2})$, mientras que nosotros demostramos que $\mathcal{V}(d,s,\boldsymbol{a}) = \mu_d\, q + \mathcal{O}(1)$. Por último, obtenemos una expresión explícita de la constante que subyace a la notación $\mathcal{O}$, de forma tal que el término de error tiende a cero cuando d tiende a infinito.

Capítulo 2

Preliminares

En este capítulo damos las definiciones, notaciones y resultados básicos de geometría algebraica que utilizaremos a lo largo de esta tesis. Además, enunciaremos algunos resultados clásicos sobre la cantidad de puntos q-racionales de $\mathbb{F}_q$-variedades. En la exposición seguimos principalmente los textos [Eis95], [Kun85] y [Sha94].

2.1. Definiciones y resultados básicos de geometría algebraica

Sea K un cuerpo. Denotamos por $\mathbb{A}^n_K$ al espacio afín de dimensión n definido sobre K, y por $\mathbb{P}^n_K$ al espacio proyectivo de dimensión n definido sobre K. Ambos son espacios topológicos con la topología de Zariski sobre K, según la cual los cerrados son los conjuntos de ceros comunes de polinomios en $K[X_1, \ldots, X_n]$, o de polinomios homogéneos en $K[X_0, \ldots, X_n]$ en el caso proyectivo. En esta sección, vamos a notar como $\mathbb{A}^n$ y $\mathbb{P}^n$ al espacio afín y proyectivo respectivamente definidos sobre $\overline{K}$, la clausura algebraica de K.

Los conjuntos abiertos en la topología de Zariski de $\mathbb{A}^n$ o $\mathbb{P}^n$ son densos. En tal sentido, decimos que una propiedad sobre los elementos de $\mathbb{A}^n$ o $\mathbb{P}^n$ es genérica si la satisfacen todos los puntos que pertenecen a un abierto Zariski de $\mathbb{A}^n$ o $\mathbb{P}^n$.

Definición 2.1.1. *Sea K un cuerpo.*

i) Un subconjunto $V \subset \mathbb{A}^n$ es una K-variedad afín si es el conjunto de ceros comunes en $\mathbb{A}^n$ de una familia de polinomios $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. En particular, una K-hipersuperficie afín es el conjunto de ceros en $\mathbb{A}^n$ de un único polinomio $f \in K[X_1, \ldots, X_n]$ no nulo.

ii) Un subconjunto $V \subset \mathbb{P}^n$ es una K-variedad proyectiva si es el conjunto de ceros comunes en $\mathbb{P}^n$ de una familia de polinomios homogéneos $f_1, \ldots, f_m \in K[X_0, \ldots, X_n]$. En particular, una K-hipersuperficie proyectiva es el conjunto de ceros en $\mathbb{P}^n$ de un único polinomio homogéneo $f \in K[X_0, \ldots, X_n]$ no nulo.

Notemos que una K-variedad afín (resp. proyectiva) resulta un espacio topológico con la topología inducida de $\mathbb{A}^n$ (resp. de $\mathbb{P}^n$). Vamos a denotar por $V(f_1, \ldots, f_m)$

o $\{f_1 = \cdots = f_m = 0\}$ a la K-variedad afín o proyectiva dada por el conjunto de ceros comunes de los polinomios $f_1, \ldots, f_m$.

Sea V una K-variedad en $\mathbb{A}^n$ o $\mathbb{P}^n$. Denotamos por $I(V)$ al ideal de la variedad, es decir el conjunto de polinomios en $K[X_1, \ldots, X_n]$ o en $K[X_0, \ldots, X_n]$ que se anulan en todos los puntos de V. Se tiene que $I(V)$ es un ideal radical. Notamos por $K[V]$ al anillo coordenado de V, o sea $K[V]$ es el anillo cociente $K[X_1, \ldots, X_n]/I(V)$ o $K[X_0, \ldots, X_n]/I(V)$.

A continuación damos una serie de definiciones que son válidas tanto para K-variedades afines como para K-variedades proyectivas, por lo que vamos a denominarlas simplemente K-variedades.

Definición 2.1.2. *Sean K un cuerpo, $\overline{K}$ su clausura algebraica y V una K-variedad. Entonces,*

(i) V se dice irreducible *si no puede escribirse como unión de K-variedades propias.*

(ii) V se dice absolutamente irreducible *si es irreducible como $\overline{K}$-variedad.*

Toda K-variedad V se puede descomponer como unión finita de K-variedades irreducibles, llamadas las componentes K-irreducibles de V. En particular, las componentes $\overline{K}$-irreducibles se denominan las componentes absolutamente irreducibles de V. Dada una K-variedad V, definimos la dimensión r de V como la longitud de la mayor cadena de K-variedades irreducibles $V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_r \subset V$ contenida en V. Decimos que una K-variedad es equidimensional si todas sus componentes K-irreducibles tienen la misma dimensión.

Sean V y W K-variedades afines. Una función $f : V \to W$ es un morfismo regular si existen polinomios $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ tales que para todo $x \in V$, $f(x) = (f_1(x), \ldots, f_m(x))$. Decimos que f es un morfismo dominante si $\overline{f(V)} = W$, donde $\overline{f(V)}$ es la clausura de $f(V)$ con respecto a la topología Zariski de W. En esta situación, f induce, por composición, una extensión de anillos $K[W] \hookrightarrow K[V]$, y decimos que este morfismo es finito si dicha extensión es entera. En el caso en que V y W sean K-variedades proyectivas, un morfismo $f : V \to W$ se dice regular si para cada $x \in V$ existen entornos afines $U \subset V$ de x y $U' \subset W$ de $f(x)$ tales que $f : U \to U'$ es regular. Por otro lado, la definición de morfismo dominante coincide con la dada en el caso afín y $f : V \to W$ se dice finito si para todo $y \in W$ existe un abierto afín W_y tal que $U := f^{-1}(W_y)$ es afín y $f : U \to W_y$ es un morfismo finito de variedades afines. Una propiedad importante de los morfismos finitos es la siguiente. Si $S \subset W$ es una subvariedad irreducible entonces la preimagen $f^{-1}(S)$ es una variedad equidimensional de dimensión $\dim S$ (ver, por ejemplo, [Dan94, §4.2, Proposition]).

A cada K-variedad afín $V \subset \mathbb{A}^n$ podemos asociarle una K-variedad proyectiva $\mathrm{pcl}(V) \subset \mathbb{P}^r$, que llamamos la clausura proyectiva de V y definimos de la siguiente manera. Consideramos la inmersión de $\mathbb{A}^n$ en $\mathbb{P}^n$ que a cada $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$ le asigna el punto $(1 : x_1, \cdots : x_n) \in \mathbb{P}^n$. La clausura proyectiva $\mathrm{pcl}(V)$ es entonces la clausura de la imagen de V vía esta inmersión, considerando la topología Zarisky en $\mathbb{P}^n$. Así, por definición, $\mathrm{pcl}(V)$ es la menor K-variedad proyectiva que contiene

a V. Los puntos de $\mathrm{pcl}(V) \setminus V$ se llaman puntos de V *en el infinito*. Se cumplen además las siguientes propiedades:

(*i*) V es irreducible si y sólo si $\mathrm{pcl}(V)$ lo es.

(*ii*) Si $V = V_1 \cup V_2 \cup \cdots \cup V_r$ es la descomposición de V en K-variedades irreducibles entonces $\mathrm{pcl}(V) = \mathrm{pcl}(V_1) \cup \mathrm{pcl}(V_2) \cup \cdots \cup \mathrm{pcl}(V_r)$ es la descomposición de $\mathrm{pcl}(V)$ en componentes K-irreducibles.

(*iii*) V y $\mathrm{pcl}(V)$ tienen la misma dimensión.

(*iv*) El ideal $I(V)^h$ de $\mathrm{pcl}(V)$ es el ideal generado por la homogeneización $f^h \in K[X_0, \ldots, X_n]$ de todos los polinomios $f \in I(V) \subset K[X_1, \ldots, X_n]$. Además, $I(V)^h$ es radical si y sólo si $I(V)$ lo es.

Sea $V \subset \mathbb{A}^n$ una K-variedad afín, sea $I(V) \subset K[X_1, \ldots, X_n]$ el ideal de V y $x \in V$. La dimensión $\dim_x V$ de V en x es el máximo de la dimensión de las componentes K-irreducibles de V que contienen a x. Si $I(V) = (f_1, \ldots, f_r)$, entonces el espacio tangente $\mathcal{T}_x V$ de V en x se define como el núcleo de la matriz Jacobiana $(\partial f_i/\partial X_j)_{1 \le i \le r, 1 \le j \le n}(x)$ de $f_1, \ldots, f_r$ con respecto a las variables $X_1, \ldots, X_n$ en x. Se tiene la siguiente desigualdad (ver, por ejemplo, [Sha94, página 94]):

$$\dim_x V \le \dim \mathcal{T}_x V.$$

Un punto x se dice regular si $\dim_x V = \dim \mathcal{T}_x V$. En caso que $\dim_x V < \dim \mathcal{T}_x V$, decimos que x es un punto singular de V. El conjunto de puntos singulares de V se denomina el lugar singular de V y lo notamos Σ; se tiene que Σ es una K-subvariedad cerrada de V. Una K-variedad se dice no singular si el conjunto de puntos singulares es vacío. Para una K-variedad proyectiva, los conceptos de espacio tangente, punto singular y regular se definen considerando un entorno afín del punto en cuestión. Sea V una K-variedad afín o proyectiva, supongamos que $V = \cup_{i=1}^t \mathcal{C}_i$ la descomposición de V en componentes K-irreducibles, entonces $\mathcal{C}_i \cap \mathcal{C}_j \subset \Sigma$ para todo $i \ne j$.

Sea ahora $V \subset \mathbb{P}^n$ una K-variedad proyectiva. Consideramos el morfismo

$$\theta : \mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\} \to \mathbb{P}^n \tag{2.1}$$

que a un punto con coordenadas afines $(a_0, \ldots, a_n)$ le asocia el punto proyectivo con coordenadas homogéneas $(a_0 : \cdots : a_n)$. Se define el cono afín de V como la variedad afín

$$C(V) = \theta^{-1}(V) \cup \{(0, \ldots, 0)\}.$$

Se cumplen las siguientes propiedades:

(*i*) $\dim C(V) = \dim V + 1$.

(*ii*) V es irreducible si y sólo si $C(V)$ lo es.

(*iii*) V es no singular si y sólo si $C(V)$ es no singular o su único punto singular es el origen.

2.1.1. Intersecciones completas

En esta tesis vamos a considerar una familia particular de K-variedades, que se denominan intersecciones completas.

Definición 2.1.3. *Sea V una K-variedad de dimensión r.*

i) Decimos que V es una intersección completa conjuntista *si V es la intersección de $n-r$ K-hipersuperficies.*

ii) Decimos que V es una intersección completa *si $I(V)$ puede ser generado por $n-r$ polinomios en $K[X_1,\ldots,X_n]$.*

Una K-variedad V es regular en codimensión m si el lugar singular Σ de V tiene codimensión al menos $m+1$ en V, es decir si $\dim V - \dim \Sigma \geq m+1$. Una intersección completa se dice normal si es regular en codimensión 1. Un resultado importante para intersecciones completas proyectivas es el Teorema de Conexión de Hartshorne (ver, por ejemplo, [Kun85, Theorem VI.4.2]), que enunciamos a continuación. Si $V \subset \mathbb{P}^n$ es una intersección completa definida sobre K y $W \subset V$ es una K-subvariedad de codimensión al menos 2, entonces $V \setminus W$ es conexo con la topología Zariski de $\mathbb{P}^n$ sobre K. De acuerdo a este lema, considerando $W = \Sigma$, deducimos el siguiente resultado que utilizaremos frecuentemente.

Teorema 2.1.4. *Si $V \subset \mathbb{P}^n$ es una intersección completa normal, entonces V es absolutamente irreducible.*

Cada intersección completa resulta definida por polinomios que forman una sucesión regular.

Definición 2.1.5. *Sean $f_1,\ldots,f_r \in K[X_1,\ldots,X_n]$. Decimos que $f_1,\ldots,f_r$ forman una* sucesión regular *si f_1 no es el polinomio cero y cada f_i no es divisor de cero en el anillo $K[X_1,\ldots,X_n]/(f_1,\ldots,f_{i-1})$ para $2 \leq i \leq r$.*

Si $f_1,\ldots,f_{n-r}$ forman una sucesión regular en $K[X_1,\ldots,X_n]$ o $K[X_0,\ldots,X_n]$, entonces la K-variedad afín o proyectiva que ellos definen es una intersección completa conjuntista y es equidimensional de dimensión $n-r$. Más aún, si el ideal $(f_1,\ldots,f_{n-r})$ es radical entonces dicha variedad es una intersección completa.

2.1.2. El grado de una variedad

Sea V una K-variedad irreducible. Se define el grado $\deg(V)$ de V como el número máximo de puntos en la intersección de V con una variedad lineal L de codimensión $\dim V$ para la cual dicha intersección es finita. Más generalmente, si $V = V_1 \cup V_2 \cup \cdots \cup V_r$ es la descomposición de V en componentes K-irreducibles, definimos el grado de V como $\deg V = \sum_{i=1}^{r} \deg V_i$ (ver [Hei83, Ful84]). El grado de una K-hipersuperficie H es el grado de un polinomio de grado mínimo que define a H. El grado de un abierto denso contenido en una K-variedad V es igual al grado de V. A continuación enunciamos una desigualdad de Bézout que resultará sumamente útil al momento de obtener las estimaciones (ver [Hei83, Ful84, Vog84]).

Teorema 2.1.6. *Si V y W son K-variedades, entonces*

$$\deg(V \cap W) \leq \deg V \cdot \deg W. \tag{2.2}$$

También usaremos frecuentemente el siguiente resultado.

Proposición 2.1.7 ([HS82, Proposition 2.3])**.** *Sean $V_1, \ldots, V_s$ K-variedades afines. Supongamos que $\dim V_1 = r$ y sea D el máximo de los grados de $V_2, \ldots, V_s$. Entonces $\deg(V_1 \cap \cdots \cap V_s) \leq \deg V_1 D^r$.*

Las siguientes son propiedades estándar relacionadas con la noción de grado de K-variedades.

(*i*) Sean $V \subset \mathbb{A}^n$, $\operatorname{pcl}(V) \subset \mathbb{P}^n$ su clausura proyectiva y $\widehat{V} \subset \mathbb{A}^{n+1}$ el cono afín de $\operatorname{pcl}(V)$. Entonces, (ver, por ejemplo, [CGH91, Proposition 1.11])

$$\deg V = \deg \operatorname{pcl}(V) = \deg \widehat{V}.$$

(*ii*) Sea $\phi : V \to W$ un morfismo regular lineal de K-variedades proyectivas. Entonces [Hei83, Lemma 2],

$$\deg \overline{\phi(V)} \leq \deg V, \tag{2.3}$$

donde $\overline{\phi(V)}$ denota la clausura Zariski de $\phi(V)$ en $\mathbb{P}^n$.

Sea $V \subset \mathbb{P}^n$ una K-variedad intersección completa, de grado δ, dimensión r y sea $f_1, \ldots, f_{n-r}$ un conjunto de generadores de $I(V)$. Los grados $d_1, \ldots, d_{n-r}$ dependen de V y no del sistema de generadores de $I(V)$. Sin pérdida de generalidad, podemos suponer que $d_1 \geq \cdots \geq d_{n-r}$. Definimos entonces el multigrado de V como $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$. Un resultado fundamental sobre intersecciones completas, *Teorema de Bézout*, asegura que $\delta = \prod_{i=1}^{n-r} d_i$ (ver, por ejemplo, [Har92, Theorem 18.3]).

2.2. El espacio multiproyectivo

En el Capítulo 3, tendremos que considerar hipersuperficies multiproyectivas. Es por esto que dedicamos esta sección a hacer una revisión de las definiciones y conceptos básicos del espacio multiproyectivo. Nos basamos aquí en [DKS13].

Sea $\mathbb{N} := \mathbb{Z}_{\geq 0}$ el conjunto de enteros no negativos. Dado $\boldsymbol{n} := (n_1, \ldots, n_m) \in \mathbb{N}^m$ notamos como $|\boldsymbol{n}| := n_1 + \cdots + n_m$ y $\boldsymbol{n!} := n_1! \ldots n_m!$. Si $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^m$ escribimos $\boldsymbol{\alpha} \geq \boldsymbol{\beta}$ cada vez que $\alpha_i \geq \beta_i$ para $1 \leq i \leq m$. Dado $\boldsymbol{d} := (d_1, \ldots, d_m) \in \mathbb{N}^m$, definimos el conjunto $\mathbb{N}_{\boldsymbol{d}}^{\boldsymbol{n+1}} := \mathbb{N}_{d_1}^{n_1+1} \times \cdots \times \mathbb{N}_{d_m}^{n_m+1}$ formado por los elementos $\boldsymbol{a} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) \in \mathbb{N}^{n_1+1} \times \cdots \times \mathbb{N}^{n_m+1}$ con $|\boldsymbol{a}_i| = d_i$, para $1 \leq i \leq m$.

Denotamos por $\mathbb{P}^{\boldsymbol{n}}$ al espacio multiproyectivo $\mathbb{P}^{\boldsymbol{n}} := \mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_m}$.

Para $1 \leq i \leq m$, sean $\boldsymbol{X}_i := \{X_{i,0}, \ldots, X_{i,n_i}\}$ un grupo de $n_i + 1$ variables y $\boldsymbol{X} := \{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_m\}$. Un polinomio multihomogéneo $F \in K[\boldsymbol{X}]$ de multigrado $\boldsymbol{d} := (d_1, \ldots, d_m)$ es un polinomio homogéneo de grado d_i en cada grupo de variables $\boldsymbol{X}_i$ para $1 \leq i \leq m$. Decimos que un ideal $I \subset K[\boldsymbol{X}]$ es multihomogéneo si está generado

por una familia de polinomios multihomogéneos. Dado un ideal multihomogéneo $I \subset K[\boldsymbol{X}]$, denotamos por $V(I) \subset \mathbb{P}^{\boldsymbol{n}}$ a la K-variedad definida como el conjunto de ceros comunes de los polinomios de I. En particular, una K-hipersuperficie de $\mathbb{P}^{\boldsymbol{n}}$ es el conjunto de ceros de un polinomio multihomogéneo $F \in K[\boldsymbol{X}]$. Las nociones de variedad K-irreducible y dimensión de una K-variedad de $\mathbb{P}^{\boldsymbol{n}}$ se definen igual que en el espacio proyectivo.

Sean $V \subset \mathbb{P}^{\boldsymbol{n}}$ una K-variedad multiproyectiva y

$$\boldsymbol{\Theta} : \mathbb{A}^{n_1+1} \setminus \{\mathbf{0}\} \times \cdots \times \mathbb{A}^{n_m+1} \setminus \{\mathbf{0}\} \to \mathbb{P}^{\boldsymbol{n}}$$

el morfismo dado por $\boldsymbol{\Theta} := (\theta_1, \ldots, \theta_m)$, donde θ_i es el morfismo definido en (2.1), $(1 \leq i \leq m)$. Definimos el *cono afín* de V como la siguiente variedad:

$$\begin{aligned}\boldsymbol{C}(V) = \boldsymbol{\Theta}^{-1}(V) \cup (\{\mathbf{0}\} \times \mathbb{A}^{n_2+1} \times \cdots \times \mathbb{A}^{n_m+1}) \cup (\mathbb{A}^{n_1+1} \times \{\mathbf{0}\} \times \cdots \times \mathbb{A}^{n_m+1}) \\ \cup \cdots \cup (\mathbb{A}^{n_1+1} \times \mathbb{A}^{n_2+1} \times \cdots \times \{\mathbf{0}\}).\end{aligned}$$

Se tiene que $\dim \boldsymbol{C}(V) = \dim V + m$.

Sea $V \subset \mathbb{P}^{\boldsymbol{n}}$ una $\overline{\mathbb{F}}_q$-variedad irreducible, el anillo cociente $\overline{\mathbb{F}}_q[\boldsymbol{X}]/I(V)$ es multigraduado y denotamos por $(\overline{\mathbb{F}}_q[\boldsymbol{X}]/I(V))_{\boldsymbol{b}}$ a la componente de multigrado $\boldsymbol{b} \in \mathbb{N}^m$. La función Hilbert–Samuel de V es la función $H_V : \mathbb{N}^m \to \mathbb{N}$ definida como $H_V(\boldsymbol{b}) := \dim(\overline{\mathbb{F}}_q[\boldsymbol{X}]/I(V))_{\boldsymbol{b}}$. Dada una variedad irreducible V de dimensión r, se tiene que existe $\boldsymbol{\delta_0} \in \mathbb{N}^m$ y un único polinomio $P_V \in \mathbb{Q}[z_1, \ldots, z_m]$ de grado $r = \dim V$ tal que $P_V(\boldsymbol{\delta}) = H_V(\boldsymbol{\delta})$ para cada $\boldsymbol{\delta} \in \mathbb{N}^m$ con $\boldsymbol{\delta} \geq \boldsymbol{\delta_0}$ (ver, por ejemplo, [Rém01, Theorem 2.10 (i)]).

Sea V una variedad irreducible de dimensión r, dado $\boldsymbol{r} \in \mathbb{N}_r^m$, es decir, $\boldsymbol{r} \in \mathbb{N}^m$ tal que $|\boldsymbol{r}| = r$, definimos el grado mixto de V de índice $\boldsymbol{r}$ como el entero no negativo

$$\deg_{\boldsymbol{r}}(V) := \boldsymbol{r}! \operatorname{coeff}_{\boldsymbol{r}}(P_V).$$

Equivalentemente el grado mixto de V de índice $\boldsymbol{r}$ se puede definir de la siguiente manera: si $\boldsymbol{r} := (r_1, \ldots, r_m) \in \mathbb{N}^m$ es tal que $r_1 + \cdots + r_m = r$, para cada $1 \leq i \leq m$, y $H_i^1, \ldots, H_i^{r_i} \subset \mathbb{P}^{n_i}$ hiperplanos genéricos, luego el grado mixto de V de índice $\boldsymbol{r}$ se define como el cardinal de la intersección

$$V \cap \bigcap_{i=1}^{m} \bigcap_{j=1}^{r_i} \mathbb{P}_1^n \times \cdots \times \mathbb{P}^{n_i-1} \times H_j^i \times \mathbb{P}^{n_i+1} \times \cdots \times \mathbb{P}^{n_m},$$

.

El anillo de Chow en $\mathbb{P}^{\boldsymbol{n}}$ es el anillo graduado

$$A^*(\mathbb{P}^{\boldsymbol{n}}) := \mathbb{Z}[\theta_1, \ldots, \theta_m]/(\theta_1^{n_1+1}, \ldots, \theta_m^{n_m+1}),$$

donde cada θ_i denota la preimagen de un hiperplano contenido en $\mathbb{P}^{n_i}$ bajo la proyección $\mathbb{P}^{\boldsymbol{n}} \to \mathbb{P}^{n_i}$. Dada una K-variedad $V \subset \mathbb{P}^{\boldsymbol{n}}$ equidimensional de dimensión r, su clase en el anillo de Chow es

$$[V] := \sum_{\boldsymbol{b}} \deg_{\boldsymbol{b}}(V) \theta_1^{n_1-b_1} \cdots \theta_m^{n_m-b_1} \in A^*(\mathbb{P}^{\boldsymbol{n}}),$$

donde la suma recorre el conjunto de multiíndices $\boldsymbol{b} \in \mathbb{N}_r^m$ con $\boldsymbol{b} \leq \boldsymbol{n}$. Éste es un elemento homogéneo de grado $|\boldsymbol{n}| - r$. En particular, si $\mathcal{H} \subset \mathbb{P}^{\boldsymbol{n}}$ es una K-hipersuperficie y $F \in K[\boldsymbol{X}]$ es un polinomio de grado mínimo que define a $\mathcal{H}$, entonces

$$[\mathcal{H}] := \sum_{i=1}^{m} \deg_{\boldsymbol{X}_i}(F)\, \theta_i, \tag{2.4}$$

equivalentemente, $\deg_{\boldsymbol{n}-e_i}(\mathcal{H}) = \deg_{\boldsymbol{X}_i}(F)$ para $1 \leq i \leq m$, donde e_i denota el i-ésimo vector de la base canónica de $\mathbb{R}^m$, (ver, por ejemplo, [DKS13, Proposition 1.10]).

Una herramienta fundamental para estimar el grado mixto de intersecciones de variedades multiproyectivas es el teorema de Bézout multiproyectivo (ver [DKS13, Theorem 1.11]). Si $V \subset \mathbb{P}^{\boldsymbol{n}}$ es una variedad multiproyectiva equidimensional de dimensión $r > 0$ y $F \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ un polinomio multihomogéneo libre de cuadrados tal que $V \cap V(F)$ es equidimensional de dimensión $r-1$, entonces

$$[V \cap V(F)] = [V][V(F)], \tag{2.5}$$

Finalmente, mencionamos el siguiente resultado, que muestra que los grados mixtos son monótonos con respecto a proyecciones lineales. Sea $\boldsymbol{l} := (l_1, \ldots, l_m) \in \mathbb{N}^m$ una m-upla con $\boldsymbol{l} \leq \boldsymbol{n}$ y sea $\pi : \mathbb{P}^{\boldsymbol{n}} \dashrightarrow \mathbb{P}^{\boldsymbol{l}}$ la proyección lineal que a cada $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \in \mathbb{P}^{\boldsymbol{n}}$ le asigna las primeras coordenadas l_i de cada coordenada $\boldsymbol{x}_i$, es decir,

$$\pi(x_{i,j} : 1 \leq i \leq m, 0 \leq j \leq n_i) := (x_{i,j} : 1 \leq i \leq m, 0 \leq j \leq l_i).$$

Este morfismo racional induce el siguiente morfismo $\mathbb{Z}$-lineal inyectivo:

$$\jmath : A^*(\mathbb{P}^{\boldsymbol{l}}) \to A^*(\mathbb{P}^{\boldsymbol{n}}), \quad \jmath(P) := \boldsymbol{\theta}^{\boldsymbol{n}-\boldsymbol{l}} P.$$

Si $V \subset \mathbb{P}^{\boldsymbol{n}}$ es una variedad equidimensional y $\dim \overline{\pi(V)} = \dim V$, entonces se tiene la siguiente desigualdad (ver [DKS13, Proposition 1.16]):

$$\jmath([\overline{\pi(V)}]) \leq [V]. \tag{2.6}$$

2.3. Puntos q-racionales de $\mathbb{F}_q$-variedades

De ahora en más consideraremos $K = \mathbb{F}_q$ y $\mathbb{A}^n$ y $\mathbb{P}^n$ denotarán el espacio afín y proyectivo de dimensión n definidos sobre $\overline{\mathbb{F}}_q$ respectivamente. Sea V una $\mathbb{F}_q$-variedad afín o proyectiva. Dado $x \in V$, decimos que x es un punto q-racional de V si todas sus coordenadas pertenecen a $\mathbb{F}_q$. Notamos por $V(\mathbb{F}_q)$ al conjunto de puntos q-racionales de V. Cabe observar que el espacio afín de dimensión n sobre $\mathbb{F}_q$ tiene cardinal $|\mathbb{A}^n(\mathbb{F}_q)| = q^n$ y el espacio proyectivo de dimensión n sobre $\mathbb{F}_q$ tiene cardinal

$$p_n := |\mathbb{P}^n(\mathbb{F}_q)| = q^n + q^{n-1} + \cdots + q + 1.$$

Dada una $\mathbb{F}_q$-variedad V, determinar de manera exacta, estimar o garantizar la existencia de puntos q-racionales de V es un problema clásico de geometría aritmética. Dado que se conocen pocos resultados sobre la cantidad exacta de puntos q-racionales, muchas veces resulta útil contar con cotas, estimaciones y resultados que

garanticen la existencia de dichos puntos. En esta sección hacemos una revisión de las cotas superiores que se conocen y damos un resultado propio sobre la cantidad de puntos q-racionales de hipersuperficies multiproyectivas.

2.3.1. Algunas cotas superiores y resultados de existencia

Comenzamos con algunos resultados clásicos para hipersuperficies.

Proposición 2.3.1 ([LN83, Theorems 6.13 y 6.15]). *Sea H una $\overline{\mathbb{F}}_q$-hipersuperficie en $\mathbb{A}^n$ o $\mathbb{P}^n$ definida por un polinomio $f \in \overline{\mathbb{F}}_q[X_1, \ldots, X_n]$ de grado δ en el caso afín, o $f \in \overline{\mathbb{F}}_q[X_0, \ldots, X_n]$ homogéneo de grado δ en el caso proyectivo. Entonces*

(i) Si H es una $\overline{\mathbb{F}}_q$-hipersuperficie afín, $|H(\mathbb{F}_q)| \leq \delta \cdot q^{n-1}$.

(ii) Si H es una $\overline{\mathbb{F}}_q$-hipersuperficie proyectiva, $|H(\mathbb{F}_q)| \leq \delta \cdot p_{n-1}$.

Observamos que la cota para el caso afín es óptima si $\delta \leq q$. En efecto, considerando el polinomio $f = (X_1 - c_1) \cdots (X_1 - c_\delta)$, siendo $c_1, \ldots, c_\delta$ elementos distintos en $\mathbb{F}_q$, la cantidad de puntos q-racionales de la hipersuperficie definida por f es δq^{n-1}. Sin embargo, para $\overline{\mathbb{F}}_q$-hipersuperficies proyectivas la cota de la Proposición 2.3.1 no es la mejor posible. Para $\mathbb{F}_q$-hipersuperficies proyectivas, J. P. Serre proporciona una cota más precisa, que enunciamos a continuación.

Proposición 2.3.2 ([Ser91]). *Sea $F \in \mathbb{F}_q[X_0, \ldots, X_n]$ un polinomio homogéneo, no nulo, de grado $\delta < q$. Entonces se verifica que $|H(\mathbb{F}_q)| \leq \delta q^{n-1} + p_{n-2}$.*

Cabe mencionar que es fácil extender el resultado a $\overline{\mathbb{F}}_q$-hipersuperficies. En efecto, tenemos el siguiente resultado.

Proposición 2.3.3. *Sea $F \in \overline{\mathbb{F}}_q[X_0, \ldots, X_n]$ un polinomio homogéneo, no nulo, de grado $\delta < q$. Entonces se satisface la siguiente cota superior:*

$$|H(\mathbb{F}_q)| \leq \delta q^{n-1} + p_{n-2}.$$

Demostración. Sea K la extensión finita de $\mathbb{F}_q$ definida por los coeficientes de F y sea $\{\alpha_1, \ldots, \alpha_r\}$ una base de K como $\mathbb{F}_q$-espacio vectorial. Entonces existen únicos polinomios $F_1, \ldots, F_r \in \mathbb{F}_q[X_0, \ldots, X_r]$, homogéneos de grado δ o cero, tales que $F = \alpha_1 F_1 + \cdots + \alpha_r F_r$. Supongamos sin pérdida de generalidad que $F_1 \neq 0$. Entonces es claro que el conjunto de ceros de F en $\mathbb{P}^n(\mathbb{F}_q)$ está contenido en el conjunto de ceros de F_1 en $\mathbb{P}^n(\mathbb{F}_q)$. Notamos por N_1 a la cantidad de ceros en $\mathbb{P}^n(\mathbb{F}_q)$ de F_1. De acuerdo a la proposición anterior se obtiene que $|H(\mathbb{F}_q)| \leq N_1 \leq \delta q^{n-1} + p_{n-2}$, lo que concluye la demostración. □

A continuación damos cotas superiores sobre la cantidad de puntos q-racionales de variedades proyectivas y afines que generalizan la Proposición 2.3.1.

Proposición 2.3.4. *Sea V una variedad afín o proyectiva de dimensión r y grado δ definida en el espacio de dimensión n sobre $\overline{\mathbb{F}}_q$. Entonces la cantidad de puntos q-racionales de V satisface*

(i) Si V es una variedad afín, $|V(\mathbb{F}_q)| \leq \delta q^r$.

(ii) Si V es una variedad proyectiva, $|V(\mathbb{F}_q)| \leq \delta p_r$.

En [CM06, Lemma 2.1] y [CM07a, Proposition 3.1] podemos encontrar demostraciones simples de estos resultados que se basan en la aplicación de la desigualdad de Bézout del Teorema 2.2.

En cuanto a la existencia de puntos q-racionales, un resultado clásico es el teorema de Chevalley-Warning.

Teorema 2.3.5 ([LN83, Corollary 6.9]). *Sean $f_1, \ldots, f_r \in \overline{\mathbb{F}}_q[X_1, \ldots, X_n]$ polinomios con $f_i(0, \ldots, 0) = 0$ para $1 \leq i \leq r$ y $\sum_{i=1}^{r} \deg f_i < n$. Entonces existe un punto q-racional $c = (c_1, \ldots, c_n) \neq (0, \ldots, 0)$ de la variedad afín que ellos definen.*

En lo que respecta a la existencia de puntos q-racionales de $\mathbb{F}_q$-hipersuperficies, el mejor resultado que se conoce es el siguiente.

Teorema 2.3.6 ([CM06, Theorem 5.4]). *Si $q > 2\,\delta^4$ y $H \subset \mathbb{A}^n$ es una $\mathbb{F}_q$-hipersuperficie absolutamente irreducible de grado δ, entonces H tiene al menos un punto q-racional.*

La condición sobre q dada en el Teorema 2.3.6 es casi óptima, en el sentido de que si q es del orden de δ^3, existen $\mathbb{F}_q$-hipersuperficies absolutamente irreducibles sin puntos q-racionales (ver [HLT05] o [Yek07] para familias de ejemplos).

2.3.2. Número promedio de ceros

A continuación exhibimos fórmulas sobre el número promedio y la varianza de ceros q-racionales (ver, por ejemplo, [LN83, Theorems 6.116 y 6.17]). Estos resultados dan una idea sobre cómo estimar la cantidad de puntos q-racionales de una $\mathbb{F}_q$-hipersuperficie y sobre el error que cometemos al estimar dicho número por el valor promedio.

Sea d un entero positivo y sea Ω_d el conjunto de polinomios $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ de grado a lo sumo d. Si $N(f)$ es la cantidad de ceros q-racionales de f, se tiene que

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

Con las mismas hipótesis, se tiene la siguiente fórmula para la desviación de este promedio:

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

De aquí se ve que un polinomio $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ tiene en promedio q^{n-1} ceros q-racionales y el error que se comete al estimar la cantidad de ceros q-racionales por dicho promedio es del orden de $q^{\frac{n-1}{2}}$. Luego, si H es una $\mathbb{F}_q$-hipersuperficie afín, estimamos la cantidad de puntos q-racionales de la misma, por q^{n-1}. Sería de esperar que el error cometido $\left||H(\mathbb{F}_q)| - q^{n-1}\right|$ sea del orden de $q^{\frac{n-1}{2}}$. Desafortunadamente,

esto no es cierto para una hipersuperficie afín arbitraria; por ejemplo, si H es relativamente irreducible (es decir, es $\mathbb{F}_q$-irreducible pero no absolutamente irreducible) se tiene el siguiente resultado.

Proposición 2.3.7 ([CM06, Lemma 2.3]). *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$-variedad relativamente irreducible de dimensión r y grado δ. Entonces $|V(\mathbb{F}_q)| \leq \delta^2\, q^{r-1}/4$.*

En el caso en que la $\mathbb{F}_q$-hipersuperficie $H \subset \mathbb{A}^n$ es absolutamente irreducible, es posible estimar en forma satisfactoria el error $||H(\mathbb{F}_q)| - q^{n-1}|$, como se expresa en el siguiente resultado (ver, por ejemplo, [Sch76, GL02a, GL02b] por otras estimaciones y [Sch74] por una cota inferior).

Teorema 2.3.8 ([CM06, Theorems 5.2 y 5.3]). *Sea $H \subset \mathbb{A}^n$ una $\mathbb{F}_q$-hipersuperficie de grado δ. Entonces se satisface la siguiente estimación:*

$$\big||H(\mathbb{F}_q)| - q^{n-1}\big| \leq (\delta-1)(\delta-2)\, q^{n-3/2} + 5\delta^{13/3}\, q^{n-2}.$$

Si además $q > 15\,\delta^{13/3}$, entonces

$$\big||H(\mathbb{F}_q)| - q^{n-1}\big| \leq (\delta-1)(\delta-2)\, q^{n-3/2} + (5\delta^2+\delta+1)\, q^{n-2}.$$

Cabe mencionar, de todas formas, que la absoluta irreducibilidad no es una restricción significativa dado que "casi todas" las hipersuperficies son absolutamente irreducibles (ver [vzGVZ13, Corollary 6.8]).

Se tiene un resultado similar al del número promedio de ceros de un polinomio definido sobre $\mathbb{F}_q$ para $\mathbb{F}_q$-variedades afines.

Teorema 2.3.9. *Sea $\boldsymbol{d} = (d_1, \ldots, d_{n-r}) \in \mathbb{N}^{n-r}$ y $\Omega_{\boldsymbol{d}}$ el conjunto de polinomios*

$$\Omega_{\boldsymbol{d}} := \{\boldsymbol{F} := (f_1, \ldots, f_{n-r}) : \ \ f_i \in \mathbb{F}_q[X_1, \ldots, X_n],\ \deg f_i \leq d_i \ \text{ para } \ 1 \leq i \leq n-r\}.$$

Se obtiene entonces

$$\frac{1}{|\Omega_{\boldsymbol{d}}|} \sum_{\boldsymbol{F} \in \Omega_{\boldsymbol{d}}} |V(\boldsymbol{F})(\mathbb{F}_q)| = q^r.$$

Demostración. Se tiene

$$\sum_{\boldsymbol{F} \in \Omega_{\boldsymbol{d}}} |V(\boldsymbol{F})(\mathbb{F}_q)| = \sum_{\boldsymbol{F} \in \Omega_{\boldsymbol{d}}} \sum_{\substack{x \in \mathbb{F}_q^n \\ \boldsymbol{F}(x) = \boldsymbol{0}}} 1 = \sum_{x \in \mathbb{F}_q^n} \sum_{\substack{\boldsymbol{F} \in \Omega_{\boldsymbol{d}} \\ \boldsymbol{F}(x) = \boldsymbol{0}}} 1 = \sum_{x \in \mathbb{F}_q^n} q^{\dim \Omega_{\boldsymbol{d}} - (n-r)} = |\Omega_{\boldsymbol{d}}| q^r.$$

El enunciado del teorema se sigue fácilmente. □

Análogamente, se puede obtener un resultado similar para la varianza, a saber:

$$\frac{1}{|\Omega_{\boldsymbol{d}}|} \sum_{\boldsymbol{F} \in \Omega_{\boldsymbol{d}}} (V(\boldsymbol{F})(\mathbb{F}_q) - q^r)^2 = q^r - q^{r-1}.$$

A partir de estos resultados, al igual que en el caso de hipersuperficies, resulta natural pensar en estimar la cantidad de puntos de una $\mathbb{F}_q$-variedad afín de dimensión r por q^r y esperar que el error cometido sea del orden $q^{\frac{r}{2}}$. En el caso en que la variedad en consideración es absolutamente irreducible, tenemos los siguientes resultados (ver [GL02a, GL02b, CM07a]).

Teorema 2.3.10 ([GL02b, Theorem 4.1]). *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$-variedad absolutamente irreducible de dimensión r y grado δ. Entonces se verifica que:*

$$\big||V(\mathbb{F}_q)| - q^r\big| \leq (\delta-1)(\delta-2)q^{r-1/2} + 6 \cdot 2^s(sd+3)^{n+1}q^{r-1},$$

donde s es el número de ecuaciones que definen a V y d es el grado máximo de las mismas.

Teorema 2.3.11 ([CM07a, Theorem 7.1]). *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$-variedad absolutamente irreducible de dimensión r y grado δ. Si $q > 2(r+1)\delta^2$, entonces se satisface la siguiente estimación:*

$$\big||V(\mathbb{F}_q)| - q^r\big| \leq (\delta-1)(\delta-2)q^{r-1/2} + 5\,\delta^{13/3}q^{r-1}.$$

En el caso en que la variedad no es absolutamente irreducible, no es válido estimar la cantidad de puntos por q^r. Por ejemplo, en [FHJ94, Proposition 3.3 (b)] los autores prueban que una $\mathbb{F}_q$-variedad normal que no es absolutamente irreducible no tiene puntos q-racionales.

En esta tesis veremos que es posible obtener mejores estimaciones que las de los Teoremas 2.3.10 y 2.3.11 cuando las variedades en consideración son intersecciones completas cuyo lugar singular tiene codimensión al menos 2.

2.3.3. Conteo de puntos q-racionales de hipersuperficies multihomogéneas

Como mencionamos anteriormente, en esta tesis, vamos a trabajar en diversas oportunidades con hipersuperficies multiproyectivas. Desafortunadamente, no existen resultados al respecto. Es por ello que dedicamos esta sección a obtener un resultado sobre la cantidad de puntos q-racionales de hipersuperficies multiproyectivas.

Sea $\boldsymbol{n} := (n_1, \ldots, n_m) \in \mathbb{N}^m$ y consideremos el espacio multiproyectivo $\mathbb{P}^{\boldsymbol{n}}$. Denotamos por $\mathbb{P}^{\boldsymbol{n}}(\mathbb{F}_q)$ al conjunto de puntos q-racionales de $\mathbb{P}^{\boldsymbol{n}}$. Para $1 \leq i \leq m$, sea $\boldsymbol{X}_i := \{X_{i,0} \ldots X_{i,n_i}\}$ un grupo de $n_i + 1$ variables y $\boldsymbol{X} := \{\boldsymbol{X}_1 \ldots \boldsymbol{X}_m\}$. Sea $F \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ un polinomio multihomogéneo de multigrado $\boldsymbol{d} := (d_1, \ldots, d_m)$. En esta sección vamos a dar dos resultados sobre la cantidad de ceros q-racionales de F. En primer lugar proporcionamos una cota superior no trivial para dicha cantidad, que generaliza la Proposición 2.3.4 (ii) para el caso multiproyectivo. En segundo lugar, damos un resultado que establece condiciones sobre q que aseguran la existencia de un punto $\boldsymbol{x} \in \mathbb{P}^{\boldsymbol{n}}(\mathbb{F}_q)$ que no anula a F.

Para $\boldsymbol{\alpha} \in \mathbb{N}^m$, fijamos las siguientes notaciones: $\boldsymbol{d}^{\boldsymbol{\alpha}} := d_1^{\alpha_1} \cdots d_m^{\alpha_m}$ y $p_{\boldsymbol{n}-\boldsymbol{\alpha}} := p_{n_1-\alpha_1} \cdots p_{n_m-\alpha_m}$ si $\boldsymbol{n} \geq \boldsymbol{\alpha}$. Sea además

$$\eta_m(\boldsymbol{d}, \boldsymbol{n}) := \sum_{\boldsymbol{\varepsilon} \in \{0,1\}^m \setminus \{\boldsymbol{0}\}} (-1)^{|\boldsymbol{\varepsilon}|+1} \boldsymbol{d}^{\boldsymbol{\varepsilon}} p_{\boldsymbol{n}-\boldsymbol{\varepsilon}}.$$

Observamos que $\eta_m(\boldsymbol{d}, \boldsymbol{n}) \leq p_{n_1} \cdots p_{m_n} = |\mathbb{P}^{\boldsymbol{n}}(\mathbb{F}_q)|$ si $q \geq \max\limits_{1 \leq i \leq m} d_i$, pero esta desigualdad podría no verificarse para $q < \max\limits_{1 \leq i \leq m} d_i$.

Proposición 2.3.12. *Sea $F \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ un polinomio multihomogéneo de multigrado $\boldsymbol{d} := (d_1, \ldots, d_m)$ con $\max\limits_{1\leq i\leq m} d_i \leq q$ y sea N la cantidad de ceros de F en $\mathbb{P}^{\boldsymbol{n}}(\mathbb{F}_q)$. Entonces*

$$N \leq \eta_m(\boldsymbol{d}, \boldsymbol{n}) := \sum_{\boldsymbol{\varepsilon}\in\{0,1\}^m\setminus\{\boldsymbol{0}\}} (-1)^{|\boldsymbol{\varepsilon}|+1} \boldsymbol{d}^{\boldsymbol{\varepsilon}} p_{\boldsymbol{n}-\boldsymbol{\varepsilon}}.$$

Demostración. Hacemos inducción en m. El caso $m = 1$ sigue de la Proposición 2.3.4 (ii) para $\mathbb{F}_q$-hipersuperficies.

Supongamos que el enunciado es válido para $m-1$ y sea $F \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ un polinomio multihomogéneo en los grupos de variables $\boldsymbol{X} := \{\boldsymbol{X}_1 \ldots \boldsymbol{X}_m\}$. Sea Z_m el subconjunto de $\mathbb{P}^{n_m}(\mathbb{F}_q)$ formado por los elementos $\boldsymbol{x}_m$ para los que la sustitución $F(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_{m-1}, \boldsymbol{x}_m)$ de $\boldsymbol{X}_m$ por $\boldsymbol{x}_m$ en F da lugar al polinomio nulo de $\overline{\mathbb{F}}_q[\boldsymbol{X}_1, \ldots, \boldsymbol{X}_{m-1}]$. Consideremos a F como un elemento de $\mathbb{F}_q[\boldsymbol{X}_m][\boldsymbol{X}_1, \ldots, \boldsymbol{X}_{m-1}]$ y sea $A \in \mathbb{F}_q[\boldsymbol{X}_m]$ un polinomio homogéneo no nulo de grado d_m que aparece como el coeficiente de un monomio dado $\boldsymbol{X}_1^{\boldsymbol{\alpha}_1} \cdots \boldsymbol{X}_{m-1}^{\boldsymbol{\alpha}_{m-1}}$ en la representación densa de F. Es claro que Z_m está contenido en el conjunto de ceros q-racionales de A. Por lo tanto, la Proposición 2.3.4 (ii) implica que $|Z_m| \leq d_m p_{n_m-1}$.

Como $d_m \leq q$ por hipótesis, se sigue que $|Z_m| \leq d_m p_{n_m-1} < p_{n_m}$. Dado que $|\mathbb{P}^{n_m}(\mathbb{F}_q)| = p_{n_m}$, se tiene que $\mathbb{P}^{n_m}(\mathbb{F}_q) \setminus Z_m$ es no vacío y, por lo tanto, podemos fijar un elemento $\boldsymbol{x}_m \in \mathbb{P}^{n_m}(\mathbb{F}_q) \setminus Z_m$. Notemos por N_{m-1} a la cantidad de ceros de $F(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_{m-1}, \boldsymbol{x}_m)$ en $\mathbb{P}^{n_1}(\mathbb{F}_q) \times \cdots \times \mathbb{P}^{n_{m-1}}(\mathbb{F}_q)$. Combinando la hipótesis inductiva y el hecho de que $\max\limits_{1\leq i\leq m} d_i \leq q$, se tiene que

$$N_{m-1} \leq \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*) \leq p_{n_1} \cdots p_{n_{m-1}},$$

donde $\boldsymbol{d}^* := (d_1, \ldots, d_{m-1})$ y $\boldsymbol{n}^* := (n_1, \ldots, n_{m-1})$. En consecuencia, obtenemos

$$\begin{aligned} N &\leq |Z_m| \cdot p_{n_1} \cdots p_{n_{m-1}} + (p_{n_m} - |Z_m|) \cdot \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*) \\ &= |Z_m| \left(p_{n_1} \cdots p_{n_{m-1}} - \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*)\right) + \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*) \cdot p_{n_m} \\ &\leq d_m \cdot p_{n_m-1}(p_{n_1} \cdots p_{n_{m-1}} - \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*)) + \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*) \cdot p_{n_m} \end{aligned}$$

Como $\max\limits_{1\leq i\leq m} d_i \leq q$ se tiene que $p_{n_1} \cdots p_{n_{m-1}} - \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*) \geq 0$. Luego

$$N \leq d_m p_{n_m-1} p_{n_1} \cdots p_{n_{m-1}} - \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*) d_m p_{n_m-1} + \eta_{m-1}(\boldsymbol{d}^*, \boldsymbol{n}^*) p_{n_m} = \eta_m(\boldsymbol{d}, \boldsymbol{n}).$$

Esto concluye la demostración de la proposición. □

Cabe mencionar que en la demostración de la proposición anterior utilizamos la cota superior de la Proposición 2.3.4 (ii) para acotar el número de ceros de un polinomio homogéneo en $\overline{\mathbb{F}}_q[\boldsymbol{X}_m]$ dado. Por otro lado, si utilizamos la cota de la Proposición 2.3.3, la cota de la Proposición 2.3.12 mejora sensiblemente. En particular si $\boldsymbol{d}, \boldsymbol{n} \in \mathbb{N}^m$ son de la forma $\boldsymbol{d} := (d, \ldots, d)$ y $\boldsymbol{n} := (n, \ldots, n)$ con $d < q$, combinando la demostración de la Proposición 2.3.12 y la Proposición 2.3.3 obtenemos

$$N \leq p_n^m - (q^n - (d-1)q^{n-1})^m. \tag{2.7}$$

Como consecuencia de la proposición anterior obtenemos el siguiente resultado que proporciona condiciones sobre el tamaño del cuerpo finito que permiten asegurar la existencia de un punto q-racional que no anula a un cierto polinomio multihomogéneo.

Corolario 2.3.13. *Sea $F \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ un polinomio multihomogéneo de multigrado $\boldsymbol{d}$ y sea $d := \max_{1\leq i\leq m} d_i$. Si $q > d$, entonces existe $\boldsymbol{x} \in \mathbb{P}^{\boldsymbol{n}}(\mathbb{F}_q)$ tal que $F(\boldsymbol{x}) \neq 0$.*

Demostración. Sea N la cantidad de ceros q-racionales de F. De acuerdo a la Proposición 2.3.12 se tiene que la cantidad de puntos $\boldsymbol{x} \in \mathbb{P}^{\boldsymbol{n}}(\mathbb{F}_q)$ tales que $f(\boldsymbol{x}) \neq 0$ está acotado inferiormente por

$$\boldsymbol{p_n} - N \geq \boldsymbol{p_n} - \sum_{\boldsymbol{\varepsilon}\in\{0,1\}^m\setminus\{\boldsymbol{0}\}} (-1)^{|\boldsymbol{\varepsilon}|+1}\boldsymbol{d}^{\boldsymbol{\varepsilon}} p_{\boldsymbol{n}-\boldsymbol{\varepsilon}} = \sum_{\boldsymbol{\varepsilon}\in\{0,1\}^m} (-1)^{|\boldsymbol{\varepsilon}|+1}\boldsymbol{d}^{\boldsymbol{\varepsilon}} p_{\boldsymbol{n}-\boldsymbol{\varepsilon}}.$$

Asimismo, tenemos la siguiente igualdad:

$$\sum_{\boldsymbol{\varepsilon}\in\{0,1\}^m} (-1)^{|\boldsymbol{\varepsilon}|+1}\boldsymbol{d}^{\boldsymbol{\varepsilon}} p_{\boldsymbol{n}-\boldsymbol{\varepsilon}} = \prod_{i=1}^{m}(p_{n_i} - d_i \cdot p_{n_i-1}). \tag{2.8}$$

Como $q > d$ por hipótesis, se tiene que $p_{n_i} > d_i \cdot p_{n_i-1}$ para $1 \leq i \leq m$. Luego, el lado derecho de (2.8) es estrictamente positivo, lo que implica que $\boldsymbol{p_n} - N > 0$. Esto concluye la demostración del corolario. □

El Corolario 2.3.13 será sumamente útil en este trabajo por los motivos que exponemos a continuación. En el Capítulo 3 nos encontraremos con diversas propiedades genéricas que se enuncian en términos de la no anulación de ciertos polinomios multihomogéneos. El resultado arriba mencionado nos permite dar cotas superiores sobre el grado de dichas condiciones, es decir, nos permite establecer condiciones sobre q que implican que existe un punto q-racional que no anula a dichos polinomios, con lo cual tales condiciones genéricas resultan satisfactibles sobre el correspondiente cuerpo finito $\mathbb{F}_q$. Cabe destacar que dichas cotas de grado mejoran notablemente las que se obtienen considerando al polinomio en cuestión como un polinomio homogéneo en todas las variables, debido precisamente a la estructura multihomogénea subyacente.

Finalizamos esta sección con un resultado para la cantidad de ceros de un polinomio multihomogéneo F en $\mathbb{F}_q^{\boldsymbol{n+1}} := \mathbb{F}_q^{n_1+1} \times \cdots \times \mathbb{F}_q^{n_m+1}$ que será utilizado en la Sección 4.2.3. Su demostración sigue un argumento similar al de la Proposición 2.3.12. Sea

$$\eta_m^a(\boldsymbol{d}, \boldsymbol{n}) := \sum_{\boldsymbol{\varepsilon}\in\{0,1\}^m\setminus\{\boldsymbol{0}\}} (-1)^{|\boldsymbol{\varepsilon}|+1}\boldsymbol{d}^{\boldsymbol{\varepsilon}}\boldsymbol{q}^{\boldsymbol{n+1-\varepsilon}}, \tag{2.9}$$

donde $\boldsymbol{q}, \boldsymbol{1} \in \mathbb{N}^m$ se definen como $\boldsymbol{q} := (q, \ldots, q)$ y $\boldsymbol{1} := (1, \ldots, 1)$. Observemos que $\eta_m^a(\boldsymbol{d}, \boldsymbol{n}) < q^{n_1+\ldots+n_m+m}$ si $\max\limits_{1\leq i\leq m} d_i < q$. Obtenemos el siguiente resultado.

Proposición 2.3.14. *Sea $F \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ un polinomio multihomogéneo de multigrado $\boldsymbol{d}$ con $\max\limits_{1\leq i\leq m} d_i < q$ y sea N_a la cantidad de ceros de F en $\mathbb{F}_q^{\boldsymbol{n+1}}$. Entonces*

$$N_a \leq \eta_m^a(\boldsymbol{d}, \boldsymbol{n}).$$

Demostración. La demostración es similar a la de la Proposición 2.3.12. Hacemos inducción en m. El caso $m = 1$ se deduce de la Proposición 2.3.4 (i).

Supongamos que la afirmación es válida para $m-1$ y sea $F \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ un polinomio multihomogéneo en los grupos de variables $\boldsymbol{X} := \{\boldsymbol{X}_1 \dots \boldsymbol{X}_m\}$ y multigrado $\boldsymbol{d} = (d_1, \dots, d_m)$. Sea Z_m^a el siguiente subconjunto de $\mathbb{F}_q^{n_m+1}$:

$$Z_m^a := \{\boldsymbol{x}_m \in \mathbb{F}_q^{n_m+1} : \ F(\boldsymbol{X}_1, \dots, \boldsymbol{X}_{m-1}, \boldsymbol{x}_m) = 0\}.$$

Sea $A \in \overline{\mathbb{F}}_q[\boldsymbol{X}_m]$ un polinomio homogéneo no nulo de grado d_m que aparece como coeficiente de un monomio dado $\boldsymbol{X}_1^{\boldsymbol{\alpha}_1} \cdots \boldsymbol{X}_{m-1}^{\boldsymbol{\alpha}_{m-1}}$ en la representación densa de F, considerando a F como un elemento de $\overline{\mathbb{F}}_q[\boldsymbol{X}_m][\boldsymbol{X}_1, \dots, \boldsymbol{X}_{m-1}]$. Es claro que Z_m^a está contenido en el conjunto de ceros en $\mathbb{F}_q^{n_m+1}$ de A. Por lo tanto, la Proposición 2.3.4 parte (i) implica que $|Z_m^a| \leq d_m q^{n_m}$. Como $d_m < q$ entonces $|Z_m^a| < q^{n_m+1}$, lo que implica que $\mathbb{F}_q^{n_m+1} \setminus Z_m^a$ es no vacío. Fijamos $\boldsymbol{x}_m \in \mathbb{F}_q^{n_m+1} \setminus Z_m^a$ y sea N_{m-1}^a la cantidad de ceros de $F(\boldsymbol{X}_1, \dots, \boldsymbol{X}_{m-1}, \boldsymbol{x}_m)$ en $\mathbb{F}_q^{n_1+1} \times \cdots \times \mathbb{F}_q^{n_{m-1}+1}$. Por hipótesis inductiva y el hecho de que $d < q$ obtenemos

$$N_{m-1}^a \leq \eta_{m-1}^a(\boldsymbol{d}^*, \boldsymbol{n}^*) < q^{n_1+\cdots+n_{m-1}+m-1},$$

donde $\boldsymbol{d}^* := (d_1, \dots, d_{m-1})$ y $\boldsymbol{n}^* := (n_1, \dots, n_{m-1})$. En consecuencia

$$\begin{aligned} N_a &\leq |Z_m^a| \cdot q^{n_1+\cdots+n_{m-1}+m-1} + (q^{n_m+1} - |Z_m^a|) \cdot \eta_{m-1}^a(\boldsymbol{d}^*, \boldsymbol{n}^*) \\ &= |Z_m^a| \left(q^{n_1+\cdots+n_{m-1}+m-1} - \eta_{m-1}^a(\boldsymbol{d}^*, \boldsymbol{n}^*)\right) + \eta_{m-1}^a(\boldsymbol{d}^*, \boldsymbol{n}^*) \cdot q^{n_m+1} \\ &\leq \eta_m^a(\boldsymbol{d}, \boldsymbol{n}). \end{aligned}$$

Esto concluye la demostración de la proposición. □

Capítulo 3

Teoremas de Bertini

El objetivo de este capítulo es presentar diferentes versiones efectivas de una familia de enunciados que se conocen bajo el nombre de segundo teorema de Bertini. Nuestro interés en estos teoremas se debe a que ellos constituyen una herramienta fundamental para obtener estimaciones y resultados de existencia de puntos q-racionales. Los teoremas de *tipo Bertini* son aquellos que garantizan la preservación de una cierta propiedad de una variedad afín o proyectiva (por ejemplo, absoluta irreducibilidad, no singularidad, normalidad, etc.) al intersecar dicha variedad con una variedad lineal genérica de cierta dimensión. Siguiendo la terminología de [Sha94], llamamos segundo teorema de Bertini al enunciado que asegura que, si V es una variedad afín o proyectiva no singular, entonces la intersección de V con una variedad lineal genérica es no singular. En esta tesis damos la siguiente variante de este teorema: si $V \subset \mathbb{P}^n$ es una variedad proyectiva de dimensión r y lugar singular de dimensión a lo sumo s, entonces existe una sección lineal genérica de V de codimensión al menos $s+1$ que es no singular (ver [GL02a, Proposition 1.3]). Dichas secciones lineales no singulares se obtienen intersecando a V con una variedad lineal genérica, o considerando la clausura Zariski de un fibra definida sobre $\mathbb{F}_q$ de un morfismo lineal genérico $\Pi : V \dashrightarrow \mathbb{P}^{s+1}$. Este último enfoque es el que se considera en [CM07a], donde los autores obtienen una versión efectiva del segundo teorema de Bertini para intersecciones completas normales. En esta tesis generalizamos este resultado a intersecciones completas V cuyo lugar singular es de dimensión a lo sumo s con $0 \leq s \leq \dim V - 2$ arbitrario. Para esto, estudiamos en detalle la geometría del conjunto de puntos excepcionales S de dicha proyección, el cual, como vamos a ver, identificamos con una cierta variedad polar asociada a V.

3.1. Variedades polares

En esta sección damos una breve introducción a la teoría de variedades polares. La variedad polar es un concepto clásico de la geometría proyectiva, introducido en los años treinta por F. Severi y J. Tood y retomado en el año 1975 por R. Piene [Pie78] y B. Teissier [Tei82, Tei88]. Sea $V \subset \mathbb{P}^n$ una variedad proyectiva equidimensional de dimensión r. Denotamos por $\Sigma \subset V$ al lugar singular de V y por $V_{\mathrm{sm}} := V \setminus \Sigma$ al conjunto de puntos regulares de V. Para cada entero $0 \leq s \leq r-2$

y $x \in V_{\text{sm}}$, consideramos una variedad lineal L_s de dimensión $n-s-2$. Notamos que la dimensión de la intersección $\mathcal{T}_x V \cap L_s$ es al menos $r-s-2$. El conjunto de puntos regulares de V para los cuales la dimensión de dicha intersección es mayor o igual a $r-s-1$ se denomina la s-ésima variedad polar de V con respecto a L_s, que denotamos $\mathsf{M}(L_s)$, es decir,

$$\mathsf{M}(L_s) := \{x \in V_{\text{sm}} \,:\, \dim(\mathcal{T}_x V \cap L_s) \geq r-s-1\}.$$

Ejemplo 3.1.1. *Sea $V \subset \mathbb{P}^3$ una superficie. Sean $L_1 := \{p\}$ y L_0 una recta proyectiva. Entonces $\mathsf{M}(\{p\}) = \{x \in V_{\text{sm}} : p \in \mathcal{T}_x V\}$ y $\mathsf{M}(L_0) = \{x \in V_{\text{sm}} : L_0 \subset \mathcal{T}_x V\}$.*

De ahora en más prescindiremos del subíndice s en L_s. Como mencionamos anteriormente, la variedad polar $\mathsf{M}(L)$ nos permitirá describir el conjunto de puntos de V_{sm} que resultan ser puntos críticos de la proyección lineal asociada a L. Más aún, $\mathsf{M}(L)$ nos permitirá dar una caracterización del conjunto de puntos singulares de $V \cap L$. Para demostrar estas afirmaciones, comenzamos fijando las siguientes notaciones.

Sean $X := (X_0, \ldots, X_n)$ indeterminadas sobre $\overline{\mathbb{F}}_q$ y $\mu := (\mu_0 : \cdots : \mu_n) \in \mathbb{P}^n$. Utilizaremos la notación $\mu \cdot X := \mu_0 X_0 + \cdots + \mu_n X_n$. Sean $\lambda_0, \ldots, \lambda_{s+1} \in \mathbb{P}^n$ puntos linealmente independientes y L la variedad lineal de dimensión $n-s-2$ definida como

$$L := \{x \in \mathbb{P}^n : \lambda_0 \cdot x = \cdots = \lambda_{s+1} \cdot x = 0\}. \tag{3.1}$$

Sea $Y_i := \lambda_i \cdot X$ $(0 \leq i \leq s+1)$ y consideremos el morfismo racional de V en $\mathbb{P}^{s+1}$ definido por $Y_0, \ldots, Y_{s+1}$, es decir

$$\begin{aligned} \pi : V &\dashrightarrow \mathbb{P}^{s+1} \\ x &\mapsto (\lambda_0 \cdot x : \cdots : \lambda_{s+1} \cdot x). \end{aligned} \tag{3.2}$$

Este morfismo está bien definido fuera del conjunto de puntos excepcionales E, es decir el conjunto de puntos $x \in V$ para los cuales $\lambda_0 \cdot x = \cdots = \lambda_{s+1} \cdot x = 0$. En otras palabras, π está bien definido en $V \setminus L$ y $\mathsf{E} = V \cap L$.

Para cada $x \in V_{\text{sm}}$ consideramos el morfismo racional

$$\begin{aligned} \pi_x : T_x V &\dashrightarrow \mathbb{P}^{s+1} \\ v &\mapsto (\lambda_0 \cdot v : \cdots : \lambda_{s+1} \cdot v). \end{aligned} \tag{3.3}$$

El conjunto de puntos excepcionales E_x de π_x es el conjunto de elementos $v \in T_x V$ con $\lambda_0 \cdot v = \cdots = \lambda_{s+1} \cdot v = 0$. Notar que π_x se puede interpretar como la diferencial del morfismo lineal $\Pi : C_V \to \mathbb{A}^{s+2}$ definido por las formas lineales $Y_0, \ldots, Y_{s+1}$, donde $C_V \subset \mathbb{A}^{n+1}$ denota el cono afín de la variedad V.

Lema 3.1.2. *Sea $V \subset \mathbb{P}^n$ una variedad equidimensional de dimensión r y sea Σ el lugar singular de V. Sea $L \subset \mathbb{P}^n$ la variedad lineal de dimensión $n-s-2$ definida en (3.1) y sean π y π_x definidos como en (3.2) y (3.3). Son válidas las siguientes afirmaciones:*

i) La variedad polar $\mathsf{M}(L)$ coincide con el conjunto de puntos $x \in V_{\text{sm}}$ tales que la dimensión de E_x es al menos $r-s-1$.

ii) $\operatorname{Sing}(V \cap L) = (\Sigma \cap L) \cup (\mathsf{M}(L) \cap L)$, *donde* $\operatorname{Sing}(V \cap L)$ *denota el lugar singular de* $V \cap L$.

Demostración. Probamos la primera afirmación. Por definición, dado $x \in V_{\mathrm{sm}}$, el conjunto de puntos excepcionales E_x de π_x es el conjunto de puntos $v \in \mathcal{T}_x V$ tales que $\lambda_0 \cdot v = \cdots = \lambda_{s+1} \cdot v = 0$, es decir, $\mathsf{E}_x = \mathcal{T}_x V \cap L$. En consecuencia, se tiene que $\dim \mathsf{E}_x \geq r - s - 1$ si y solo si $\dim(\mathcal{T}_x V \cap L) \geq r - s - 1$ para todo $x \in V_{\mathrm{sm}}$. Por lo tanto, podemos caracterizar a la variedad polar $\mathsf{M}(L)$ como el conjunto de puntos $x \in V_{\mathrm{sm}}$ para los cuales $\dim \mathsf{E}_x \geq r - s - 1$.

Demostramos a continuación la segunda afirmación del lema. Por [GL02a, Lemma 1.1.], se tiene que

$$\begin{aligned} \operatorname{Sing}(V \cap L) &= (V \cap \operatorname{Sing} L) \cup (\Sigma \cap L) \cup N(V, L) \\ &= (\Sigma \cap L) \cup N(V, L), \end{aligned} \tag{3.4}$$

donde $N(V, L)$ es el conjunto de puntos $x \in V_{\mathrm{sm}}$ para los cuales V y L no se cortan transversalmente, es decir $\dim \mathcal{T}_x V \cap L > \dim \mathcal{T}_x V - \operatorname{codim} L = r - s - 2$. Luego, por la definición de variedad polar se sigue que $N(V, L) = \mathsf{M}(L)$, lo que concluye la demostración del lema. □

Nos interesa estudiar la dimensión de una variedad polar dada. Es bien sabido que $\mathsf{M}(L)$ es vacía o es equidimensional de dimensión al menos s. Asimismo, si L es una variedad lineal génerica, de dimensión $n - s - 2$ entonces la variedad polar tiene dimensión s (ver [Pie78, Transversality Lemma 1.3]). Por completitud, damos a continuación una prueba de este resultado, en base a [Kle77, Chapter 4, §B].

Proposición 3.1.3. *Para una variedad lineal genérica* L *de dimensión* $n - s - 2$, *la variedad polar* $\mathsf{M}(L)$ *tiene dimensión* s.

Demostración. Sea $\mathbb{G}(r, n)$ la grassmaniana de los espacios lineales de dimensión r en $\mathbb{P}^n$. Consideramos el morfismo de Gauss $\mathcal{G} : V_{\mathrm{sm}} \to \mathbb{G}(r, n)$ que a cada x le asigna el espacio tangente $\mathcal{T}_x V$ y sea $S \subset \mathbb{G}(r, n)$ la siguiente variedad de Schubert

$$S := \{\Lambda \in \mathbb{G}(r, n) : \dim(\Lambda \cap L) \geq r - s - 1\}.$$

Observemos que S tiene dimensión $\dim \mathbb{G}(r, n) - (r - s)$ (ver, por ejemplo, [Har92, Example 11.42]). Por otro lado, es fácil ver que $\mathsf{M}(L) = \mathcal{G}^{-1}(S \cap \mathcal{G}(V_{\mathrm{sm}}))$. Consideramos la inclusión $i : S \hookrightarrow \mathbb{G}(r, n)$. Afirmamos que la variedad polar $\mathsf{M}(L)$ coincide con el producto fibrado $V_{\mathrm{sm}} \times_{\mathbb{G}(r,n)} S$. En efecto,

$$\begin{aligned} V_{\mathrm{sm}} \times_{\mathbb{G}(r,n)} S &:= \{(x, \Lambda) \in V_{\mathrm{sm}} \times S : \mathcal{T}_x V = \Lambda\} \\ &= \{x \in V_{\mathrm{sm}} : \dim(\mathcal{T}_x V \cap L) \geq r - s - 1\} = \mathsf{M}(L). \end{aligned}$$

$GL(n)$ actúa transitivamente sobre $\mathbb{G}(r, n)$; más aún, S está en posición general con respecto a esta acción, pues L lo está por hipótesis. Así, de acuerdo a [Kle74, Theorem 2(i)], concluimos que $\mathsf{M}(L)$ es equidimensional de dimensión

$$\dim \mathsf{M}(L) = \dim V_{\mathrm{sm}} + \dim S - \dim \mathbb{G}(r, n) = s. \qquad \square$$

3.1.1. Variedades polares de intersecciones completas

En esta sección vamos a considerar variedades polares asociadas a intersecciones completas. Vamos a probar que, en este caso, podemos obtener ecuaciones que definan a la variedad polar $\mathsf{M}(L)$. Más precisamente, la variedad polar $\mathsf{M}(L)$ se puede definir como el conjunto de ceros comunes de ciertos menores maximales que involucran a las derivadas parciales de los polinomios que definen a V y a L. De esta forma se obtiene un sistema de ecuaciones polinomiales explícito para $\mathsf{M}(L)$. En los trabajos [BGHM97, BGHM01, BGHP05, BGH$^+$10, BGH$^+$12] las variedades polares se describen localmente por sucesiones regulares formadas por los polinomios que definen a V y ciertos menores maximales de sus jacobianos.

En lo que sigue V denotará una intersección completa en $\mathbb{P}^n$ de dimensión r, definida por polinomios homogéneos $F_1, \ldots, F_{n-r} \in \mathbb{F}_q[X_0, \ldots, X_n]$ de grados $d_1 \geq d_2 \geq \cdots \geq d_{n-r} \geq 2$ respectivamente y grado $\delta := \deg V = d_1 \cdots d_{n-r}$. Notamos por Σ el conjunto de puntos singulares de V y supongamos que existe $0 \leq s \leq r-2$ tal que $\dim \Sigma \leq s$. En particular, V es normal y por el Teorema 2.1.4 es absolutamente irreducible. Sea también $D := \sum_{i=1}^{n-r}(d_i - 1)$.

Dado $x \in V$, como $F_1, \ldots, F_{n-r}$ definen el ideal de V, el espacio tangente $\mathcal{T}_x V$ de V en x es la siguiente variedad lineal:

$$\mathcal{T}_x V = \big\{v \in \mathbb{P}^n : \nabla F_1(x) \cdot v = \cdots = \nabla F_{n-r}(x) \cdot v = 0\big\}. \tag{3.5}$$

Dado $x \in V_{\mathrm{sm}}$, los gradientes $\nabla F_1(x), \ldots, \nabla F_{n-r}(x)$ son linealmente independientes y por lo tanto $\dim \mathcal{T}_x V = r$.

Sea $0 \leq s \leq r-2$, sean $\lambda_i := (\lambda_{i,0}, \ldots, \lambda_{i,n})$ con $0 \leq i \leq s+1$ y $\boldsymbol{\lambda} := (\lambda_0, \ldots, \lambda_{s+1})$. Consideramos la variedad lineal L de dimensión $n-s-2$ definida como en (3.1). Sea la matriz de tamaño $(n-(r-s-2)) \times (n+1)$

$$\mathsf{M}(X, \boldsymbol{\lambda}) := \begin{pmatrix} \frac{\partial F_1}{\partial X_0} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_{n-r}}{\partial X_0} & \cdots & \frac{\partial F_{n-r}}{\partial X_n} \\ \lambda_{0,0} & \cdots & \lambda_{0,n} \\ \vdots & & \vdots \\ \lambda_{s+1,0} & \cdots & \lambda_{s+1,n} \end{pmatrix}. \tag{3.6}$$

Dado $x \in V_{\mathrm{sm}}$, la dimensión de $\mathcal{T}_x V \cap L$ es $r-s-2$ si y sólo si $\mathsf{M}(X, \boldsymbol{\lambda})$ tiene rango máximo. Equivalentemente, $\mathsf{M}(X, \boldsymbol{\lambda})$ no tiene rango máximo si y sólo si la dimensión de $\mathcal{T}_x V \cap L$ es al menos $r-s-1$. Si notamos $\Delta_1(X, \boldsymbol{\lambda}), \ldots, \Delta_N(X, \boldsymbol{\lambda})$ los menores maximales de $\mathsf{M}(X, \boldsymbol{\lambda})$, tenemos entonces que la variedad polar $\mathsf{M}(L)$ está dada por

$$\mathsf{M}(L) = \{x \in V_{\mathrm{sm}} : \Delta_1(x, \boldsymbol{\lambda}) = \cdots = \Delta_N(x, \boldsymbol{\lambda}) = 0\}.$$

De acuerdo a la Proposición 3.1.3, para una elección genérica de L la dimensión de $\mathsf{M}(L)$ es igual a s. Nuestro objetivo es obtener condiciones sobre $\boldsymbol{\lambda} := (\lambda_0, \ldots, \lambda_{s+1}) \in (\mathbb{P}^n)^{s+2}$ que impliquen que la variedad polar $\mathsf{M}(L)$ tiene dimensión

s. Para $0 \leq i \leq s+1$, denotamos por $\Lambda_i := (\Lambda_{i,0}, \ldots, \Lambda_{i,n})$ a un grupo de $n+1$ variables y sea $\mathbf{\Lambda} := (\Lambda_0, \ldots, \Lambda_{s+1})$. Consideramos la variedad polar "genérica"

$$W := (V_{\mathrm{sm}} \times \mathcal{U}) \cap \{\Delta_1(X, \mathbf{\Lambda}) = \cdots = \Delta_N(X, \mathbf{\Lambda}) = 0\}, \tag{3.7}$$

donde $\mathcal{U} \subset (\mathbb{P}^n)^{s+2}$ es el abierto Zariski formado por las matrices de tamaño $(s+2)\times(n+1)$ que tienen rango máximo, luego es una variedad irreducible de dimensión $n \cdot (s+2)$, y $\Delta_1, \ldots, \Delta_N$ son los menores maximales de la versión genérica $\mathsf{M}(X, \mathbf{\Lambda})$ de la matriz $\mathsf{M}(X, \boldsymbol{\lambda})$ definida en (3.6).

Proposición 3.1.4. *Sea $t := n(s+2)$. Entonces W es una variedad irreducible de $\mathbb{P}^n \times \mathcal{U}$ de dimensión $s+t$.*

Demostración. Sea $\Pi_1 : W \to V_{\mathrm{sm}}$ la proyección lineal $\Pi_1(x, \boldsymbol{\lambda}) := x$. Fijamos $x \in V_{\mathrm{sm}}$ y consideramos la fibra $\Pi_1^{-1}(x)$. Se tiene que $\Pi_1^{-1}(x) = \{x\} \times \mathcal{L}$, donde $\mathcal{L} \subset \mathcal{U}$ denota el conjunto de matrices $\boldsymbol{\lambda} := (\lambda_0, \ldots, \lambda_{s+1})$ para las cuales la matriz $\mathsf{M}(X, \boldsymbol{\lambda})$ no tiene rango máximo. Esto es lo mismo que decir que

$$\langle \lambda_0, \ldots, \lambda_{s+1} \rangle \cap \big\langle \nabla F_1(x), \ldots, \nabla F_{n-r}(x) \big\rangle \neq \emptyset,$$

donde $\langle v_0, \ldots, v_m \rangle \subset \mathbb{A}^{n+1}$ es la variedad lineal generada por $v_0, \ldots, v_m$ en $\mathbb{A}^{n+1}$. Equivalentemente, los vectores $\lambda_0, \ldots, \lambda_{s+1}$ son linealmente dependientes en el $\overline{\mathbb{F}}_q$-espacio vectorial cociente, de dimensión $r+1$ porque x es un punto regular de V

$$\mathbb{V} := \mathbb{A}^{n+1} / \big(\nabla F_1(x), \ldots, \nabla F_{n-r}(x)\big).$$

El cono afín $(\mathbb{A}^{n+1})^{s+2}$ de $(\mathbb{P}^n)^{s+2}$ se puede identificar con el $\overline{\mathbb{F}}_q$-espacio vectorial $\mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1})$ de los morfismos lineales de $\mathbb{A}^{s+2}$ en $\mathbb{A}^{n+1}$. En particular, el abierto Zariski $\mathcal{U}_{\mathrm{aff}} \subset (\mathbb{A}^{n+1})^{s+2}$ de las matrices de rango completo es el cono afín de $\mathcal{U} \subset (\mathbb{P}^n)^{s+2}$ y podemos identificarlo con el siguiente subconjunto abierto de los morfismos lineales de rango completo de $\mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1})$:

$$L^{=}_{s+2}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1}) := \{f \in \mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1}) : \mathrm{rg}(f) = s+2\}.$$

La proyección al cociente $\mathbb{A}^{n+1} \to \mathbb{V}$ induce el siguiente morfismo lineal suryectivo:

$$\Phi : \mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1}) \to \mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{V}).$$

Notamos como $\Phi(\mathcal{U}_{\mathrm{aff}})$ a la imagen de $L^{=}_{s+2}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1})$ vía Φ. Por lo tanto, el cono afín $C(\mathcal{L})$ de $\mathcal{L}$, es, módulo $\big(\nabla F_1(x), \ldots, \nabla F_{n-r}(x)\big)$, isomorfo al abierto Zariski $L_{s+1}(\mathbb{A}^{s+2}, \mathbb{V}) \cap \Phi(\mathcal{U}_{\mathrm{aff}})$, donde

$$L_{s+1}(\mathbb{A}^{s+2}, \mathbb{V}) := \{f \in \mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{V}) : \mathrm{rg}(f) \leq s+1\}.$$

Teniendo en cuenta [BV88, Proposición 1.1], $L_{s+1}(\mathbb{A}^{s+2}, \mathbb{V})$ es una variedad irreducible de dimensión $(s+1)(r+2)$. Luego, como estamos considerando subespacios de $\mathbb{A}^{n+1}$ de dimensión $s+2$ módulo el subespacio $\big(\nabla F_1(x), \ldots, \nabla F_{n-r}(x)\big)$, cuya dimensión es $n-r$ porque x es un punto regular de V, vemos que el cono afín de $C(\mathcal{L})$ es una

variedad irreducible de dimensión $(s+1)(r+2)+(n-r)(s+2) = (n+1)(s+2)+s-r$. Por lo tanto, $\mathcal{L}$ es una variedad irreducible de dimensión $\dim C(\mathcal{L})-(s+2) = t+s-r$. Así, hemos probado que $\Pi_1^{-1}(x) = \{x\} \times \mathcal{L}$ es una variedad irreducible contenida en $(\mathbb{P}^n)^{s+2}$ de dimensión $t+s-r$ y además $\Pi_1 : W \to V_{\text{sm}}$ es suryectiva. En particular todas las fibras tienen la misma dimensión.

Finalmente, probamos que W es irreducible. Consideremos la proyección $V \times \mathcal{U} \to V$ y veamos que es cerrada. Alcanza con probar que $\mathcal{U}$ es un espacio completo. Sea $\mathbb{G}(n, s+2)$ la grassmanniana de las variedades lineales en $\mathbb{P}^n$ de dimensión $s+2$. Se tiene que $\mathbb{G}(n, s+2)$ es un espacio completo por ser una variedad proyectiva y, como $\mathcal{U}$ es la preimagen de $\mathbb{G}(n, s+2)$ por un morfismo propio, el que definen las coordenadas de Plucker, $\mathcal{U}$ resulta completo (ver, por ejemplo, [Mil80, Proposition 8.24]). Luego la restricción $V_{\text{sm}} \times \mathcal{U} \to V_{\text{sm}}$ es también cerrada. Sea $W = \bigcup_{j=1}^{t} \mathcal{C}_j$ la descomposición de W en componentes irreducibles. De la suryectividad de Π_1 se deduce que $\Pi_1(W) = V_{\text{sm}} = \bigcup_j \Pi_1(\mathcal{C}_j)$, donde cada $\Pi_1(\mathcal{C}_j)$ es un subconjunto cerrado de V_{sm}. Como V es una intersección completa normal, y por lo tanto irreducible (ver el Teorema 2.1.4), entonces V_{sm} es irreducible y existe j tal que $\Pi_1(\mathcal{C}_j) = V_{\text{sm}}$.

Sea I_1 el conjunto de los índices $j \in \{1, \ldots, t\}$ tales que $\Pi_1(\mathcal{C}_j) = V_{\text{sm}}$. Para cada $j \in I_1$, la restricción $\Pi_{1,j}$ de Π_1 a $\mathcal{C}_j$ es suryectiva y, por [Sha94, §I.6.3, Theorem 7 (ii)], existe un abierto $U_j \subset V_{\text{sm}}$ tal que para todo $y \in U_j$, $\dim \Pi_{1,j}^{-1}(y) = \dim(\mathcal{C}_j) - \dim(V_{\text{sm}}) = \dim(\mathcal{C}_j) - r$. Por otro lado consideremos el conjunto I_2 de los índices $j \in \{1, \ldots, t\}$ tales que $\Pi_1(\mathcal{C}_j) \subsetneq V_{\text{sm}}$. Para cada $j \in I_2$ definimos el abierto $U_j := V_{\text{sm}} \setminus \Pi_1(\mathcal{C}_j)$. Sea $y \in \bigcap_{j=1}^{t} U_j$. Como $\Pi_1^{-1}(y)$ es irreducible, se tiene que $\Pi_1^{-1}(y) \subset \mathcal{C}_{j_0}$ para cierto j_0. Entonces $\Pi_1^{-1}(y) \subset \Pi_{1,j_0}^{-1}(y)$, y como la inclusión inversa es trivial, deducimos que $\Pi_1^{-1}(y) = \Pi_{1,j_0}^{-1}(y)$ y $\dim(\mathcal{C}_{j_0}) - r = m$, donde $m := t+s-r$ es la dimensión de cada una de las fibras de Π_1. Por la suryectividad de Π_{1,j_0} se tiene que $\Pi_{1,j_0}^{-1}(y) \subset \Pi_1^{-1}(y)$ es no vacía para todo $y \in V_{\text{sm}}$. Por [Sha94, §I.6.3, Theorem 7 (i)], $\dim \Pi_{1,j_0}^{-1}(y) \geq \dim(\mathcal{C}_{j_0}) - r = m$. Deducimos entonces que, para todo $y \in V_{\text{sm}}$, resulta $\Pi_1^{-1}(y) = \Pi_{1,j_0}^{-1}(y)$. Por lo tanto, $W = \mathcal{C}_{j_0}$ es una subvariedad irreducible de $V_{\text{sm}} \times \mathcal{U}$.

Finalmente, por el Teorema de la dimensión de las fibras (ver, por ejemplo, [Sha94, §I.6.3, Theorem 7]), para cada $x \in V_{\text{sm}}$ se tiene

$$t+s-r = \dim \Pi_1^{-1}(x) = \dim W - \dim V_{\text{sm}} = \dim W - r.$$

Esto muestra que la dimensión de W es $t+s$ y concluye la demostración de la proposición. □

Consideramos la proyección $\Pi_2 : W \to (\mathbb{P}^n)^{s+2}$ dada por $\Pi_2(x, \boldsymbol{\lambda}) := \boldsymbol{\lambda}$, donde $W \subset V_{\text{sm}} \times \mathcal{U}$ es la variedad polar genérica definida en (3.7). Dado $\boldsymbol{\lambda} \in \mathcal{U}$ se tiene que $\Pi_2^{-1}(\boldsymbol{\lambda}) = \mathsf{M}(L)$. De acuerdo a la Proposición 3.1.3, para un punto $\boldsymbol{\lambda} \in \mathcal{U}$ genérico, la variedad polar $\mathsf{M}(L)$ tiene dimensión s. Luego la dimensión de la fibra genérica de Π_2 es $s \geq 0$, lo que implica que Π_2 es un morfismo dominante. Por otro lado, por la Proposición 3.1.4 la variedad polar genérica W es irreducible de dimensión $t+s$, donde $t := n(s+2)$. Luego, por el Teorema de la dimensión de las fibras (ver, por ejemplo, [Sha94, §I.6.3, Theorem 7]), dado $\boldsymbol{\lambda} \in \Pi_2(W)$, para cada componente

irreducible $\mathcal{C}$ de la fibra $\Pi_2^{-1}(\boldsymbol{\lambda})$, se tiene

$$\dim \mathcal{C} \geq \dim W - \dim \mathcal{U} = t + s - t = s.$$

Más aún, existe un abierto Zariski de $\mathcal{U}$ donde vale la igualdad.

El resultado principal de esta sección afirma que existe un conjunto cerrado de $(\mathbb{P}^n)^{s+2}$ de grado "bajo" que contiene las fibras de Π_2 de dimensión mayor a s. Con el objetivo de demostrar la existencia de este cerrado, damos el siguiente lema técnico.

Lema 3.1.5. *Sea $\mathcal{W} \subset \mathbb{P}^{\boldsymbol{n}}$ una variedad multiproyectiva equidimensional de dimensión e y sea $\mathcal{W}_1 \subset \mathbb{P}^{\boldsymbol{n}}$ una subvariedad de $\mathcal{W}$ de dimensión a lo sumo $e_1 < e$. Supongamos que existen polinomios multihomogéneos $H_1, \ldots, H_M \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ de multigrado $\boldsymbol{e}$ tales que*

$$\mathcal{W} \cap \{H_1 = \cdots = H_M = 0\} = \mathcal{W}_1. \tag{3.8}$$

Entonces existen combinaciones lineales $H^1, \ldots, H^{e-e_1}$ de $H_1, \ldots, H_M$ tales que la variedad $\mathcal{W} \cap \{H^1 = \cdots = H^{e-e_1} = 0\}$ contiene a $\mathcal{W}_1$ y es equidimensional de dimensión e_1.

Demostración. Mostramos por inducción que para $1 \leq i \leq e - e_1$ existen combinaciones lineales $H^1, \ldots, H^i$ de $H_1, \ldots, H_M$ tales que $\mathcal{W} \cap \{H^1 = \cdots = H^i = 0\}$ contiene a $\mathcal{W}_1$ y es equidimensional de dimensión $e-i$. El caso $i = e-e_1$ corresponde a la afirmación del lema.

Comenzamos con $i = 1$. Sea $\mathcal{W}^0 := \mathcal{W}$ y sea $\mathcal{W}^0 = \bigcup_{j=1}^t \mathcal{C}_{0,j}$ la descomposición de $\mathcal{W}^0$ en componentes irreducibles. Observemos que $\dim \mathcal{C}_{0,j} = e$ para $1 \leq j \leq t$. Como $\dim(\mathcal{W}_1) \leq e_1 < e$, existe $\boldsymbol{x}_{0,j} \in \mathcal{C}_{0,j} \setminus \mathcal{W}_1$ para cada $1 \leq j \leq t$.

Sea $\Gamma := (\Gamma_1, \ldots, \Gamma_M)$ un vector de indeterminadas en $\overline{\mathbb{F}}_q$ y sea $\mathcal{H}_1 \in \mathbb{F}_q[\Gamma]$ el siguiente polinomio:

$$\mathcal{H}_1 := \prod_{j=1}^{t} \big(\Gamma_1 H_1(\boldsymbol{x}_{0,j}) + \cdots + \Gamma_M H_M(\boldsymbol{x}_{0,j})\big).$$

Como $\boldsymbol{x}_{0,j} \in \mathcal{W}^0 \setminus \mathcal{W}_1$ para $1 \leq j \leq t$, por (3.8) vemos que para cada j existe H_{i_j} con $H_{i_j}(\boldsymbol{x}_{0,j}) \neq 0$. Esto muestra que $\mathcal{H}_1$ es un polinomio no nulo y, por lo tanto, existe $\gamma_1 := (\gamma_{1,1}, \ldots, \gamma_{1,M}) \in \overline{\mathbb{F}}_q^M$ tal que $\mathcal{H}_1(\gamma_1) \neq 0$. En particular, el polinomio homogéneo $H^1 := \sum_{k=1}^M \gamma_{1,k} H_k \in \overline{\mathbb{F}}_q[\boldsymbol{X}]$ tiene multigrado $\boldsymbol{e}$ y no se anula en $\boldsymbol{x}_{0,j}$ para $1 \leq j \leq t$. Luego, la variedad multiproyectiva $\mathcal{C}_{0,j} \cap \{H^1 = 0\}$ es equidimensional de dimensión $e-1$ para $1 \leq j \leq t$. Esto implica que $\mathcal{W}^1 := \mathcal{W}^0 \cap \{H^1 = 0\}$ es una subvariedad de $\mathcal{W}^0$ equidimensional de dimensión $e-1$. Por (3.8) se tiene que H^1 es idénticamente cero en $\mathcal{W}_1$, y por lo tanto $\mathcal{W}_1 \subset \mathcal{W}^1$. Así finalizamos la demostración de la primera parte de nuestro argumento inductivo.

Sea i con $1 < i \leq e - e_1$ y supongamos que existen combinaciones lineales $H^1, \ldots, H^{i-1}$ de $H_1, \ldots, H_M$ tales que la variedad $\mathcal{W}^{i-1} := \mathcal{W} \cap \{H^1 = \cdots = H^{i-1} = 0\}$ es equidimensional de dimensión $e-i+1$ con $\mathcal{W}_1 \subset \mathcal{W}^{i-1}$. Sea $\mathcal{W}^{i-1} = \bigcup_{j=1}^{t'} \mathcal{C}_{i-1,j}$ la descomposición de $\mathcal{W}^{i-1}$ en componentes irreducibles. Se tiene que $\dim \mathcal{C}_{i-1,j} = e-i+1 > e_1+1 \geq \dim \mathcal{W}_1$ para $1 \leq j \leq t'$. Haciendo el mismo razonamiento que en el

primer paso del argumento inductivo, concluimos que existen combinaciones lineales $H^1, \ldots, H^i$ de $H_1, \ldots, H_M$ tales que la variedad $\mathcal{W}^i := \mathcal{W} \cap \{H^1 = \cdots = H^i = 0\}$ es equidimensional de dimensión $e-i$ con $\mathcal{W}_1 \subset \mathcal{W}^i$. Esto concluye la demostración del lema. □

En lo que sigue, a cada punto $\boldsymbol{\lambda} := (\lambda_0, \ldots, \lambda_{s+1}) \in (\mathbb{P}^n)^{s+2}$ le asociamos la variedad lineal $L := \{x \in \mathbb{P}^n : \lambda_0 \cdot x = \cdots = \lambda_{s+1} \cdot x = 0\}$.

A continuación, vamos a probar la existencia de una hipersuperficie multiproyectiva $\mathcal{H}_1 \subset (\mathbb{P}^n)^{s+2}$ que contiene a los $\boldsymbol{\lambda}$ para los cuales la dimensión de la variedad polar es mayor a s.

Teorema 3.1.6. *Existe una hipersuperficie $\mathcal{H}_1 \subset (\mathbb{P}^n)^{s+2}$, definida por un polinomio multihomogéneo de grado a lo sumo $(n-s)(r-s)D^{r-s-1}\delta + 1$ en cada grupo de variables Λ_i, donde $D = \sum_{i=1}^{n-r}(d_i - 1)$ y δ es el grado de V, tal que para cada $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}_1$ la variedad polar $\mathsf{M}(L)$ de V tiene dimensión a lo sumo s.*

Demostración. Como Π_2 es un morfismo dominante, entonces la extensión de cuerpos $\overline{\mathbb{F}}_q(\boldsymbol{\Lambda}) \hookrightarrow \overline{\mathbb{F}}_q(W)$ tiene grado de trascendencia $s+1$, lo cual implica que existen índices $i_0, \ldots, i_s$ tales que las funciones coordenadas de $\overline{\mathbb{F}}_q(W)$ definidas por $X_{i_0}, \ldots, X_{i_s}$ forman una base de trascendencia de esta extensión.

Fijemos $i \in \Gamma := \{0, \ldots, n\} \setminus \{i_0, \ldots, i_s\}$ y consideremos la aplicación lineal $\pi_i : W \dashrightarrow \mathbb{P}^{s+1} \times (\mathbb{P}^n)^{s+2}$ definida por $X_{i_0}, \ldots, X_{i_s}, X_i$ y $\boldsymbol{\Lambda}$, es decir, $\pi_i(x, \boldsymbol{\lambda}) = (x_{i_0} : \cdots : x_{i_s} : x_i, \boldsymbol{\lambda})$.

Afirmación. *Sea $W_i := \overline{\pi_i(W)} \subset \mathbb{P}^{s+1} \times (\mathbb{P}^n)^{s+2}$ la clausura Zariski de $\pi_i(W)$. Se tiene que W_i es una $\mathbb{F}_q$-hipersuperficie.*

Demostración. Como las funciones coordenadas de $\overline{\mathbb{F}}_q(W)$ definidas por $X_{i_0}, \ldots, X_{i_s}$ forman una base de trascendencia de la extensión $\overline{\mathbb{F}}_q(\boldsymbol{\Lambda}) \hookrightarrow \overline{\mathbb{F}}_q(W)$, la extensión $\overline{\mathbb{F}}_q(X_{i_0}, \ldots, X_{i_s}, \boldsymbol{\Lambda}) \hookrightarrow \overline{\mathbb{F}}_q(W)$ es algebraica y, por lo tanto, para cada $i \in \Gamma$ existe un polinomio $m_i \in \overline{\mathbb{F}}_q[X_{i_0}, \ldots, X_{i_s}, \boldsymbol{\Lambda}, T]$ de grado mínimo $D_i > 0$ en T, que es primitivo como elemento de $\overline{\mathbb{F}}_q[X_{i_0}, \ldots, X_{i_s}, \boldsymbol{\Lambda}][T]$, tal que se anula en la función coordenada definida por X_i en $\overline{\mathbb{F}}_q(W)$. Sea $A_i \in \overline{\mathbb{F}}_q[X_{i_0}, \ldots, X_{i_s}, \boldsymbol{\Lambda}]$ el polinomio no nulo que es el coeficiente de T^{D_i} en m_i, considerando a m_i como un elemento de $\overline{\mathbb{F}}_q[X_{i_0}, \ldots, X_{i_s}, \boldsymbol{\Lambda}][T]$. Sea finalmente $A_\Gamma := X_{i_0} \prod_{i \in \Gamma} A_i$. Como $A_\Gamma \in \overline{\mathbb{F}}_q[X_{i_0}, \ldots, X_{i_s}, \boldsymbol{\Lambda}]$ y las funciones coordenadas definidas por $X_{i_0}, \ldots, X_{i_s}$ forman una base de trascendencia de la extensión $\overline{\mathbb{F}}_q(\boldsymbol{\Lambda}) \hookrightarrow \overline{\mathbb{F}}_q(W)$, entonces A_Γ no se anula idénticamente en W. Como además W es irreducible, concluimos que $W \cap \{A_\Gamma \neq 0\}$ es un abierto Zariski denso y no vacío de W.

Fijemos $(x, \boldsymbol{\lambda}) \in W \cap \{A_\Gamma \neq 0\}$. Entonces, $\pi_i(x, \boldsymbol{\lambda})$ está bien definida y su fibra tiene dimensión cero pues para cada $j \in \Gamma$ y para cada $(\widetilde{x}, \lambda) \in \pi_i^{-1}\big(\pi_i(x, \boldsymbol{\lambda})\big)$, la coordenada j de $\widetilde{x}$ se anula en el polinomio $m_j(X_{i_0}, \ldots, X_{i_s}, \boldsymbol{\lambda}, X_j)$. Por el Teorema de la dimensión de las fibras aplicado al morfismo regular $\pi_i : W \setminus \mathsf{E}_{\pi_i} \to \mathbb{P}^{s+1} \times (\mathbb{P}^n)^{s+2}$, donde E_{π_i} es el conjunto de puntos expcecionales de π_i, se tiene

$$0 = \dim \pi_i^{-1}\big(\pi_i(x, \boldsymbol{\lambda})\big) \geq \dim W - \dim \pi_i(W).$$

Por lo tanto, $\dim \pi_i(W) \geq \dim W$, de donde concluimos que $\dim \pi_i(W) = \dim W = t + s = n(s+2) + s$. Como $\pi_i(W)$ es irreducible, su clausura Zariski W_i también lo es, y por lo tanto, W_i es una hipersuperficie. Esto concluye la demostración de la afirmación. □

Nuestro próximo objetivo es encontrar una cota superior para el multigrado de la hipersuperficie W_i. Observemos que $F_1, \ldots, F_{n-r}$ definen la subvariedad $V \times (\mathbb{P}^n)^{s+2}$ de $(\mathbb{P}^n)^{s+3}$ equidimensional de dimensión $t + r$. Más aún, por la definición de W en (3.7), se tiene que

$$W \subset (V \times (\mathbb{P}^n)^{s+2}) \cap \{\Delta_1 = \cdots = \Delta_N = 0\},$$

donde $\Delta_1, \ldots, \Delta_N$ son los menores maximales de la versión genérica de la matriz $\mathsf{M}(X, \mathbf{\Lambda})$ de (3.6). La Proposición 3.1.4 afirma que W es una subvariedad de codimensión $r - s$ de $V \times (\mathbb{P}^n)^{s+2}$. Luego, es de esperar que existan $r - s$ combinaciones lineales genéricas de $\Delta_1, \ldots, \Delta_N$ cuya intersección con $V \times (\mathbb{P}^n)^{s+2}$ definan una variedad equidimensional de dimensión $t + s$ que contiene a W. Probamos esto a continuación.

Afirmación. *Existen combinaciones lineales genéricas $\Delta^1, \ldots, \Delta^{r-s}$ de $\Delta_1, \ldots, \Delta_N$ tales que $F_1, \ldots, F_{n-r}, \Delta^1, \ldots, \Delta^{r-s}$ definen una subvariedad W' de $(\mathbb{P}^n)^{s+3}$ equidimensional de dimensión $t + s$ que contiene a W.*

Demostración. Observemos que $\Sigma \times (\mathbb{P}^n)^{s+2}$ tiene dimensión a lo sumo $t + s$. Por otro lado, recordemos que el cono afín de $\mathcal{U} \subset (\mathbb{P}^n)^{s+2}$ representa el abierto Zariski de todas las matrices de tamaño $(s+2) \times (n+1)$ con entradas en $\overline{\mathbb{F}}_q$ que tienen rango completo. El cono afín de $(\mathbb{P}^n)^{s+2} \setminus \mathcal{U}$ resulta entonces el cerrado cuyos elementos son las matrices de rango a lo sumo $s + 1$, es decir, $L_{s+1}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1})$. Por [BV88, Proposition 1.1], $L_{s+1}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1})$ es una subvariedad irreducible de $(\mathbb{A}^{n+1})^{s+2}$ de dimensión $(s + 1)(n + 2) = t - n + s + s + 2$. Por lo tanto, $(\mathbb{P}^n)^{s+2} \setminus \mathcal{U}$ es una variedad multiproyectiva de dimensión $t - n + s$ y $V \times ((\mathbb{P}^n)^{s+2} \setminus \mathcal{U})$ es una variedad de dimensión $t + r - n + s < t + s$. Concluimos que

$$W'' := W \cup (\Sigma \times (\mathbb{P}^n)^{s+2}) \cup \big(V \times ((\mathbb{P}^n)^{s+2} \setminus \mathcal{U})\big) \tag{3.9}$$

tiene dimensión $t + s$.

Ahora, para un punto arbitrario $(x, \boldsymbol{\lambda}) \in V \times (\mathbb{P}^n)^{s+2}$ se tienen las siguientes tres posibilidades: $x \in \Sigma$, $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{U}$, o $(x, \boldsymbol{\lambda}) \in V_{\mathrm{sm}} \times \mathcal{U}$. En los dos primeros casos, $(x, \boldsymbol{\lambda}) \in W''$ y la igualdad $\Delta_j(x, \boldsymbol{\lambda}) = 0$ se satisface para $1 \leq j \leq N$. En el último caso se tiene que $(x, \boldsymbol{\lambda}) \in W''$ si y sólo si $\Delta_j(x, \boldsymbol{\lambda}) = 0$ para $1 \leq j \leq N$. En consecuencia, vemos que

$$W'' = (V \times (\mathbb{P}^n)^{s+2}) \cap \{\Delta_1 = \cdots = \Delta_N = 0\}, \tag{3.10}$$

y, por lo tanto, W'' es una variedad de $(\mathbb{P}^n)^{s+3}$ de dimensión $t + s$.

Ahora aplicamos el Lema 3.1.5 a las variedades $\mathcal{W} := V \times (\mathbb{P}^n)^{s+2}$ y $\mathcal{W}_1 := W''$. Como W'' tiene codimensión $r - s$ en $V \times (\mathbb{P}^n)^{s+2}$, por el Lema 3.1.5 concluimos

que existen combinaciones lineales $\Delta^1, \dots, \Delta^{r-s}$ de $\Delta_1, \dots, \Delta_N$ tales que la variedad multiproyectiva $W' := (V \times (\mathbb{P}^n)^{s+2}) \cap \{\Delta^1 = \cdots = \Delta^{r-s} = 0\}$ es equidimensional de dimensión $t+s$ y contiene a W'' y, por lo tanto, a W. Esto concluye la demostración de la afirmación. □

Definimos W_i' como la unión de las componentes irreducibles de la subvariedad $W' := \{F_1 = \cdots = F_{n-r} = 0, \Delta^1 = \cdots = \Delta^{r-s} = 0\}$, tales que la clausura Zariski de su imagen por π_i es una hipersuperficie de $\mathbb{P}^{s+1} \times (\mathbb{P}^n)^{s+2}$. Como $\overline{\pi_i(W)}$ tiene codimensión 1 y $W \subset W'$, dicha unión es no vacía. Por lo tanto, $\overline{\pi_i(W_i')}$ es una hipersuperficie $\mathbb{P}^{s+1} \times (\mathbb{P}^n)^{s+2}$ que contiene a W_i.

Vamos a estimar el multigrado de W_i', y por lo tanto, el de W_i. Para ello, consideramos la clase $[W']$ de W' en el anillo de Chow $\mathcal{A}^*((\mathbb{P}^n)^{s+3})$ de $(\mathbb{P}^n)^{s+3}$. Notamos como θ_{j-2} a la clase de la imagen inversa de un hiperplano de $\mathbb{P}^n$ por la j-ésima proyección canónica $(\mathbb{P}^n)^{s+3} \to \mathbb{P}^n$ para $1 \le j \le s+3$. En particular, θ_{-1} está asociada a la proyección $\pi_1 : \mathbb{P}^n \times (\mathbb{P}^n)^{s+2} \to \mathbb{P}^n$. De (2.4) se sigue que

$$\begin{aligned} &[V(F_i)] \le d_i\theta_{-1} \quad (1 \le i \le n-r), \\ &[V(\Delta^i)] \le D\theta_{-1} + \theta_0 + \cdots + \theta_{s+1} \quad (1 \le i \le r-s). \end{aligned}$$

Teniendo en cuenta el Teorema de Bézout multihomogéneo (2.5), vemos que

$$\begin{aligned} [W'] &\le \prod_{i=1}^{n-r}(d_i\theta_{-1}) \prod_{k=1}^{r-s}(D\theta_{-1} + \theta_0 + \cdots + \theta_{s+1}) \\ &\le \delta D^{r-s-1}\left(D(\theta_{-1})^{n-s} + (r-s)(\theta_{-1})^{n-s-1}(\theta_0 + \cdots + \theta_{s+1})\right) \\ &\quad + \mathcal{O}\big((\theta_{-1})^{n-s-2}\big), \end{aligned} \tag{3.11}$$

donde $\mathcal{O}\big((\theta_{-1})^{n-s-2}\big)$ representa la suma de los términos de grado a lo sumo $n-s-2$ en θ_{-1} en la expresión de $[W']$. Por otro lado, de (2.4) se tiene

$$[\overline{\pi_i(W_i')}] = \deg_X m_i' \, \theta_{-1} + \deg_{\Lambda_0} m_i' \, \theta_0 + \cdots + \deg_{\Lambda_{s+1}} m_i' \, \theta_{s+1},$$

donde $m_i' \in \mathbb{F}_q[X_{i_0}, \dots, X_{i_s}, X_i, \mathbf{\Lambda}]$ es un polinomio de grado mínimo que define a $\overline{\pi_i(W_i')}$. Sea $\jmath : \mathcal{A}^*\big(\mathbb{P}^{s+1} \times (\mathbb{P}^n)^{s+2}\big) \hookrightarrow \mathcal{A}^*\big((\mathbb{P}^n)^{s+3}\big)$ la aplicación $\mathbb{Z}$-lineal e inyectiva $P \mapsto (\theta_{-1})^{n-s-1}P$ que induce π_i. Por (2.6), como $\dim \overline{\Pi_i(W_i')} = \dim W_i'$, se tiene $\jmath([\overline{\pi_i(W_i')}]) \le [W_i']$ y, por definición, $[W_i'] \le [W']$. Por lo tanto,

$$\jmath([\overline{\pi_i(W_i')}]) = \deg_X m_i' \, (\theta_{-1})^{n-s} + \sum_{j=0}^{s+1} \deg_{\Lambda_j} m_i' (\theta_{-1})^{n-s-1} \, \theta_j \le [W'],$$

donde las desigualdades se entienden coeficiente a coeficiente. De (3.11) deducimos que $\deg_{\Lambda_j} m_i' \le (r-s)D^{r-s-1}\delta$ para $0 \le j \le s+1$.

Sea $m_i \in \mathbb{F}_q[X_{i_0}, \dots, X_{i_s}, X_i, \mathbf{\Lambda}]$ un polinomio de grado mínimo que define a W_i. Notemos que $D_i := \deg_{X_i} m_i > 0$. Sea $A_i \in \overline{\mathbb{F}}_q[X_{i_0}, \dots, X_{i_s}, \mathbf{\Lambda}]$ el polinomio no nulo que es el coeficiente de $X_i^{D_i}$ en m_i, considerando m_i como un elemento de $\overline{\mathbb{F}}_q[X_{i_0}, \dots, X_{i_s}, \mathbf{\Lambda}][X_i]$. Sea además $A_i^* \in \overline{\mathbb{F}}_q[\mathbf{\Lambda}]$ un coeficiente no nulo de A_i,

considerando A_i como un elemento de $\overline{\mathbb{F}}_q[\mathbf{\Lambda}][X_{i_0},\ldots,X_{i_s}]$. Finalmente, sea $A_0 \in \overline{\mathbb{F}}_q[\mathbf{\Lambda}]$ un menor maximal arbitrario de la matriz genérica $(\Lambda_{i,j})_{0\le i\le s+1,0\le j\le n}$. Tomemos $A := A_0 \cdot \prod_{i\in\Gamma} A_i^* \in \overline{\mathbb{F}}_q[\mathbf{\Lambda}]$. Afirmamos que la hipersuperficie $\mathcal{H}_1 \subset (\mathbb{P}^n)^{s+2}$ definida como el conjunto de ceros de A satisface las condiciones del teorema. Con el objetivo de demostrar esta afirmación, consideremos $\boldsymbol{\lambda} := (\lambda_0,\ldots,\lambda_{s+1}) \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}_1$ y notemos $m_i^{(\boldsymbol{\lambda})} := m_i(X_{i_0},\ldots,X_{i_s},X_i,\boldsymbol{\lambda})$. Dado que $A_0(\boldsymbol{\lambda}) \neq 0$, se tiene que $\boldsymbol{\lambda} \in \mathcal{U}$. Más aún, $A_i^*(\boldsymbol{\lambda}) \neq 0$, lo que implica que $A_i(X_{i_0},\ldots,X_{i_s},\boldsymbol{\lambda})$ es un polinomio no nulo de $\overline{\mathbb{F}}_q[X_{i_0},\ldots,X_{i_s}]$. Este polinomio es el coeficiente de $X_i^{D_i}$ en $m_i^{(\boldsymbol{\lambda})}$, considerando $m_i^{(\boldsymbol{\lambda})}$ como un elemento de $\overline{\mathbb{F}}_q[X_{i_0},\ldots,X_{i_s}][X_i]$. Concluimos que $m_i^{(\boldsymbol{\lambda})}$ es un polinomio no nulo en $\overline{\mathbb{F}}_q[X_{i_0},\ldots,X_{i_s},X_i]$ tal que $\deg_{X_i} m_i^{(\boldsymbol{\lambda})} > 0$ y se anula en $\mathsf{M}(L)$ para todo $i \in \Gamma$, donde L es la variedad lineal asociada a $\boldsymbol{\lambda}$. Esto implica que, para cada $i \in \Gamma$, la función coordenada X_i de $\overline{\mathbb{F}}_q[\mathsf{M}(L)]$ verifica una ecuación algebraica no trivial sobre $\overline{\mathbb{F}}_q(X_{i_0},\ldots,X_{i_s})$. De esto se sigue que $\mathsf{M}(L)$ tiene dimensión a lo sumo s.

Como $A_i^* \in \overline{\mathbb{F}}_q[\mathbf{\Lambda}]$ es a un polinomio multihomogéneo con $\deg_{\Lambda_i} A_i^* \le (r-s)D^{r-s-1}\delta$ y $|\Gamma| = n-s$, obtenemos $\deg_{\Lambda_i} A \le (n-s)(r-s)D^{r-s-1}\delta + 1$ dado que$A := A_0 \cdot \prod_{i\in\Gamma} A_i^*$. Esto concluye con la demostración del teorema. □

3.2. Sobre la existencia de secciones lineales no singulares de dimensión $r-s-2$

Recordemos que $V \subset \mathbb{P}^n$ es una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r y grado δ, y que $F_1,\ldots,F_{n-r} \in \mathbb{F}_q[X_0,\ldots,X_n]$ son polinomios homogéneos de grados $d_1 \ge \ldots \ge d_{n-r} \ge 2$ respectivamente, que generan el ideal $I(V)$ de V. Supongamos que la dimensión de Σ, el lugar singular de V, es a lo sumo $s \le r-2$. En particular, V es normal y, por lo tanto, absolutamente irreducible (ver Teorema 2.1.4). En esta sección vamos a mostrar la existencia de secciones lineales no singulares de V de codimensión $s+2$. Identificando cada sección de este tipo con un punto en el espacio multiproyectivo $(\mathbb{P}^n)^{s+2}$, vamos a mostrar que existe una hipersuperficie $\mathcal{H}_2 \subset (\mathbb{P}^n)^{s+2}$ que contiene a las subvariedades lineales de codimensión $s+2$ de $(\mathbb{P}^n)^{s+2}$ que definen secciones singulares de V. Más aún, vamos a dar una cota superior para el grado de dicha hipersuperficie.

Sean $\boldsymbol{\lambda} := (\lambda_0,\ldots,\lambda_{s+1}) \in (\mathbb{P}^n)^{s+2}$ y L la variedad lineal de $\mathbb{P}^n$ asociada a $\boldsymbol{\lambda}$ definida como en (3.1). Nuestro objetivo es dar condiciones sobre $\lambda_0,\ldots,\lambda_{s+1}$ bajo las cuales $V \cap L$ es no singular y tiene dimensión $r-s-2$. Recordamos las notaciones

$$D := \sum_{i=1}^{n-r}(d_i-1), \qquad \delta := \deg V = \prod_{i=1}^{n-r} d_i, \qquad t := n(s+2).$$

Comenzamos dando un resultado que nos permitirá establecer condiciones sobre los elementos $\boldsymbol{\lambda}$ para los cuales $V \cap L$ tiene dimensión $r-s-2$.

Lema 3.2.1. *Existe una hipersuperficie $\mathcal{H}_2' \subset (\mathbb{P}^n)^{s+2}$, definida por un polinomio multihomogéneo en $\overline{\mathbb{F}}_q[\mathbf{\Lambda}]$ de multigrado a lo sumo δ en cada grupo de variables Λ_i, con la siguiente propiedad: sea $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}_2'$, y sea $\pi : V \dashrightarrow \mathbb{P}^{s+1}$ la proyección*

lineal definida en (3.2). Entonces la clausura Zariski V_y de cualquier fibra $\pi^{-1}(y)$ es equidimensional de dimensión $r-s-1$ y el conjunto de puntos excepcionales de π es equidimensional de dimensión $r-s-2$.

Demostración. Sean $U_0,\ldots,U_r$ $r+1$ grupos de $n+1$ indeterminadas en $\overline{\mathbb{F}}_q[X_0,\ldots,X_n]$, donde $U_i := (U_{i,0},\ldots,U_{i,n})$ y $\boldsymbol{U} := (U_0,\ldots,U_r)$. Consideramos la forma de Chow $\mathcal{F}_V \in \mathbb{F}_q[\boldsymbol{U}]$ de V (ver [HP94b, Chapter X, §6] o [Sam67, Chapter I, §9]). Se tiene que $\mathcal{F}_V \in \mathbb{F}_q[\boldsymbol{U}]$ es un polinomio irreducible en $\overline{\mathbb{F}}_q[\boldsymbol{U}]$ que caracteriza al conjunto de los sistemas lineales sobredeterminados sobre V. Más precisamente, dado $\boldsymbol{u} \in (\mathbb{P}^n)^r$, $\mathcal{F}_V(\boldsymbol{u}) \neq 0$ si y sólo si $V \cap \{u_i \cdot X = 0 : 0 \leq i \leq r\}$ es vacía. Además, $\mathcal{F}_V$ es homogéneo en cada grupo de variables U_i y satisface $\deg_{U_{i,0}} \mathcal{F}_V = \deg_{U_i} \mathcal{F}_V = \delta$ para $0 \leq i \leq r$.

Consideremos $\mathcal{F}_V$ como un polinomio de $\mathbb{F}_q[U_0,\ldots,U_{s+1}][U_{s+2},\ldots,U_r]$ y fijemos $u_{s+2},\ldots,u_r \in \mathbb{P}^n$ tal que $B := \mathcal{F}_V(U_0,\ldots,U_{s+1},u_{s+2},\ldots,u_r)$ es no nulo. Afirmamos que si $\boldsymbol{\lambda} := (\lambda_0,\ldots,\lambda_{s+1}) \in (\mathbb{P}^n)^{s+2}$ verifica $B(\boldsymbol{\lambda}) \neq 0$, entonces $\boldsymbol{\lambda}$ satisface los requerimientos del lema. En efecto, por la definición de $\boldsymbol{\lambda}$ y $\boldsymbol{u} := (u_{s+2},\ldots,u_r)$ se tiene que $\mathcal{F}_V(\boldsymbol{\lambda},\boldsymbol{u}) \neq 0$. Esto implica que

$$V \cap \{\lambda_0 \cdot X = \cdots = \lambda_{s+1} \cdot X = 0, u_{s+2} \cdot X = \cdots = u_r \cdot X = 0\} = \emptyset. \tag{3.12}$$

Luego, el morfismo $\pi_r : V \dashrightarrow \mathbb{P}^r$ definido por las formas lineales $\lambda_0 \cdot X,\ldots,\lambda_{s+1} \cdot X, u_{s+2} \cdot X,\ldots,u_r \cdot X$ es finito (ver, por ejemplo, [Sha94, §I.5.3, Theorem 8]). Sea $\pi : V \dashrightarrow \mathbb{P}^{s+1}$ el morfismo definido por las formas lineales $\lambda_0 \cdot X,\ldots,\lambda_{s+1} \cdot X$. Observemos que $\pi = \pi_{r,s} \circ \pi_r$, donde $\pi_{r,s} : \mathbb{P}^r \dashrightarrow \mathbb{P}^{s+1}$ es el morfismo lineal definido por $(x_0 : \cdots : x_r) \mapsto (x_0 : \cdots : x_{s+1})$. Como $\pi_{r,s}$ es suryectiva, la clausura Zariski $L_y \subset \mathbb{P}^r$ de la preimagen de $\pi_{r,s}^{-1}(y)$ para $y \in \mathbb{P}^{s+1}$ es una variedad lineal de dimensión $r-s-1$. Entonces, la clausura Zariski V_y de cualquier fibra $\pi^{-1}(y)$ coincide con la preimagen por π_r de la variedad lineal $L_y \subset \mathbb{P}^r$ y, por lo tanto, es equidimensional de dimensión $r-s-1$. Por otro lado, de (3.12) se obtiene que el conjunto de puntos excepcionales $\mathsf{E} := V \cap \{\lambda_0 \cdot X = \cdots = \lambda_{s+1} \cdot X = 0\}$ de π es equidimensional de dimensión $r-s-2$. En efecto, cada componente irreducible de E tiene dimensión al menos $r-s-2$ (ver, por ejemplo, [Sha94, §I.6.2, Corollary 2, p. 75]). Más aún, si existiera una componente irreducible $\mathcal{C}$ de E de dimensión al menos $r-s-1$, entonces $\mathcal{C} \cap \{u_{s+2} \cdot X = \cdots = u_r \cdot X = 0\}$ sería no vacía, contradiciendo (3.12).

Finalmente, definimos $\mathcal{H}_2' \subset (\mathbb{P}^n)^{s+2}$ como el conjunto de ceros del polinomio $B \in \overline{\mathbb{F}}_q[U_0,\ldots,U_{s+1}]$, lo que concluye la demostración del lema. □

Recordemos que queremos obtener condiciones sobre $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2}$ que nos permitan garantizar que $V \cap L$ es no singular. Para eso, de acuerdo al Lema 3.1.2, necesitamos dar condiciones sobre los elementos $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2}$ tales que $\Sigma \cap L = \emptyset$ y $\mathsf{M}(L) \cap L = \emptyset$.

Lema 3.2.2. *Existe una hipersuperficie $\mathcal{H}_2'' \subset (\mathbb{P}^n)^{s+2}$, definida por un polinomio multihomogéneo en $\overline{\mathbb{F}}_q[\boldsymbol{\Lambda}]$ de multigrado a lo sumo $D^{r-s-1}\delta$ en cada grupo de variables Λ_i, con la siguiente propiedad: si $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}_2''$, entonces $\Sigma \cap L$ es vacía.*

Demostración. Un punto x de V es singular de V si y sólo si la matriz Jacobiana de $F_1(x),\ldots,F_{n-r}(x)$ no tiene rango máximo. Sean $\Delta'_1,\ldots,\Delta'_M$ los menores maximales de la matriz Jacobiana de $F_1,\ldots,F_{n-r}$. Entonces se tiene que

$$\Sigma = \{x \in V : \Delta'_1 = \cdots = \Delta'_M = 0\}.$$

Observemos que todos los polinomios Δ'_j son homogéneos de grado D y $\Sigma \subset V$ tiene dimensión a lo sumo $s < s+1$. Entonces el Lema 3.1.5 afirma que existen combinaciones lineales $H^1,\ldots,H^{r-s-1}$ de $\Delta'_1,\ldots,\Delta'_M$ tales que la variedad proyectiva $Z := V \cap \{H^1 = \cdots = H^{r-s-1} = 0\} \subset \mathbb{P}^n$ es equidimensional de dimensión $s+1$ y $\Sigma \subset Z$. Por la desigualdad de Bézout (2.2) se tiene que el grado de Z es a lo sumo $D^{r-s-1}\delta$.

Consideramos la forma de Chow $\mathcal{F}_Z \in \mathbb{F}_q[\mathbf{\Lambda}]$ de Z. Luego $\mathcal{F}_Z$ es homogéneo en cada grupo de variables Λ_i y se satisface $\deg_{\Lambda_i} \mathcal{F}_Z \leq D^{r-s-1}\delta$ para $0 \leq i \leq s+1$.

Sea $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2}$ tal que $\mathcal{F}_Z(\boldsymbol{\lambda}) \neq 0$ y sea $L := \{\lambda_i \cdot X = 0,\ 0 \leq i \leq s+1\}$. Entonces, por la definición de $\mathcal{F}_Z$, obtenemos que $Z \cap L$ es vacía y, por lo tanto, $\Sigma \cap L = \emptyset$. Definiendo $\mathcal{H}''_2 \subset (\mathbb{P}^n)^{s+2}$ como el conjunto de ceros de $\mathcal{F}_Z$, se concluye la demostración del lema. □

A continuación vamos a dar condiciones sobre $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2}$ tal que $\mathsf{M}(L) \cap L = \emptyset$. Para ello, de manera similar a la Sección 3.1, consideramos la siguiente variedad de incidencia:

$$\begin{aligned} W_s := (V_{\mathrm{sm}} \times \mathcal{U}) \cap \{&\Lambda_0 \cdot X = 0,\ldots,\Lambda_{s+1} \cdot X = 0,\\ &\Delta_1(\mathbf{\Lambda}, X) = 0,\ldots,\Delta_N(\mathbf{\Lambda}, X) = 0\}, \end{aligned} \tag{3.13}$$

donde $\mathcal{U} \subset (\mathbb{P}^n)^{s+2}$ es el abierto Zariski de las matrices de tamaño $(s+2)\times(n+1)$ con rango máximo y $\Delta_1,\ldots,\Delta_N$ son los menores maximales de la versión genérica $\mathsf{M}(X,\mathbf{\Lambda})$ de la matriz de (3.6). Notamos por $\pi_2 : W_s \to \mathcal{U}$ la proyección a la segunda coordenada. Entonces cada $\boldsymbol{\lambda} \in \Pi_2(W_s)$ corresponde a una variedad lineal $L \subset \mathbb{P}^n$ de codimensión $s+2$ tal que $L \cap \mathsf{M}(L) \neq \emptyset$ lo que en particular implica por la Proposición 3.1.2 que $V \cap L$ es singular.

En primer lugar probamos que W_s es irreducible de dimensión $t-1$.

Proposición 3.2.3. *W_s es una subvariedad irreducible de $\mathbb{P}^n \times \mathcal{U}$ de dimensión $t-1$.*

Demostración. Como los argumentos son similares a los de la Proposición 3.1.4, omitiremos algunos detalles.

Sea $\pi_1 : W_s \to V_{\mathrm{sm}}$ el morfismo lineal definido por $\pi_1(x,\boldsymbol{\lambda}) := x$. Fijemos $x \in V_{\mathrm{sm}}$ y consideremos una fibra arbitraria $\pi_1^{-1}(x)$. Se tiene entonces que $\pi_1^{-1}(x) = \{x\} \times \mathcal{L}$, donde $\mathcal{L} \subset \mathcal{U}$ denota el conjunto de matrices $\boldsymbol{\lambda} := (\lambda_0,\ldots,\lambda_{s+1})$ tales que $\lambda_j \cdot x = 0$ para $0 \leq j \leq s+1$ y la matriz $\mathsf{M}(x,\boldsymbol{\lambda})$ no tiene rango completo. Esta última condición es equivalente a

$$\langle \lambda_0,\ldots,\lambda_{s+1}\rangle \cap \langle \nabla F_1(x),\ldots,\nabla F_{n-r}(x)\rangle \neq \{\mathbf{0}\}, \tag{3.14}$$

donde $\langle v_0,\ldots,v_m\rangle \subset \mathbb{A}^{n+1}$ denota la variedad lineal generada por $v_0,\ldots,v_m$ en $\mathbb{A}^{n+1}$. Sea $\mathbb{V} := \{v \in \mathbb{A}^{n+1} : v \cdot x = 0\}$ y observemos que $\nabla F_j(x) \in \mathbb{V}$ para $1 \leq j \leq n-r$.

Entonces $\lambda_j \cdot x = 0$ para $0 \leq j \leq s+1$ y vale (3.14) si y sólo si $\lambda_0, \ldots, \lambda_{s+1}$ pertenecen a $\mathbb{V}$ y son linealmente dependientes en el $\overline{\mathbb{F}}_q$-espacio vectorial cociente

$$\mathbb{W} := \mathbb{V}/\big(\nabla F_1(x), \ldots, \nabla F_{n-r}(x)\big).$$

Esto muestra que el cono afín $\mathcal{C}(\mathcal{L})$ de $\mathcal{L}$ resulta, módulo $\big(\nabla F_1(x), \ldots, \nabla F_{n-r}(x)\big)$, isomorfo al abierto Zariski $L'_{s+1}(\mathbb{A}^{s+2}, \mathbb{W}) \cap \Phi(\mathcal{U}_{\text{aff}})$ de $L'_{s+1}(\mathbb{A}^{s+2}, \mathbb{W})$, donde

$$L'_{s+1}(\mathbb{A}^{s+2}, \mathbb{W}) := \{f \in \operatorname{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{V}) : \operatorname{rg}(f) \leq s+1\},$$

$\mathcal{U}_{\text{aff}} \subset (\mathbb{A}^{n+1})^{s+2}$ es el cono afín de $\mathcal{U}$ y $\Phi : \operatorname{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{A}^{n+1}) \to \operatorname{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+2}, \mathbb{W})$ es el morfismo suryectivo inducido por la proyección al cociente $\mathbb{A}^{n+1} \to \mathbb{W}$. De acuerdo a [BV88, Proposition 1.1], $L'_{s+1}(\mathbb{A}^{s+2}, \mathbb{W})$ es una variedad irreducible de dimensión $(s+1)(r+1)$. Como estamos considerando subespacios de $\mathbb{V}$ de dimensión $s+2$ módulo $\langle \nabla F_1(x), \ldots, \nabla F_{n-r}(x)\rangle$, cuya dimensión es $n-r$ pues $x \in V_{\text{sm}}$, se sigue que el cono afín de $\pi_1^{-1}(x) = \{x\} \times \mathcal{L}$ es un abierto denso contenido en una variedad irreducible de $V_{\text{sm}} \times \mathcal{U}_{\text{aff}}$ de dimensión $(s+1)(r+1) + (n-r)(s+2) = (n+1)(s+2) - r - 1$. Esto implica que $\pi_1^{-1}(x) = \{x\} \times \mathcal{L}$ es una variedad irreducible de $V_{\text{sm}} \times \mathcal{U}$ de dimensión $t - r - 1$.

Como en la demostración de la Proposición 3.1.4 la proyección a la segunda coordenada $V_{\text{sm}} \times \mathcal{U} \to V_{\text{sm}}$ es cerrada. Sea $W_s = \bigcup_j \mathcal{C}_j$ la descomposición de W_s en componentes irreducible. Nuestros argumentos previos muestran que $\pi_1 : W_s \to V_{\text{sm}}$ es suryectiva. Por lo tanto, $\pi_1(W_s) = V_{\text{sm}} = \bigcup_j \pi_1(\mathcal{C}_j)$ y cada $\pi_1(\mathcal{C}_j)$ es un subconjunto cerrado de V_{sm}. Como V_{sm} es irreducible existe un j tal que $V_{\text{sm}} = \pi_1(\mathcal{C}_j)$.

El mismo razonamiento hecho en el penúltimo párrafo de la demostración de la Proposición 3.1.4 prueba que W_s es una subvariedad irreducible de $V_{\text{sm}} \times \mathcal{U}$.

Finalmente, por el Teorema de la dimensión de las fibras (ver, por ejemplo, [Sha94, §I.6.3, Theorem 7]), para cada $x \in V_{\text{sm}}$ tenemos

$$t - r - 1 = \dim \pi_1^{-1}(x) = \dim W_s - \dim V_{\text{sm}} = \dim W_s - r.$$

Esto muestra que la dimension de W_s es $t-1$ y concluye la demostración de la proposición. □

Como consecuencia de la Proposición 3.2.3 se tiene que la clausura Zariski $\mathcal{H}_s \subset (\mathbb{P}^n)^{s+2}$ de la imagen de la proyección $\pi_2 : W_s \to \mathcal{U}$ es una variedad irreducible de dimensión a lo sumo $t-1$. A continuación probamos que $\mathcal{H}_s \subset (\mathbb{P}^n)^{s+2}$ es una hipersuperficie.

Teorema 3.2.4. *Sea $\mathcal{H}_s \subset (\mathbb{P}^n)^{s+2}$ la clausura Zariski de la imagen de $\pi_2 : W_s \to \mathcal{U}$. Entonces $\mathcal{H}_s$ es una hipersuperficie de $(\mathbb{P}^n)^{s+2}$, definida por un polinomio multihomogéneo de $\overline{\mathbb{F}}_q[\mathbf{\Lambda}]$ de grado a lo sumo $\delta D^{r-s-2}(D+r-s-1)$ en cada grupo de variables Λ_i.*

Demostración. Primero veamos que $\mathcal{H}_s$ es una hipersuperficie. De acuerdo al Teorema de la dimensión de las fibras, resulta suficiente mostrar que existe una fibra de π_2 de dimensión cero. En efecto, en estas condiciones se sigue de dicho teorema que

$$0 = \dim \pi_2^{-1}(\boldsymbol{\lambda}) \geq \dim W_s - \dim \pi_2(W_s).$$

Luego, $\dim \pi_2(W_s) \geq \dim W_s = t-1$. Por otro lado, es claro que $\dim \pi_2(W_s) \leq t-1$, lo que prueba que $\dim \pi_2(W_s) = t-1$. Como la clausura Zariski $\mathcal{H}_s$ de $\pi_2(W_s)$ es irreducible y de dimensión $t-1$, se concluye que es una hipersuperficie.

Fijemos entonces $s+1$ formas lineales genéricas $\lambda_0 \cdot X, \ldots, \lambda_s \cdot X$ y consideremos la variedad lineal L' definida por $\lambda_i \cdot X = 0$ para $0 \leq i \leq s$. Por [GL02a, Proposition 1.3] se tiene que $V \cap L'$ es no singular y equidimensional de dimensión $r-s-1$. Afirmamos que es posible elegir $\lambda_{s+1} \in \mathbb{P}^n$ tal que $\boldsymbol{\lambda} := (\lambda_0, \ldots, \lambda_{s+1}) \in \mathcal{U}$ y, si L es la variedad lineal definida por $L := \{x \in \mathbb{P}^n : \lambda_0 \cdot X = \cdots = \lambda_{s+1} \cdot X = 0\}$, entonces $V \cap L$ es singular y $\Sigma \cap L = \emptyset$. En efecto, como $V \cap L'$ es no singular, los vectores $\nabla F_1(x), \ldots, \nabla F_{n-r}(x), \lambda_0, \ldots, \lambda_s$ son linealmente independientes para todo $x \in V \cap L'$. Para $x \in V \cap L'$ elegimos $\lambda_{s+1} := \nabla F_1(x)$; de esta forma, las ecuaciones $\lambda_i \cdot X = 0$ con $0 \leq i \leq s+1$ definen una variedad lineal L de dimensión $n-s-2$ para la cual x resulta ser un punto singular de $V \cap L$, ya que el rango de la matriz $\mathsf{M}(x, \boldsymbol{\lambda})$ definida como en (3.6) no es máximo. Más aún, de acuerdo a [Hoo91, Appendix, Theorem 2], la dimensión del lugar singular de $V \cap L$ es cero. Finalmente, teniendo en cuenta el Lema 3.1.2 *ii*) se obtiene que $L' \cap \Sigma = \emptyset$, lo que implica que $L \cap \Sigma = \emptyset$. Dado que el lugar singular de $V \cap L$ coincide con la fibra $\pi_2^{-1}(\lambda_0, \ldots, \lambda_{s+1})$, probamos la existencia de una fibra de π_2 de dimensión cero.

A continuación encontramos una cota de grado para la hipersuperficie $\mathcal{H}_s$. Para eso vamos a mostrar la existencia de una variedad $W_s' \subset (\mathbb{P}^n)^{s+3}$ equidimensional de dimensión $t-1$ y grado bajo que contiene a W_s.

Afirmación. *Existen combinaciones lineales $\Delta^1, \ldots, \Delta^{r-s-1}$ de los polinomios $\Delta_1(\boldsymbol{\Lambda}, X), \ldots, \Delta_N(\boldsymbol{\Lambda}, X)$ tales que la subvariedad $W_s' \subset (\mathbb{P}^n)^{s+3}$ definida por los ceros comunes de las ecuaciones*

$$\begin{aligned} F_1 = 0, \ldots, F_{n-r} = 0, \Lambda_0 \cdot X = 0, \ldots, \Lambda_{s+1} \cdot X = 0, \\ \Delta^1(\boldsymbol{\Lambda}, X) = 0, \ldots, \Delta^{r-s-1}(\boldsymbol{\Lambda}, X) = 0, \end{aligned} \tag{3.15}$$

es equidimensional de dimensión $t-1$.

Demostración. Sea $L_\Lambda := \{\Lambda_0 \cdot X = 0, \ldots, \Lambda_{s+1} \cdot X = 0\} \subset (\mathbb{P}^n)^{s+3}$ y sea $W_s'' \subset (\mathbb{P}^n)^{s+3}$ la siguiente variedad:

$$W_s'' := W_s \cup \big((\Sigma \times (\mathbb{P}^n)^{s+2}) \cap L_\Lambda\big) \cup \big((V \times ((\mathbb{P}^n)^{s+2} \setminus \mathcal{U})) \cap L_\Lambda\big).$$

Por la definición de W y W_s en (3.7) y (3.13) se concluye que $W_s = W \cap L_\Lambda$. Luego, $W_s'' = W'' \cap L_\Lambda$, donde W'' es la variedad definida en (3.9). Por lo tanto, intersecando ambos lados de (3.10) con L_Λ deducimos la identidad

$$W_s'' = \big(\big(V \times (\mathbb{P}^n)^{s+2}\big) \cap L_\Lambda\big) \cap \{\Delta_1(\boldsymbol{\Lambda}, X) = 0, \ldots, \Delta_N(\boldsymbol{\Lambda}, X) = 0\}.$$

A continuación, determinamos la dimensión de W_s''. Primero observemos que $\Sigma \times (\mathbb{P}^n)^{s+2}$ es un cilindro cuya intersección con las ecuaciones $\Lambda_0 \cdot X = 0, \ldots, \Lambda_{s+1} \cdot X = 0$ tiene codimensión $s+2$ en $\Sigma \times (\mathbb{P}^n)^{s+2}$. Por lo tanto, la dimensión de $(\Sigma \times (\mathbb{P}^n)^{s+2}) \cap L_\Lambda$ es a lo sumo $s+t-(s+2) < t-1$.

En la segunda afirmación de la Proposición 3.1.4 probamos que $V \times ((\mathbb{P}^n)^{s+2} \setminus \mathcal{U})$ tiene dimensión $t+r-n+s$. Consideremos la proyección en la segunda coordenada

$\pi_2 : \big(V \times ((\mathbb{P}^n)^{s+2} \setminus \mathcal{U})\big) \cap L_\Lambda \to (\mathbb{P}^n)^{s+2} \setminus \mathcal{U}$. Una variedad lineal genérica de $\mathbb{P}^n$ de codimensión $s+1$ interseca a V en una variedad equidimensional de dimensión $r-s-1$. Por lo tanto, una fibra genérica $\pi_2^{-1}(\boldsymbol{\lambda})$ tiene dimensión $r-s-1$. Luego, el Teorema de la dimensión de las fibras muestra que

$$r-s-1 = \dim \pi_2^{-1}(\boldsymbol{\lambda}) \geq \dim \big(V \times ((\mathbb{P}^n)^{s+2} \setminus \mathcal{U})\big) \cap L_\Lambda - (t-n+s).$$

Deducimos que $\big(V \times ((\mathbb{P}^n)^{s+2} \setminus \mathcal{U})\big) \cap L_\Lambda$ tiene dimensión a lo sumo $t-n+r-1 < t-1$. Combinando estos hechos con la Proposición 3.2.3, concluimos que W_s'' tiene dimensión $t-1$.

Ahora aplicamos el Lema 3.1.5 a las variedades $\mathcal{W} := \big(V \times (\mathbb{P}^n)^{s+2}\big) \cap L_\Lambda$ y $\mathcal{W}_1 := W_s''$. Del Lema 3.1.5 se deduce fácilmente la afirmación. □

Sea $\mathcal{H}_s' \subset (\mathbb{P}^n)^{s+2}$ la unión de las componentes de la clausura Zariski de $\pi_2(W_s')$ de dimensión $t-1$. Notar que $\mathcal{H}_s'$ es una hipersuperficie que contiene $\mathcal{H}_s$.

Estimamos finalmente el multigrado de $\mathcal{H}_s'$. Sea $[W_s']$ la clase de W_s' en el anillo de Chow $\mathcal{A}^*((\mathbb{P}^n)^{s+3})$ de $(\mathbb{P}^n)^{s+3}$. Notamos como θ_{j-2} a la clase de la imagen inversa de un hiperplano de $\mathbb{P}^n$ por la j-ésima proyección canónica $(\mathbb{P}^n)^{s+3} \to \mathbb{P}^n$ para $1 \leq j \leq s+2$. De acuerdo a la definición de W_s' dada en (3.20) y por el Teorema de Bézout multihomogéneo (2.5), se tiene

$$\begin{aligned}[W_s'] &\leq \prod_{i=1}^{n-r}(d_i\theta_{-1}) \prod_{j=0}^{s+1}(\theta_{-1}+\theta_j) \prod_{k=1}^{r-s-1}(D\theta_{-1}+\theta_0+\cdots+\theta_{s+1}) \\ &\leq \delta D^{r-s-2}(D+r-s-1)(\theta_{-1})^n(\theta_0+\cdots+\theta_{s+1}) \\ &\quad + \text{términos de grado menor en } \theta_{-1}.\end{aligned}$$

Por otro lado, $[\mathcal{H}_s'] = \deg_X H_s'\,\theta_{-1} + \deg_{\Lambda_0} H_s'\,\theta_0 + \cdots + \deg_{\Lambda_{s+1}} H_s'\,\theta_{s+1}$, donde $H_s' \in \mathbb{F}_q[\Lambda]$ es un polinomio de grado mínimo que define $\mathcal{H}_s'$. Sea $\jmath : \mathcal{A}^*\big((\mathbb{P}^n)^{s+2}\big) \hookrightarrow A^*\big((\mathbb{P}^n)^{s+3}\big)$, $P \mapsto (\theta_{-1})^n P$ el morfismo $\mathbb{Z}$–lineal inyectivo inducido por π_2. Entonces por (2.6) se tiene que $\jmath([\mathcal{H}_s']) \leq [W_s']$. Esto implica que $\deg_{\Lambda_j} H_s' \leq \delta D^{r-s-2}(D+r-s-1)$ para $0 \leq j \leq s+1$, finalizando así la demostración del teorema. □

Por último, combinando los Lemas 3.2.1 y 3.2.2 y el Teorema 3.2.4, obtenemos el resultado más importante de esta sección.

Corolario 3.2.5. *Existe una hipersuperficie $\mathcal{H}_2 \subset (\mathbb{P}^n)^{s+2}$, definida por un polinomio multihomogéneo de grado a lo sumo $\big(D^{r-s-2}(2D+r-s-1)+1\big)\delta$ en cada grupo de variables Λ_i, con la siguiente propiedad: si $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}_2$ y $L \subset \mathbb{P}^n$ y $\pi \dashrightarrow \mathbb{P}^{s+1}$ están definidos como en (3.1) y (3.3) respectivamente, entonces se satisfacen las siguientes condiciones:*

1. *$V \cap L$ es no singular y equidimensional de dimensión $r-s-2$;*
2. *$\Sigma \cap L$ es vacía;*
3. *La clausura Zariski V_y de la fibra $\pi^{-1}(y)$ es equidimensional de dimensión $r-s-1$ para todo $y \in \mathbb{P}^{s+1}$.*

Demostración. Sea $\mathcal{H}_2 = \mathcal{H}_2' \cup \mathcal{H}_2'' \cup \mathcal{H}_s$, donde $\mathcal{H}_2'$, $\mathcal{H}_2''$ y $\mathcal{H}_s$ son las hipersuperficies definidas en los Lemas 3.2.1 y 3.2.2 y el Teorema 3.2.4 respectivamente.

Si $\boldsymbol{\lambda} \notin \mathcal{H}_2$ entonces por el Lema 3.2.1 vale (3) y $V \cap L$ es equidimensional de dimensión $r-s-2$. En particular, $L \subset \mathbb{P}^n$ tiene codimensión $s+2$, es decir, $\boldsymbol{\lambda} \in \mathcal{U}$. Por otro lado, por el Lema 3.2.2, se satisface (2), de lo que se obtiene que $V \cap L = V \cap V_{\mathrm{sm}}$. Finalmente, como $\boldsymbol{\lambda} \notin \mathcal{H}_s$, se tiene que $\boldsymbol{\lambda} \notin \pi_2(W_s)$, donde W_s es la variedad de incidencia definida en (3.13). Esto implica que

$$V \cap L \cap \{\Delta_1(\boldsymbol{\lambda}, X) = 0, \ldots, \Delta_N(\boldsymbol{\lambda}, X) = 0\} = \emptyset.$$

Concluimos que $V \cap L$ es no singular, dado que $\Delta_1(\boldsymbol{\lambda}, X), \ldots, \Delta_N(\boldsymbol{\lambda}, X)$ son los menores maximales de la matriz Jacobiana de los polinomios que definen a $V \cap L$.

La cota de grado de la hipersuperficie $\mathcal{H}_2$ se obtiene como consecuencia inmediata de los Lemas 3.2.1 y 3.2.2 y del Teorema 3.2.4 □

Finalmente combinando el Teorema 3.1.6 y el Corolario 3.2.5 obtenemos el siguiente resultado.

Proposición 3.2.6. *Sea $\mathcal{H} \subset (\mathbb{P}^n)^{s+2}$ la hipersuperficie definida por $\mathcal{H} := \mathcal{H}_1 \cup \mathcal{H}_2$, donde $\mathcal{H}_1$ y $\mathcal{H}_2$ son las hipersuperficies dadas en los Teorema 3.1.6 y el Corolario 3.2.5 respectivamente. Luego $\mathcal{H}$ está definida por un polinomio multihomogéneo en $\mathbb{F}_q[\boldsymbol{\Lambda}]$ de grado a lo sumo*

$$B_{\boldsymbol{d},s} := D^{r-s-2}\delta\big(((n-s)(r-s)+2)D + r - s - 1\big) + \delta + 1,$$

en cada grupo de variables Λ_i, con la siguiente propiedad: dado $\boldsymbol{\lambda} := (\lambda_0, \ldots, \lambda_{s+1}) \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}$, si $Y_j := \lambda_j \cdot X$ para $0 \leq j \leq s+1$, $\pi : V \dashrightarrow \mathbb{P}^{s+1}$ es el morfismo lineal definido por $Y_0, \ldots, Y_{s+1}$ y $L := \{Y_0 = \cdots = Y_{s+1} = 0\} \subset \mathbb{P}^n$, entonces

i) la variedad polar $\mathsf{M}(L)$ tiene dimensión a lo sumo s,

ii) para todo $y \in \mathbb{P}^{s+1}$, la clausura Zariski de la fibra $\pi^{-1}(y)$ es equidimensional de dimensión $r-s-1$, y

iii) el conjunto de puntos excepcionales $V \cap L$ de π es no singular y equidimensional de dimensión $r-s-2$.

Demostración. Dado que $\mathcal{H}_1$ y $\mathcal{H}_2$ están definidas por polinomios en $\overline{\mathbb{F}}_q[\boldsymbol{\Lambda}]$ de grado a lo sumo $(n-s)(r-s)D^{r-s-1}\delta + 1$ y $\delta\big(D^{r-s-2}(2D + r - s - 1) + 1\big)$ en cada grupo de variables Λ_i respectivamente, se sigue que $\mathcal{H}$ está definida por un polinomio multihomogéneo en $\overline{\mathbb{F}}_q[\boldsymbol{\Lambda}]$ de grado a lo sumo $B_{\boldsymbol{d},s}$ en cada grupo de variables Λ_i. Dado $\boldsymbol{\lambda} \notin \mathcal{H}$, la condición *i)* se deduce del hecho de que $\boldsymbol{\lambda} \notin \mathcal{H}_1$ y las condiciones *ii)* y *iii)* del hecho de que $\boldsymbol{\lambda} \notin \mathcal{H}_2$. □

3.3. Primera versión efectiva del segundo teorema de Bertini

Una versión del segundo teorema de Bertini es la siguiente (ver, por ejemplo, [Sha94, §II.6.2, Theorem 2]): si $f : V_1 \to V_2$ es un morfismo dominante de variedades irreducibles definidas sobre un cuerpo de característica cero y V_1 es no singular, existe un abierto U de V_2 tal que la fibra $f^{-1}(y)$ es no singular para todo $y \in U$. En esta sección daremos una versión efectiva de este teorema válida en cualquier característica. Más precisamente, vamos a probar que, para una elección genérica de formas lineales $Y_0, \ldots, Y_{s+1}$, existe un abierto no vacío U contenido en $\mathbb{P}^{s+1}$ tal que la clausura Zariski V_y de $\pi^{-1}(y)$ es no singular para cada $y \in U$. Decimos que nuestra versión es efectiva dado que proporcionamos una cota de grado sobre la condición genérica inherente a la elección de la formas lineales $Y_0, \ldots, Y_{s+1}$ y una cota superior para el grado de la subvariedad U que contiene los puntos que definen fibras singulares. Además, esta versión es válida para variedades definidas sobre cuerpos de cualquier característica. Cabe mencionar que en [Bal03, Theorem 1] se obtiene una versión efectiva del segundo teorema de Bertini, pero la condición sobre q es exponencialmente más alta que la nuestra.

Recordemos que $V \subset \mathbb{P}^n$ es una intersección completa definida sobre $\mathbb{F}_q$ de dimensión r. Sean $F_1, \ldots, F_{n-r} \in \mathbb{F}_q[X_0, \ldots, X_n]$ polinomios homogéneos de grados $d_1 \geq \cdots \geq d_{n-r} \geq 2$ respectivamente, los cuales generan el ideal $I(V)$ de V. El grado de V es $\delta = d_1 \cdots d_{n-r}$ y $D = \sum_{i=1}^{n-r}(d_i - 1)$. Supongamos que el lugar singular Σ de V tiene dimensión a lo sumo $s \leq r-2$.

Fijamos $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}$, donde $\mathcal{H}$ es la hipersuperficie definida en la Proposición 3.2.6. Sea $\pi : V \dashrightarrow \mathbb{P}^{s+1}$ la proyección definida por las formas lineales $Y_i = \lambda_i \cdot X$, $0 \leq i \leq s+1$. Vamos a probar que existe un abierto no vacío $U \subset \mathbb{P}^{s+1}$ tal que la clausura Zariski V_y de $\pi^{-1}(y)$ es no singular para todo $y \in U$. Más aún, vamos a estimar el grado de la variedad $\mathbb{P}^{s+1} \setminus U$ que contiene a las fibras no singulares.

En primer lugar, obtenemos una condición suficiente de no singularidad de la sección lineal V_y de V definida por un punto $y \in \mathbb{P}^{s+1}$. Fijemos $y := (y_0 : \cdots : y_s) \in \mathbb{P}^{s+1}$ y supongamos sin pérdida de generalidad que $y_0 \neq 0$. Entonces

$$V_y = \big\{x \in V : y_j Y_0(x) - y_0 Y_j(x) = 0,\ 1 \leq j \leq s+1\big\}. \tag{3.16}$$

En particular, se tiene que $V \cap L \subset V_y$, donde $L = \{Y_0 = \cdots Y_{s+1} = 0\} \subset \mathbb{P}^n$.

Consideremos el morfismo lineal $\pi_x : \mathcal{T}_x V \dashrightarrow \mathbb{P}^{s+1}$ definido por $Y_0, \ldots, Y_{s+1}$, es decir, $\pi_x(v) := (\lambda_0 \cdot v : \cdots : \lambda_{s+1} \cdot v)$ con $x \in V \setminus \mathsf{E}$.

Lema 3.3.1. *Sea $y \in \mathbb{P}^{s+1}$ tal que para cada $x \in \pi^{-1}(y)$ se cumplen las siguientes condiciones:*

i) x es un punto regular de V,

ii) el conjunto de puntos excepcionales de π_x tiene dimensión a lo sumo $r-s-2$.

Entonces V_y es una variedad no singular.

Demostración. Como $\boldsymbol{\lambda} \notin \mathcal{H}$, por el Corolario 3.2.5, V_y es equidimensional de dimensión $r-s-1$. Por lo tanto, es suficiente probar que para cada $x \in V_y$ el espacio tangente $\mathcal{T}_x V_y$ tiene dimensión a lo sumo $r-s-1$. Fijemos $x \in \pi^{-1}(y)$. Por la condición (i) sabemos que el espacio tangente $\mathcal{T}_x V$ tiene dimensión r. Consideramos el morfismo lineal

$$\begin{array}{rccc} \pi_x|_{\mathcal{T}_x V_y}: & \mathcal{T}_x V_y & \dashrightarrow & \mathbb{P}^{s+1} \\ & v & \mapsto & (Y_0(v) : \cdots : Y_{s+1}(v)). \end{array}$$

Es claro que el conjunto $\mathsf{E}_{x,y}$ de puntos excepcionales de $\pi_x|_{\mathcal{T}_x V_y}$ está contenido en E_x, el conjunto de puntos excepcionales de π_x. Del hecho de que la imagen de la restricción $\pi|_{V_y}: V_y \dashrightarrow \mathbb{P}^{s+1}$ es el punto y se sigue que la dimensión de $\pi_x(\mathcal{T}_x V_y)$ es igual a cero 0. Luego, por el Teorema de la dimensión (ver, por ejemplo, [HP94a, Chapter 8, Section 1]) se tiene que

$$\dim \mathcal{T}_x V_y = \dim \mathsf{E}_{x,y} + \dim \pi_x(\mathcal{T}_x V_y) + 1.$$

De la condición (ii) deducimos que

$$\dim \mathcal{T}_x V_y \leq \dim \mathsf{E}_x + 1 \leq r-s-1.$$

Concluimos entonces que $\dim \mathcal{T}_x V_y = r-s-1$ y, por lo tanto, x es un punto regular de V_y.

Finalmente, sea $x \in V_y \setminus \pi^{-1}(y)$. Entonces $x \in V \cap L$. Teniendo en cuenta que $\boldsymbol{\lambda} \notin \mathcal{H}$, x es un punto regular de $V \cap L$. Luego, la matriz $\mathsf{M}(x, \boldsymbol{\lambda})$ definida en (3.6) tiene rango máximo. Asumimos sin pérdida de generalidad que $y_0 \neq 0$ y recordemos la definición de V_y dada en (3.16). Luego

$$\mathsf{M}'(X, \boldsymbol{\lambda}) := \begin{pmatrix} \frac{\partial F_1}{\partial X_0}(x) & \cdots & \frac{\partial F_1}{\partial X_n}(x) \\ \vdots & & \vdots \\ \frac{\partial F_{n-r}}{\partial X_0}(x) & \cdots & \frac{\partial F_{n-r}}{\partial X_n}(x) \\ y_1\lambda_{0,0} - y_0\lambda_{1,0} & \cdots & y_1\lambda_{0,n} - y_0\lambda_{1,n} \\ \vdots & & \vdots \\ y_{s+1}\lambda_{0,0} - y_0\lambda_{s+1,0} & \cdots & y_{s+1}\lambda_{0,n} - y_0\lambda_{s+1,n} \end{pmatrix} \tag{3.17}$$

tiene rango máximo y, por lo tanto, x es un punto regular de V_y. □

Observación 3.3.2. *Notar que el Lema 3.3.1 nos proporciona un criterio para determinar cuando $x \in V_y$ es un punto regular de V_y. En efecto, si x es un punto regular de V y además el conjunto de puntos excepcionales de π_x tiene dimensión a lo sumo $r-s-2$, es decir $x \notin \mathsf{M}(L)$, entonces x resulta ser un punto regular de V_y.*

De acuerdo al Lema 3.3.1, resulta esencial analizar el conjunto de puntos regulares de V para los cuales el conjunto de puntos excepcionales de π_x tiene dimensión al menos $r-s-1$. El Lema 3.1.2 asegura que dicho conjunto coincide con la variedad polar $\mathsf{M}(L)$. De aquí, las secciones lineales V_y definidas por puntos $y \in \mathbb{P}^{s+1}$ tales que $\pi^{-1}(y)$ no interseca a $\Sigma \cup \mathsf{M}(L)$ son no singulares. Nuestro próximo objetivo es mostrar que el conjunto $\Sigma \cup \mathsf{M}(L)$ está contenido en una subvariedad de V equidimensional de dimensión s y grado bajo.

Lema 3.3.3. *Para $\boldsymbol{\lambda} \notin \mathcal{H}$, existe una subvariedad $Z(L) \subset V$ equidimensional de dimensión s y grado a lo sumo $D^{r-s}\delta$ con $\mathsf{M}(L) \cup \Sigma \subset Z(L)$.*

Demostración. Para $x \in V$, se tiene que $x \in \Sigma$ si y sólo si $\dim \mathcal{T}_x V > r$, lo que es equivalente a que los gradientes $\nabla F_1(x), \ldots, \nabla F_{n-r}(x)$ sean linealmente dependientes. Esto implica que la matriz $\mathsf{M}(x, \boldsymbol{\lambda})$ de (3.6) no tiene rango máximo y, por lo tanto,

$$\Sigma \subset \{x \in V : \Delta_1(x, \boldsymbol{\lambda}) = \cdots = \Delta_N(x, \boldsymbol{\lambda}) = 0\}.$$

Por otro lado, para $x \in V_{\mathrm{sm}}$ se tiene que $x \in \mathsf{M}(L)$ si y sólo si $\Delta_1(x, \boldsymbol{\lambda}) = \cdots = \Delta_N(x, \boldsymbol{\lambda}) = 0$. Concluimos que

$$\mathsf{M}(L) \cup \Sigma = \{x \in V : \Delta_1(x, \boldsymbol{\lambda}) = \cdots = \Delta_N(x, \boldsymbol{\lambda}) = 0\}. \tag{3.18}$$

Ahora aplicamos el Lema 3.1.5 a las variedades proyectivas $\mathcal{W} := V$ y $\mathcal{W}_1 := \mathsf{M}(L) \cup \Sigma$. Como $\mathsf{M}(L) \cup \Sigma$ tiene dimensión a lo sumo s y V es equidimensional de dimensión r, por el Lema 3.1.5 concluimos que existen combinaciones lineales $\Delta^1(X, \boldsymbol{\lambda}), \ldots, \Delta^{r-s}(X, \boldsymbol{\lambda})$ de los polinomios homogéneos $\Delta_1(X, \boldsymbol{\lambda}), \ldots, \Delta_N(X, \boldsymbol{\lambda})$ de grado D tales que la variedad proyectiva $Z(L) := V \cap \{\Delta^1(X, \boldsymbol{\lambda}) = \cdots \Delta^{r-s}(X, \boldsymbol{\lambda}) = 0\}$ es equidimensional de dimensión s y contiene a $\mathsf{M}(L) \cup \Sigma$. Más aún, por la desigualdad de Bézout (2.2) se tiene que $\deg Z(L) \leq \deg(V)\, D^{r-s} = D^{r-s}\delta$. Esto completa la demostración del lema. □

Tenemos entonces la siguiente versión del segundo teorema de Bertini.

Teorema 3.3.4. *Sea $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}$, donde $\mathcal{H}$ es la hipersuperficie de $(\mathbb{P}^n)^{s+2}$ definida en la Proposición 3.2.6. Sea $Y_j := \lambda_j \cdot X$ para $0 \leq j \leq s+1$ y $L := \{Y_0 = \cdots = Y_{s+1} = 0\}$. Consideramos el morfismo lineal $\pi : V \dashrightarrow \mathbb{P}^{s+1}$ definido por $Y_0, \ldots, Y_{s+1}$. Entonces existe una variedad $W(L) \subset \mathbb{P}^{s+1}$ de dimensión a lo sumo s y grado a lo sumo $D^{r-s}\delta$ tal que, para cada $y \in \mathbb{P}^{s+1} \setminus W(L)$, la clausura Zariski V_y de $\pi^{-1}(y)$ es no singular y equidimensional de dimensión $r-s-1$.*

Demostración. Dado que $\boldsymbol{\lambda} \notin \mathcal{H}$, por la Proposición 3.2.6 la variedad polar $\mathsf{M}(L)$ tiene dimensión a lo sumo s. Sea $Z(L) \subset V$ la variedad de dimensión s y grado a lo sumo $D^{r-s}\,\delta$ cuya existencia fue demostrada en el Lema 3.3.3. Luego, se tiene que

$$\mathsf{M}(L) \cup \Sigma \subset Z(L).$$

Definimos $W(L) := \overline{\pi(Z(L))}$. Es claro que $W(L) \subset \mathbb{P}^{s+1}$ tiene dimensión a lo sumo s. Más aún, por (2.3), $W(L)$ tiene grado a lo sumo $D^{r-s}\,\delta$.

Sea $y \in \mathbb{P}^{s+1} \setminus W(L)$. Por la Proposición 3.2.6 se tiene que V_y es equidimensional de dimensión $r-s-1$. Por un lado, si $x \in \pi^{-1}(y) \subset V_y$, entonces $x \notin \Sigma \cup \mathsf{M}(L)$, con lo cual x es un punto regular de V_y pues cumple las hipótesis del Lema 3.3.1. Por otro lado, si $x \in V_y \setminus \pi^{-1}(y)$, entonces $x \in V \cap L$ y como $L \cap (\mathsf{M}(L) \cup \Sigma) = \emptyset$ nuevamente tenemos que x cumple las condiciones del Lema 3.3.1, de lo cual concluimos que es un punto regular de V_y. Esto prueba que V_y es no singular. □

Observación 3.3.5. *Observemos que, con las hipótesis y notaciones del Teorema 3.3.4, si* $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}$ *e* $y \in \mathbb{P}^{s+1} \setminus W(L)$*, entonces la sección lineal* V_y *está contenida en* V_{sm}*. En efecto, por la elección de* y *vemos que* x *es un punto regular de* V *para todo* $x \in \pi^{-1}(y)$*. Por otro lado, si* $x \in V_y \setminus \pi^{-1}(y)$*, entonces* $x \in V \cap L$*. Como* $\boldsymbol{\lambda} \notin \mathcal{H}_2''$*, donde* $\mathcal{H}_2''$ *es la hipersuperficie definida en el Lema 3.2.2, deducimos que* $V \cap L \subset V_{\mathrm{sm}}$*. Por lo tanto* x *es un punto regular de* V*.*

Dado que cada sección lineal V_y con $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}$ e $y \in \mathbb{P}^{s+1} \setminus W(L)$ es una intersección completa proyectiva no singular, por el Teorema 2.1.4 se tiene que V_y es absolutamente irreducible.

Finalmente, damos una condición sobre q que asegura la existencia de una sección lineal no singular de V definida sobre $\mathbb{F}_q$.

Corolario 3.3.6. *Sea* $q > \max\{B_{\boldsymbol{d},s}, D^{r-s}\delta\}$*. Existe* $y \in \mathbb{P}^{s+1}(\mathbb{F}_q)$ *tal que* V_y *es una* $\mathbb{F}_q$*-variedad no singular equidimensional de dimensión* $r-s-1$ *y está contenida en* V_{sm}*.*

Demostración. Por el Corolario 2.3.13 concluimos que, si $q > B_{\boldsymbol{d},s}$, entonces existe un punto $\boldsymbol{\lambda} \in (\mathbb{P}^n(\mathbb{F}_q))^{s+2} \setminus \mathcal{H}$. Sea $\pi : V \dashrightarrow \mathbb{P}^{s+1}$ el morfismo lineal definido por las correspondientes formas lineales $Y_0 = \lambda_0 \cdot X, , \ldots, Y_{s+1} = \lambda_{s+1} \cdot X$. Luego π está definido sobre $\mathbb{F}_q$. Por el Teorema 3.3.4 existe una variedad $W(L) \subset \mathbb{P}^{s+1}$ de grado a lo sumo $D^{r-s}\delta$ tal que, para $y \in \mathbb{P}^{s+1} \setminus W(L)$, la sección lineal V_y es no singular, equidimensional de dimensión $r-s-1$. Además, la Observación 3.3.5 prueba que $V_y \subset V_{\mathrm{sm}}$. Como $q > D^{r-s}\delta$, se tiene que existe $y \in \mathbb{P}^{s+1}(\mathbb{F}_q) \setminus W(L)$ a partir de lo cual se sigue el corolario. □

3.4. Segunda versión efectiva del segundo teorema de Bertini

Como mencionamos al comienzo del capítulo, los teoremas de Bertini nos permitirán obtener estimaciones y resultados de existencia de puntos q-racionales de intersecciones completas singulares. En particular, a partir de la versión de dicho teorema que dimos en la sección anterior, en el Capítulo 4 obtendremos estimaciones para intersecciones completas singulares cuyo lugar singular tiene codimensión al menos dos o al menos tres. Sin embargo, si disponemos de cotas más precisas de la dimensión del lugar singular de la variedad en cuestión, nos gustaría "sacar provecho" de esa información, es decir, obtener mejores estimaciones que las que hemos obtenido para variedades que son regulares en codimensión uno o dos. Para esto, en el Capítulo 4 damos una versión explícita de la estimación de Hooley. Con este objetivo, proporcionamos otra versión efectiva del segundo teorema de Bertini. La diferencia con la versión anterior es que, en lugar de considerar las secciones lineales que definen la clausura Zariski de las fibras de una proyección lineal sobre $\mathbb{P}^{s+1}$, vamos a analizar cuando una variedad lineal de codimensión $s+1$ define una sección lineal no singular de la variedad en consideración.

Al igual que en todo el capítulo, consideramos una $\mathbb{F}_q$-intersección completa $V \subset \mathbb{P}^n$ de dimensión r, grado δ, multigrado $\boldsymbol{d} = (d_1, \ldots, d_{n-r})$, $d_1 \geq \cdots d_{n-r} \geq 2$, y la dimensión del lugar singular Σ es a lo sumo s con $0 \leq s \leq r-2$.

Nuestro objetivo es probar que existe una hipersuperficie $\mathcal{H} \subset (\mathbb{P}^n)^{s+1}$ con la propiedad de que, si $\boldsymbol{\gamma} := (\gamma_0, \ldots, \gamma_s) \in (\mathbb{P}^n)^{s+1} \setminus \mathcal{H}$, entonces la variedad lineal $\mathcal{L}$ definida por las ecuaciones $\gamma_i \cdot X = 0$, $0 \leq i \leq s$, verifica que $V \cap \mathcal{L}$ es una sección lineal no singular de V de dimensión $r-s-1$.

Comenzamos con el siguiente lema técnico. Sea $\boldsymbol{\lambda} := (\lambda_0, \ldots, \lambda_{s+1}) \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}_2$, donde $\mathcal{H}_2$ es la hipersuperficie definida en el Corolario 3.2.5. Sea L la variedad lineal definida por $\lambda_i \cdot X = 0$, $0 \leq i \leq s+1$. Entonces $V \cap L$ es equidimensional de dimensión $r-s-2$ y $L \cap (\mathsf{M}(L) \cup \Sigma) = \emptyset$. Consideramos la proyección lineal $\pi : V \dashrightarrow \mathbb{P}^{s+1}$ definida por $\lambda_i \cdot X$ para $0 \leq i \leq s+1$ y denotamos por V_y la clausura Zariski de la fibra $\pi^{-1}(y)$ para todo $y \in \mathbb{P}^{s+1}$. Vimos que $V_y = (V \cap L) \cup \pi^{-1}(y)$ y, suponiendo que la coordenada $y_0 \neq 0$, V_y está dada por las ecuaciones (3.16).

Lema 3.4.1. *Con las notaciones y definiciones precedentes, si $y \in \pi(\mathsf{M}(L)) \cup \Sigma)$, entonces $\dim \Sigma_y = 0$, donde Σ_y es el conjunto de puntos singulares de V_y.*

Demostración. De acuerdo con la Observación 3.3.2, si $x \in V_y \setminus (\Sigma \cup \mathsf{M}(L))$, entonces x es un punto regular de V_y, con lo cual $\Sigma_y \subset V_y \cap (\Sigma \cup \mathsf{M}(L))$. En particular, como $L \cap (\Sigma \cap \mathsf{M}(L)) = \emptyset$, resulta $\Sigma_y \subset \pi^{-1}(y) \cap (\Sigma \cup \mathsf{M}(L))$.

Por otro lado, como $L = \{Y_0 = \cdots = Y_{s+1} = 0\}$, $\pi : V \dashrightarrow \mathbb{P}^{s+1}$ es el morfismo lineal definido por $Y_0, \ldots, Y_{s+1}$ y $L \cap (\Sigma \cup \mathsf{M}(L)) = \emptyset$, de acuerdo a [Sha94, §I.5, Theorem 8] tenemos que la restricción $\pi|_{\Sigma \cup \mathsf{M}(L)} : \Sigma \cup \mathsf{M}(L) \dashrightarrow \pi(\Sigma \cup \mathsf{M}(L))$ es un morfismo finito. En particular, si $y \in \pi(\Sigma \cup \mathsf{M}(L))$, entonces $\dim \pi^{-1}(y) \cap (\Sigma \cup \mathsf{M}(L)) = 0$. Esto concluye la demostración del lema. □

Con el objetivo de mostrar la existencia de una hipersuperficie $\mathcal{H} \subset (\mathbb{P}^n)^{s+1}$ que contiene al conjunto de variedades lineales de codimensión $s+1$ que no definen secciones lineales no singulares de V, de forma similar a lo que hicimos en la Sección 3.2, vamos a considerar la siguiente variedad de incidencia

$$\begin{aligned} \mathcal{W} := (V_{\mathrm{sm}} \times \mathcal{U}') \cap \{&\Gamma_0 \cdot X = 0, \ldots, \Gamma_s \cdot X = 0, \\ &\Delta_1(\boldsymbol{\Gamma}, X) = 0, \ldots, \Delta_m(\boldsymbol{\Gamma}, X) = 0\}, \end{aligned}$$

donde $\mathcal{U}' \subset (\mathbb{P}^n)^{s+1}$ es el abierto Zariski de las matrices de tamaño $(s+1) \times (n+1)$ de rango máximo y $\Delta_1, \ldots, \Delta_m$ son los menores maximales de la matriz

$$\mathcal{M}(X, \boldsymbol{\Gamma}) := \begin{pmatrix} \frac{\partial F_1}{\partial X_0} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_{n-r}}{\partial X_0} & \cdots & \frac{\partial F_{n-r}}{\partial X_n} \\ \Gamma_{0,0} & \cdots & \Gamma_{0,n} \\ \vdots & & \vdots \\ \Gamma_{s,0} & \cdots & \Gamma_{s,n} \end{pmatrix}. \tag{3.19}$$

De manera análoga a la demostración de la Proposición 3.2.3 obtenemos el siguiente resultado, cuya demostración sólo vamos a esbozar.

Proposición 3.4.2. *Sea $l := n(s+1)$. Entonces $\mathcal{W}$ es una subvariedad irreducible de $V_{\mathrm{sm}} \times \mathcal{U}'$ de dimensión $l-1$.*

Demostración. Consideramos el morfismo lineal $\pi_1 : \mathcal{W} \to V_{\mathrm{sm}}$ definido por $\pi_1(x, \boldsymbol{\gamma}) := x$. Dado $x \in V_{\mathrm{sm}}$ fijo, se tiene que la fibra $\pi_1^{-1}(x) = \{x\} \times \Omega$, donde $\Omega \subset \mathcal{U}'$ es el conjunto de matrices $\boldsymbol{\gamma} := (\gamma_0, \ldots, \gamma_s)$ tales que $\gamma_i \cdot x = 0$ para $1 \leq i \leq s$ y la matriz $\mathcal{M}(x, \boldsymbol{\gamma})$ dada en (3.19) no tiene rango máximo. Luego, siguiendo la demostración de la Proposición 3.2.3, obtenemos que $\mathcal{C}(\Omega)$ el cono afín de Ω es, módulo $\big(\nabla F_1(x), \ldots, \nabla F_{n-r}(x)\big)$, isomorfo al abierto Zariski $L'_s(\mathbb{A}^{s+1}, \mathbb{W}) \cap \Phi(\mathcal{U}'_{\mathrm{aff}})$ de $L'_s(\mathbb{A}^{s+1}, \mathbb{W})$, donde

$$L'_s(\mathbb{A}^{s+1}, \mathbb{W}) := \{f \in \mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+1}, \mathbb{V}) : \mathrm{rg}(f) \leq s\},$$

$\mathbb{V}$ y $\mathbb{W}$ son los espacios lineales definidos en la Proposición 3.2.3, $\mathcal{U}'_{\mathrm{aff}} \subset (\mathbb{A}^{n+1})^{s+1}$ es el cono afín de $\mathcal{U}'$ y $\Phi : \mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+1}, \mathbb{A}^{n+1}) \to \mathrm{Hom}_{\overline{\mathbb{F}}_q}(\mathbb{A}^{s+1}, \mathbb{W})$ es el morfismo suryectivo inducido por la función cociente $\mathbb{A}^{n+1} \to \mathbb{W}$.

Por [BV88, Proposition 1.1], $L'_s(\mathbb{A}^{s+1}, \mathbb{W})$ es una variedad irreducible de dimensión $s(r+1)$ y, como estamos considerando subespacios de $\mathbb{V}$ de dimensión $s+1$ módulo $\big(\nabla F_1(x), \ldots, \nabla F_{n-r}(x)\big)$, cuya dimensión es $n-r$ pues $x \in V_{\mathrm{sm}}$, deducimos que el cono afín de $\pi_1^{-1}(x) = \{x\} \times \Omega$ es un subconjunto abierto y denso de una variedad irreducible de $V_{\mathrm{sm}} \times \mathcal{U}'_{\mathrm{aff}}$ de dimensión $s(r+1) + (n-r)(s+1) = l + s - r$. Esto implica que $\pi_1^{-1}(x) = \{x\} \times \Omega$ es una variedad irreducible de $V_{\mathrm{sm}} \times \mathcal{U}'$ de dimensión $l - r - 1$. El mismo argumento de la demostración de la Proposición 3.2.3, muestra que $\mathcal{W}$ es una subvariedad irreducible de $V_{\mathrm{sm}} \times \mathcal{U}'$ irreducible de dimensión $l-1$. □

Consideramos la proyección $\pi_2 : \mathcal{W} \to \mathcal{U}'$ dada por $\pi_2(x, \boldsymbol{\gamma}) := \boldsymbol{\gamma}$ y definimos $\mathcal{H}_1$ como la clausura Zariski de la imagen de dicha proyección. Por la Proposición 3.4.2 se tiene que $\mathcal{H}_1$ es una variedad irreducible de dimensión a lo sumo $n(s+1)-1$. El siguiente resultado nos proporciona información más precisa sobre $\mathcal{H}_1$.

Teorema 3.4.3. *$\mathcal{H}_1$ es una hipersuperficie de $(\mathbb{P}^n)^{s+1}$, definida por un polinomio multihomogéneo en $\overline{\mathbb{F}}_q[\boldsymbol{\Gamma}]$ de grado a lo sumo $\delta D^{r-s-1}(D+r-s)$ en cada grupo de variables Γ_i para $0 \leq i \leq s$.*

Demostración. En primer lugar probamos que $\mathcal{H}_1$ es una hipersuperficie. Para esto, nuevamente teniendo en cuenta el teorema de la dimensión de las fibras (ver, por ejemplo, [Sha94, §I.6, Theorem 7]), alcanza con mostrar que existe una fibra de π_2 de dimensión cero.

Fijemos $\boldsymbol{\lambda} := (\lambda_0, \ldots, \lambda_{s+1}) \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}_2$, donde $\mathcal{H}_2$ es la hipersuperficie definida en el Corolario 3.2.5, y sea L la variedad lineal de dimensión $n-s-2$ definida en (3.1). En particular, tenemos que $L \cap (\mathsf{M}(L) \cup \Sigma) = \emptyset$. Por último, fijemos $y \in \pi(\Sigma \cup \mathsf{M}(L))$. El Lema 3.4.1 asegura que el lugar singular Σ_y de V_y tiene dimensión 0. Definimos $\boldsymbol{\gamma} := (\gamma_0, \ldots, \gamma_s) \in (\mathbb{P}^n)^{s+1}$ como el elemento cuya j-ésima coordenada corresponde al vector de coeficientes de la j-ésima forma lineal en (3.16), es decir, $\gamma_j = y_j \boldsymbol{\lambda}_0 - y_0 \boldsymbol{\lambda}_j$ para $1 \leq j \leq s+1$. Observemos que $\pi_2^{-1}(\boldsymbol{\gamma})$ es isomorfo al conjunto de puntos $x \in V_{\mathrm{sm}} \cap V_y$ tales que $\mathcal{M}(x, \boldsymbol{\gamma})$ no tiene rango

máximo. Como $\mathcal{M}(X, \boldsymbol{\gamma})$ coincide con la matriz $\mathsf{M}'(X, \boldsymbol{\lambda})$ de (3.17), deducimos que $\pi_2^{-1}(\boldsymbol{\gamma}) \subset \mathsf{M}(L) \cap V_y$. Por otro lado, por el Lema 3.4.1, vemos que $\mathsf{M}(L) \cap V_y \subset \Sigma_y$. Dado que $\dim \Sigma_y = 0$, se obtiene que $\pi_2^{-1}(\boldsymbol{\gamma})$ es una fibra de dimensión cero de π_2.

A continuación vamos a calcular una cota del multigrado del polinomio que define a la hipersuperficie $\mathcal{H}_1$. Para ello mostramos la existencia de una variedad $\mathcal{W}' \subset (\mathbb{P}^n)^{s+2}$ equidimensional de dimensión $l-1$ y grado "bajo" que contiene a $\mathcal{W}$ de manera análoga a lo hecho en la demostración del Teorema 3.2.4.

Afirmación. *Existen combinaciones lineales $\Delta^1, \ldots, \Delta^{r-s}$ de los polinomios $\Delta_1(\boldsymbol{\Gamma}, X)$, $\Delta_2(\boldsymbol{\Gamma}, X), \ldots, \Delta_N(\boldsymbol{\Gamma}, X)$ tales que la subvariedad $\mathcal{W}' \subset (\mathbb{P}^n)^{s+2}$ definida por los ceros comunes de las ecuaciones*

$$\begin{aligned} F_1 = 0, \ldots, F_{n-r} = 0, \Gamma_0 \cdot X = 0, \ldots, \Gamma_s \cdot X = 0, \\ \Delta^1(\boldsymbol{\Gamma}, X) = 0, \ldots, \Delta^{r-s}(\boldsymbol{\Gamma}, X) = 0, \end{aligned} \tag{3.20}$$

es equidimensional de dimensión $l-1$.

Demostración. Sea $L_\Gamma := \{\Gamma_0 \cdot X = 0, \ldots, \Gamma_s \cdot X = 0\} \subset \mathbb{P}^n \times (\mathbb{P}^n)^{s+1}$ y sea $\mathcal{W}'' \subset (\mathbb{P}^n)^{s+2}$ la siguiente variedad:

$$\mathcal{W}'' := \mathcal{W} \cup \big((\Sigma \times (\mathbb{P}^n)^{s+1}) \cap L_\Gamma\big) \cup \big((V \times ((\mathbb{P}^n)^{s+1} \setminus \mathcal{U}') \cap L_\Gamma\big).$$

Se tiene que

$$W'' = (V \times (\mathbb{P}^n)^{s+1}) \cap L_\Gamma \cap \{\Delta_1(\boldsymbol{\Gamma}, X) = 0, \ldots, \Delta_m(\boldsymbol{\Gamma}, X) = 0\}. \tag{3.21}$$

En efecto, si $(x, \boldsymbol{\gamma}) \in V \times (\mathbb{P}^n)^{s+1} \cap L_\Gamma$ se tienen las siguientes tres posibilidades: $x \in \Sigma$, $\boldsymbol{\gamma} \in (\mathbb{P}^n)^{s+1} \setminus \mathcal{U}'$, o $(x, \gamma) \in V_{\mathrm{sm}} \times \mathcal{U}'$. En los dos primeros casos, $(x, \boldsymbol{\gamma}) \in \mathcal{W}''$ y $\Delta_j(x, \boldsymbol{\gamma}) = 0$ para todo $1 \leq j \leq m$. En el último caso se tiene que $(x, \boldsymbol{\gamma}) \in \mathcal{W}''$ si y solo si $\Delta_j(x, \boldsymbol{\gamma}) = 0$ para todo $1 \leq j \leq m$. Esto muestra (3.21).

Determinamos la dimensión de $\mathcal{W}''$. Primero observemos que $\Sigma \times (\mathbb{P}^n)^{s+1}$ es un cilindro cuya intersección con las ecuaciones $\Gamma_0 \cdot X = 0, \ldots, \Gamma_s \cdot X = 0$ tiene codimensión $s+1$ en $\Sigma \times (\mathbb{P}^n)^{s+1}$. Por lo tanto, la dimensión de $(\Sigma \times (\mathbb{P}^n)^{s+1}) \cap L_\Gamma$ es a lo sumo $s + l - (s+1) = l - 1$. Por otro lado, el cono afín de $(\mathbb{P}^n)^{s+1} \setminus \mathcal{U}'$ es el cerrado de las matrices de rango a lo sumo s, es decir, $L_s(\mathbb{A}^{s+1}, \mathbb{A}^{n+1})$. Por [BV88, Proposition 1.1] la dimensión de $L_s(\mathbb{A}^{s+1}, \mathbb{A}^{n+1})$ es $s(n+2)$ y, por lo tanto, la dimensión de $(\mathbb{P}^n)^{s+1} \setminus \mathcal{U}'$ es $s(n+1)-1 = l+s-n-1$. Luego, $V \times (\mathbb{P}^n)^{s+1} \setminus \mathcal{U}'$ tiene dimensión $r + l + s - n - 1$. Consideremos la proyección en la segunda coordenada $\pi_2 : \big(V \times ((\mathbb{P}^n)^{s+1} \setminus \mathcal{U}')\big) \cap L_\Gamma \to (\mathbb{P}^n)^{s+1} \setminus \mathcal{U}'$. Una variedad lineal genérica de $\mathbb{P}^n$ de codimensión s interseca a V en una variedad equidimensional de dimensión $r - s$. Por lo tanto, una fibra genérica $\pi_2^{-1}(\boldsymbol{\gamma})$ tiene dimensión $r - s$. Luego, el Teorema de la dimensión de las fibras muestra que

$$r - s = \dim \pi_2^{-1}(\boldsymbol{\gamma}) \geq \dim \big(V \times ((\mathbb{P}^n)^{s+1} \setminus \mathcal{U}') \cap L_\Gamma\big) - (l + s - n - 1).$$

Deducimos que $\big(V \times ((\mathbb{P}^n)^{s+1} \setminus \mathcal{U}')\big) \cap L_\Gamma$ tiene dimensión a lo sumo $l - n + r - 1 < l - 1$. Combinando estos hechos con la Proposición 3.4.2, concluimos que $\mathcal{W}''$ tiene dimensión $l - 1$.

Ahora aplicamos el Lema 3.1.5 a las variedades $\mathcal{W} := \big(V \times (\mathbb{P}^n)^{s+1}\big) \cap L_\Gamma$ y $\mathcal{W}_1 := \mathcal{W}''$. Del Lema 3.1.5 se deduce fácilmente la afirmación. □

Sea $\mathcal{H}_1'$ la unión de las componentes de la clausura Zariski de $\pi_2(\mathcal{W}')$ de dimensión $l-1$. Luego $\mathcal{H}_1'$ es una hipersuperficie que contiene a $\mathcal{H}_1$. Estimamos entonces el multigrado de $\mathcal{H}_1'$. Consideremos $[\mathcal{W}']$ la clase de $\mathcal{W}'$ en el anillo de Chow $\mathcal{A}^*((\mathbb{P}^n)^{s+2})$ de $(\mathbb{P}^n)^{s+2}$. Sea θ_{j-2} la clase de la imagen inversa de un hiperplano de $\mathbb{P}^n$ por la j-ésima proyección canónica $(\mathbb{P}^n)^{s+2} \to \mathbb{P}^n$ for $1 \leq j \leq s+1$. Por el Teorema de Bézout multiproyectivo (2.6) se obtiene que

$$\begin{aligned}[\mathcal{W}'] &\leq \prod_{i=1}^{n-r}(d_i\theta_{-1}) \prod_{j=0}^{s}(\theta_{-1}+\theta_j) \prod_{k=1}^{r-s}(D\theta_{-1}+\theta_0+\cdots+\theta_s) \\ &\leq \delta D^{r-s-1}(D+r-s)(\theta_{-1})^n(\theta_0+\cdots+\theta_s) \\ &\quad + \text{términos de grado menor en } \theta_{-1}.\end{aligned}$$

Por otra parte, $[\mathcal{H}_1'] = \deg_X F\theta_{-1} + \deg_{\Gamma_0} F\,\theta_0 + \cdots + \deg_{\Gamma_s} F\,\theta_s$, donde $F \in \mathbb{F}_q[\Gamma]$ es un polinomio de grado mínimo que define a $\mathcal{H}_1'$. Sea $\jmath : \mathcal{A}^*\big((\mathbb{P}^n)^{s+1}\big) \hookrightarrow A^*\big((\mathbb{P}^n)^{s+2}\big)$, $P \mapsto (\theta_{-1})^n P$ el morfismo $\mathbb{Z}$–lineal que induce π_2. Entonces (2.6) prueba que $\jmath([\mathcal{H}_1']) \leq [\mathcal{W}']$. Esto implica que $\deg_{\Gamma_j} F \leq \delta D^{r-s-1}(D+r-s)$ para $0 \leq j \leq s$, lo que concluye la demostración del teorema. □

Dado que estamos interesados en determinar condiciones para que una variedad lineal de dimensión $n-s-1$ defina una sección no singular de V, resulta necesario que dichas secciones lineales no corten al lugar singular de V. Por el Lema 3.2.2 existe una hipersuperficie $\mathcal{H}_2 \subset (\mathbb{P}^n)^{s+1}$, definida por un polinomio multihomogéneo en $\overline{\mathbb{F}}_q[\mathbf{\Gamma}]$ de grado a lo sumo δD^{r-s-1} en cada grupo de variables Γ_i, $0 \leq i \leq s$ con la propiedad de que si $\boldsymbol{\gamma} \in (\mathbb{P}^n)^{s+1} \setminus \mathcal{H}_2$, entonces la variedad lineal $\mathcal{L}$ definida por $\boldsymbol{\gamma}$ no interseca al conjunto de punto singulares de V.

Con todo esto estamos en condiciones de definir una hipersuperficie $\mathcal{H}$ con las propiedades que mencionamos anteriormente.

Corolario 3.4.4. *Existe una hipersuperficie $\mathcal{H} \subset (\mathbb{P}^n)^{s+1}$, definida por un polinomio multihomogéneo de grado a lo sumo $D^{r-s-1}\delta(D+r-s+1)$ en cada grupo de variables Γ_i, con la siguiente propiedad: si $\boldsymbol{\gamma} \in (\mathbb{P}^n)^{s+1} \setminus \mathcal{H}$, entonces $V \cap \mathcal{L}$ es no singular y equidimensional de dimensión $r-s-1$.*

Demostración. Dadas las hipersuperficies $\mathcal{H}_1$ y $\mathcal{H}_2$ definidas en los párrafos anteriores, consideremos $\mathcal{H} = \mathcal{H}_1 \cup \mathcal{H}_2$. Sea $\boldsymbol{\gamma} \in (\mathbb{P}^n)^{s+1} \setminus \mathcal{H}$. Afirmamos que $V \cap \mathcal{L}$ es no singular. En efecto, supongamos que existe un punto singular x de $V \cap \mathcal{L}$. Como $\Sigma \cap \mathcal{L} = \emptyset$, por (3.4) se tiene que $x \in V_{\text{sm}}$ y que V y $\mathcal{L}$ no se cortan transversalmente en x. Luego, la matriz $\mathcal{M}(x, \boldsymbol{\gamma})$ definida en (3.19) no tiene rango máximo y, por lo tanto, $(x, \boldsymbol{\gamma}) \in \mathcal{W}$. Esto contradice que $\boldsymbol{\gamma} \notin \mathcal{H}_1$ y se sigue que $V \cap \mathcal{L}$ es no singular.

Probemos ahora que $V \cap \mathcal{L}$ tiene dimensión $r-s-1$. Por [Sha94, §I.6.2, Corollary 5] sabemos que la dimensión de $V \cap \mathcal{L}$ es al menos $r-s-1$. Por otro lado, como $\Sigma \cap \mathcal{L} = \emptyset$, entonces $V \cap \mathcal{L} = V_{\text{sm}} \cap \mathcal{L}$. Sea $x \in V_{\text{sm}} \cap \mathcal{L}$. Como $\boldsymbol{\gamma} \notin \mathcal{H}_1$, entonces $(x, \boldsymbol{\gamma}) \notin \mathcal{W}$ y, por lo tanto, la matriz $\mathcal{M}(x, \boldsymbol{\gamma})$ tiene rango máximo. De esto se deduce que $\dim(\mathcal{T}_x(V \cap \mathcal{L})) \leq r-s-1$, lo que en particular implica que la dimensión de $V \cap \mathcal{L}$ es a lo sumo $r-s-1$. □

Finalmente, resta considerar la existencia de elementos $\gamma \in (\mathbb{P}^n(\mathbb{F}_q))^{s+1} \setminus \mathcal{H}$. De acuerdo al Corolario 2.3.13, existe un tal elemento $\boldsymbol{\gamma}$ si $q > D^{r-s-1}\delta(D+r-s+1)$.

Obtenemos así la segunda versión efectiva del segundo teorema de Bertini.

Teorema 3.4.5. *Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r, multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$, grado δ, cuyo lugar singular tiene dimensión a lo sumo s con $0 \leq s \leq r-2$. Sea $D := \sum_{i=1}^{n-r}(d_i - 1)$. Si $q > D^{r-s-1}\delta(D+r-s+1)$, entonces existe una variedad lineal $\mathcal{L} \subset \mathbb{P}^n$ definida sobre $\mathbb{F}_q$ de dimensión $n-s-1$ tal que $V \cap \mathcal{L}$ es una sección lineal no singular de V definida sobre $\mathbb{F}_q$ de dimensión $r-s-1$.*

Capítulo 4

Estimaciones y resultados de existencia

En este capítulo presentaremos algunas estimaciones y resultados de existencia de puntos q-racionales regulares de intersecciones completas singulares. Proporcionaremos estimaciones para intersecciones completas normales (es decir, intersecciones completas cuyo lugar singular tiene codimensión al menos dos) y para intersecciones completas que verifican que la codimensión del lugar singular es al menos tres. Finalmente, obtendremos una estimación para el caso en que la dimensión del lugar singular es arbitraria, que constituye una versión explícita de la estimación de Hooley [Hoo91].

4.1. Resultados de existencia

Se conocen pocos resultados sobre la cantidad exacta de puntos q-racionales de $\mathbb{F}_q$-variedades. Los resultados existentes son fundamentalmente de dos tipos: resultados para variedades particulares (por ejemplo, hipersuperficies definidas por cierto tipo de ecuaciones "diagonales", formas cuadráticas, etc.; ver, por ejemplo, [LN83, Chapter 6]) o resultados sobre funciones zeta de Riemann. En cuanto al primer tipo de resultados, su aplicabilidad queda naturalmente restringida a la clase particular de variedades en consideración. Por otro lado, el cálculo de las funciones zeta de Riemann es sumamente dificultoso (ver [Wan08]). Por estos motivos, frecuentemente resulta necesario disponer de estimaciones o resultados que aseguren la existencia de puntos q-racionales en variedades sobre cuerpos finitos. Comenzamos entonces este capítulo proporcionando resultados que garantizan la existencia de puntos q-racionales. Posteriormente, probaremos la existencia de puntos q-racionales regulares de la variedad.

Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r, grado δ, multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ con $d_1 \geq \cdots \geq d_{n-r} \geq 2$ y lugar singular Σ de dimensión a lo sumo $s \leq r-2$. Recordemos que V_{sm} denota el conjunto de puntos regulares de V. Vamos a establecer condiciones sobre q que garanticen que $V_{\mathrm{sm}}(\mathbb{F}_q)$ es no vacío. Usualmente este tipo de resultados se obtienen combinando

estimaciones sobre el número de puntos q-racionales de la variedad en consideración y cotas superiores para el número de puntos q-racionales singulares. Nosotros en cambio vamos a utilizar nuestra versión efectiva del segundo teorema de Bertini (Teorema 3.3.4) a fin de probar que existe una sección lineal de V definida sobre $\mathbb{F}_q$ contenida en V_{sm}, para luego aplicar la conocida estimación de Deligne [Del74] sobre la cantidad de puntos q-racionales: dada una intersección completa no singular $V \subset \mathbb{P}^n$ definida sobre $\mathbb{F}_q$, de dimensión r, grado δ y multigrado $\boldsymbol{d}$, se tiene

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_r(n, \boldsymbol{d})\, q^{r/2}, \tag{4.1}$$

donde $p_r = |\mathbb{P}^r(\mathbb{F}_q)|$ y $b'_r(n, \boldsymbol{d})$ denota el r-ésimo número de Betti primitivo de una intersección completa no singular contenida en $\mathbb{P}^n$ de dimensión r y multigrado $\boldsymbol{d}$.

Los números primitivos de Betti son ciertos invariantes asociados a espacios de cohomología étale ℓ-ádica (ver, por ejemplo, [Mil80]). Existen fórmulas explícitas para los mismos; de hecho, de acuerdo a, por ejemplo, [GL02a, Theorem 4.1], tenemos que el r-ésimo número primitivo de Betti de una intersección completa no singular en $\mathbb{P}^n$ de dimensión r y multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ es

$$b_r(n, \boldsymbol{d}) = (-1)^{r+1}(r+1) + (-1)^n + \sum_{c=n-r}^{n} (-1)^c \binom{n+1}{c+1} \sum_{\boldsymbol{v} \in M(c)} \boldsymbol{d}^{\boldsymbol{v}},$$

donde para $c \geq 1$, $M(c) = \{(v_1, \ldots, v_{n-r}) \in \mathbb{N}^{n-r} : \ v_1 + \cdots + v_{n-r} = c, \ v_i \geq 1, \ 1 \leq i \leq n-r\}$ y $\boldsymbol{d}^{\boldsymbol{v}} := d_1^{v_1} \cdots d_{n-r}^{v_{n-r}}$. Sin embargo, esta fórmula puede resultar compleja, y por lo tanto es útil disponer de cotas de tales números. Dada una intersección completa no singular en $\mathbb{P}^n$ de dimensión r, grado δ y multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$, si $d := \max\{d_1, \ldots, d_{n-r}\}$, entonces se tiene la siguiente cota superior (ver, por ejemplo, [GL02a, Proposition 4.2]):

$$b'_r(n, \boldsymbol{d}) \leq (-1)^{r+1}(r+1) + \delta \binom{n+1}{r} (d+1)^r.$$

En lo que sigue, usaremos frecuentemente las siguientes expresiones explícitas para $b'_r(n, \boldsymbol{d})$ con $r \in \{1, 2\}$ (ver, por ejemplo, [GL02a, Example 4.3]):

$$b'_1(n, \boldsymbol{d}) = (d_1 \cdots d_{n-1})(d_1 + \cdots + d_{n-1} - n - 1) + 2,$$
$$b'_2(n, \boldsymbol{d}) = (d_1 \cdots d_{n-2}) \left(\binom{n+1}{2} - (n+1) \sum_{1 \leq i \leq n-2} d_i + \sum_{1 \leq i \leq j \leq n-2} d_i d_j \right) - 3.$$

Observación 4.1.1. *Sea $V \subset \mathbb{P}^n$ una intersección completa no singular definida sobre $\mathbb{F}_q$ de dimensión 2, grado δ y multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-2})$. Sea $D := \sum_{i=1}^{n-2}(d_i - 1)$. Observamos que $\delta = d_1 \cdots d_{n-2}$ y se tiene la siguiente desigualdad:*

$$b'_2(n, \boldsymbol{d}) \leq (n-1) D^2 \deg V. \tag{4.2}$$

En efecto, se tiene que

$$-(n+1) \sum_{1 \leq i \leq n-2} d_i + \sum_{1 \leq i \leq j \leq n-2} d_i d_j \leq \sum_{i=1}^{n-2} d_i \left(\sum_{i=1}^{n-2} d_i - n - 1 \right) = \sum_{i=1}^{n-2} d_i (D - 3).$$

Teniendo en cuenta que $\sum_{i=1}^{n-2} d_i \leq (n-1)D$, *se obtiene*

$$b_2'(n, \boldsymbol{d}) \leq \deg V \left(\binom{n+1}{2} + (n-1)D(D-3) \right) \leq (n-1)D^2 \deg V,$$

lo que prueba (4.2).

Sea $B_{\boldsymbol{d},s} := D^{r-s-2}\delta\big(((n-s)(r-s)+2)D + r - s - 1\big) + \delta + 1$. De acuerdo con el Corolario 3.3.6 y la Observación 3.3.5, si $q > \text{máx}\{B_{\boldsymbol{d},s}, D^{r-s}\delta\}$, entonces existe una sección lineal S de V no singular, definida sobre $\mathbb{F}_q$, equidimensional de dimensión $r-s-1$, que está contenida en V_{sm}. Vamos a mostrar que, imponiendo cierta condición adicional sobre q, el número de puntos q-racionales en S es estrictamente positivo, lo que prueba que V tiene puntos regulares q-racionales.

Teorema 4.1.2. *Sea* $V \subset \mathbb{P}^n$ *una intersección completa definida sobre* $\mathbb{F}_q$, *de dimensión* $r \geq 2$, *grado* δ, *multigrado* $\boldsymbol{d}$ *y lugar singular* Σ *de dimensión a lo sumo* $s \leq r-2$. *Si* $q > \text{máx}\left\{B_{\boldsymbol{d},s}, D^{r-s}\delta, \big(b'_{r-s-1}(n-s-1, \boldsymbol{d})\big)^{2/(r-s-1)}\right\}$, *entonces* V *tiene un punto regular* q*-racional.*

Demostración. El Corolario 3.3.6 asegura que existe una sección lineal S de V no singular. Dado que S es una intersección completa no singular definida sobre $\mathbb{F}_q$ de dimensión $r-s-1$, por (4.1) se tiene

$$|S(\mathbb{F}_q)| \geq p_{r-s-1} - b' q^{\frac{r-s-1}{2}} > q^{\frac{r-s-1}{2}}\big(q^{\frac{r-s-1}{2}} - b'\big),$$

donde $b' := b'_{r-s-1}(n-s-1, \boldsymbol{d})$. Si q satisface las condiciones del enunciado del teorema, el lado derecho de la expresión de arriba es positivo. Más aún, teniendo en cuenta la Observación 3.3.5 vemos que $S \subset V_{\text{sm}}$, lo que concluye la demostración del teorema. □

A continuación damos un resultado de existencia para dos casos particulares de intersecciones completas.

Corolario 4.1.3. *Bajo las hipótesis del Teorema 4.1.2, si*

$$q > \begin{cases} \big(\delta(D-2)+2\big)^2, & \text{para } D \geq 5 \text{ o } D = 4 \text{ y } n - r > 1 \\ \big(2(n-r+3)D + 2\big)\delta + 1, & \text{en los demás casos,} \end{cases}$$

entonces V *tiene un punto regular* q*-racional.*

Demostración. Observamos que $b'_1(n-r+1, \boldsymbol{d}) = \delta(D-2)+2$. Luego, aplicando el Teorema 4.1.2 con $s = r-2$, concluimos que, si

$$q > \text{máx}\left\{\big(2(n-r+3)D+2\big)\delta + 1, D^2\delta, \big(\delta(D-2)+2\big)^2\right\}, \tag{4.3}$$

entonces V tiene un punto regular q-racional. Si $D \leq 2$ entonces $D^2\delta \leq \big(2(n-r+3)D+2\big)\delta + 1$, y para $D \geq 3$ se tiene que $D^2\delta \leq (\delta(D-2)+2)^2$. En consecuencia, vemos que (4.3) es equivalente a

$$q > \text{máx}\left\{\big(2(n-r+3)D+2\big)\delta + 1, \big(\delta(D-2)+2\big)^2\right\}. \tag{4.4}$$

Por otro lado, si $D \geq 6$, entonces

$$\big(\delta(D-2)+2\big)^2 \geq \big(2(D+3)D+2\big)\delta+1 \geq \big(2(n-r+3)D+2\big)\delta+1.$$

Combinando esta última desigualdad con (4.4) y haciendo cálculo elementales se deduce el resultado del corolario. □

Corolario 4.1.4. *Bajo las hipótesis del Teorema 4.1.2, supongamos además que el lugar singular de V tiene dimensión a lo sumo $r-3 \geq 0$. Si $q > 3D(D+2)^2\delta$, entonces V tiene un punto regular q-racional.*

Demostración. La Observación 4.1.1 asegura que $b_2'(n-r+2, \boldsymbol{d}) \leq (n-r+1)D^2\delta$. De esto, aplicando el Teorema 4.1.2 con $s = r-3$, vemos que una condición suficiente para que exista un punto regular q-racional de V es

$$q > \text{máx}\{D^3\delta, D\delta\big((3(n-r+3)+2)D+2\big)+\delta+1\}.$$

Teniendo en cuenta la desigualdad $n-r \leq D$, deducimos que

$$D\delta\big((3(n-r+3)+2)D+2\big)+\delta+1 \leq 3D(D+2)^2\delta,$$

lo cual implica lo que queríamos probar. □

Dado que no se conocen resultados de existencia de puntos q-racionales regulares, vamos a comparar los Corolarios 4.1.3 y 4.1.4 con los resultados de existencia de puntos q-racionales que se obtienen a partir de las estimaciones de [GL02a] y [CM07a]. Cabe destacar que, a fin de deducir la existencia de puntos q-racionales regulares, es necesario imponer condiciones aún más restrictivas sobre q.

Para una intersección completa normal V que verifica las hipótesis del Corolario 4.1.3, se tiene la siguiente estimación (ver [GL02a, Corollary 6.2]):

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta(D-2)+2)q^{r-1/2} + 9\cdot 2^{n-r}((n-r)d+3)^{n+1}q^{r-1}, \tag{4.5}$$

donde $d := \text{máx}_{1\leq i\leq n-r}\, d_i$. Por otro lado, si $q > 2(n-r)d\delta+1$, se tiene (ver [CM07a, Corollary 6.2]):

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta(D-2)+2)q^{r-1/2} + 2\big((n-r)d\delta\big)^2 q^{r-1}. \tag{4.6}$$

Estas son las estimaciones más precisas que se conocen para intersecciones completas normales. A partir de (4.5) y (4.6) deducimos fácilmente la siguiente condición suficiente para la existencia de puntos q-racionales de V:

$$\begin{aligned} q &> \text{máx}\left\{(\delta(D-2)+3)^2, 18\cdot 2^{n-r}((n-r)d+3)^{n+1}\right\}, \\ q &> 4\big((n-r)d\delta\big)^2. \end{aligned}$$

Es claro que estas condiciones son más restrictivas que las del Corolario 4.1.3.

A continuación consideramos una intersección completa V regular en codimensión 2. Se tiene entonces la siguiente estimación (ver [GL02a, Theorem 6.1]):

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b_2'(n-r+2, \boldsymbol{d})q^{r-1} + 9\cdot 2^{n-r}((n-r)d+3)^{n+1}q^{r-3/2}. \tag{4.7}$$

Teniendo en cuenta la desigualdad $b'_2(n-r+2, \boldsymbol{d}) \leq (n-r+1)D^2\delta$ de la Observación 4.1.1, deducimos a partir de (4.7) la siguiente condición suficiente para la existencia de puntos q-racionales de V:

$$q > \text{máx}\left\{2(n-r+1)D^2\delta, 7\cdot 2^{2(n-r)/3}((n-r)d+3)^{(2n+2)/3}\right\}. \tag{4.8}$$

El Corolario 4.1.4 complementa el resultado (4.8) ya que es mejor en ciertos casos; por ejemplo, cuando todas las ecuaciones tienen grado 2 y la cantidad de ecuaciones es mayor a $(2n+2)/3$ o para el caso de hipersuperficies con $n \geq 6$.

4.2. Estimaciones para intersecciones completas singulares

En esta sección obtendremos estimaciones sobre la cantidad de puntos q-racionales regulares de una intersección completa V en los casos en que V es normal o V es regular en codimensión 2 (es decir, su lugar singular tiene codimensión al menos 3). Recordemos que $V \subset \mathbb{P}^n$ es una intersección completa de dimensión r, grado δ y multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ con $d_1 \geq \cdots \geq d_{n-r} \geq 2$. Supongamos que el lugar singular de V tiene dimensión a lo sumo $s \leq r-2$. Sea $D := \sum_{i=1}^{n-r}(d_i - 1)$. Fijamos $\boldsymbol{\lambda} \in (\mathbb{P}^n)^{s+2} \setminus \mathcal{H}$ donde $\mathcal{H}$ es la hipersuperficie definida en la Proposición 3.2.6. De acuerdo a nuestra versión efectiva del segundo teorema de Bertini (Teorema 3.3.4), para fijo existe una variedad $W_L := W(L) \subset \mathbb{P}^{s+1}$ de dimensión a lo sumo s y grado a lo sumo $D^{r-s}\delta$ tal que, para cada $y \in \mathbb{P}^{s+1} \setminus W_L$, la clausura Zariski V_y de la fibra $\pi^{-1}(y)$ es una intersección completa no singular.

Para estimar la cantidad de puntos q-racionales de V vamos a expresar a V como la unión de $p_{s+1} := |\mathbb{P}^{s+1}(\mathbb{F}_q)|$ secciones lineales de V de dimensión $r-s-1$. Dichas secciones lineales resultan ser la clausura Zariski V_y de las fibras $\pi^{-1}(y)$ con $y \in \mathbb{P}^{s+1}$. Dado que V_y está definida sobre $\mathbb{F}_q$ para cada $y \in \mathbb{P}^{s+1}(\mathbb{F}_q)$, podemos estimar el número $N_y := |V_y(\mathbb{F}_q)|$ para $y \in \mathbb{P}^{s+1}(\mathbb{F}_q) \setminus W_L$ usando la estimación de Deligne (4.1). Por otro lado, las fibras de los puntos en W_L no contribuyen significativamente al comportamiento asintótico del número de puntos q-racionales de V. Más precisamente tenemos el siguiente resultado.

Teorema 4.2.1. *Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión $r \geq 2$, grado δ, multigrado $\boldsymbol{d}$ y cuyo lugar singular tiene dimensión a lo sumo $s \leq r-2$. Entonces se tiene la siguiente estimación:*

$$\left||V(\mathbb{F}_q)| - p_r\right| \leq b'_{r-s-1}q^{(r+s+1)/2} + A(n,s,\boldsymbol{d})\, q^{r-1},$$

donde $A(n,s,\boldsymbol{d}) := 2b'_{r-s-1} + 2\big(7D^{r-s}\delta + 1\big)(\delta - 1)$ y $b'_{r-s-1} := b'_{r-s-1}(n-s-1, \boldsymbol{d})$ es el $(r-s-1)$-ésimo número primitivo de Betti de una intersección completa C de $\mathbb{P}^{n-s-1}$ de dimensión $r-s-1$ y multigrado $\boldsymbol{d}$.

Demostración. En primer lugar, notemos que si $D = 1$, entonces V es una cuádrica, y por lo tanto la estimación se deduce de los resultados conocidos sobre la cantidad

de puntos q-racionales para cuádricas (ver, por ejemplo, [Sch76, Theorem 2E] o [LN83, Section 6.2]).

Afirmamos que podemos suponer sin pérdida de generalidad que $q > B_{\boldsymbol{d},s}$. En efecto, supongamos que $q \leq B_{\boldsymbol{d},s}$. Si $D = 2$, entonces V es una hipersuperficie cúbica o la intersección de dos cuádricas. En ambos casos tenemos que $|V(\mathbb{F}_q)| \leq \delta q^r + p_{r-1}$ (ver [Ser91] y [ELX09], respectivamente), lo cual implica $\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta-1)q^r \leq B_{\boldsymbol{d},s}(\delta-1)q^{r-1}$. Así, teniendo en cuenta que $B_{\boldsymbol{d},s} \leq 10 \cdot 2^{r-s} \cdot \delta + 1$, deducimos que el teorema es válido para este caso. Supongamos ahora que $D \geq 3$. De acuerdo a la Proposición 2.3.4 (ii) se tiene que $|V(\mathbb{F}_q)| \leq \delta p_r$, y por lo tanto $\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta-1)p_r \leq 2B_{\boldsymbol{d},s}(\delta-1)q^{r-1}$. Dado que $B_{\boldsymbol{d},s} \leq 7D^{r-s}\delta + 1$, se deduce fácilmente que el teorema es válido para $D \geq 3$. Esto prueba nuestra afirmación.

Supongamos entonces $q > B_{\boldsymbol{d},s}$. Combinando la Proposición 3.2.6 y el Corolario 2.3.13 deducimos entonces que existe $\boldsymbol{\lambda} \in (\mathbb{P}^n(\mathbb{F}_q))^{s+2}$ tal que se verifican las condiciones $i)$–$iii)$ de la Proposición 3.2.6. Sea V_y la sección lineal de V que obtenemos al considerar la clausura Zariski de la fibra $\pi^{-1}(y)$ para un punto arbitrario $y \in \mathbb{P}^{s+1}$. Podemos expresar $|V(\mathbb{F}_q)|$ en términos de las cantidades $N_y := |V_y(\mathbb{F}_q)|$ para cada $y \in \mathbb{P}^{s+1}(\mathbb{F}_q)$:

$$|V(\mathbb{F}_q)| \;=\; \sum_{y\in\mathbb{P}^{s+1}(\mathbb{F}_q)} (N_y - e) + e = \sum_{y\in\mathbb{P}^{s+1}(\mathbb{F}_q)} N_y - (p_{s+1}-1)e, \tag{4.9}$$

donde $e := |(V \cap L)(\mathbb{F}_q)|$. Como $V \cap L$ tiene dimensión $r-s-2$, se tiene que $e \leq \delta p_{r-s-2}$, y por lo tanto $|e - p_{r-s-2}| \leq (\delta-1)p_{r-s-2}$. Restando p_r a ambos miembros de (4.9) y utilizando que $p_r = p_{s+1}p_{r-s-1} - (p_{s+1}-1)p_{r-s-2}$, obtenemos:

$$\begin{aligned}\big||V(\mathbb{F}_q)| - p_r\big| \;&\leq\; \sum_{y\in\mathbb{P}^{s+1}(\mathbb{F}_q)} |N_y - p_{r-s-1}| \;+\; (p_{s+1}-1)(\delta-1)p_{r-s-2} \\ &\leq\; \sum_{y\in\mathbb{P}^{s+1}(\mathbb{F}_q)} |N_y - p_{r-s-1}| \;+\; 2(\delta-1)q^{r-1}. \end{aligned}\tag{4.10}$$

Consideremos la variedad $W_L \subset \mathbb{P}^{s+1}$ del enunciado del Teorema 3.3.4. Podemos descomponer la sumatoria del lado derecho de (4.10) de la siguiente manera:

$$\sum_{y\in\mathbb{P}^{s+1}(\mathbb{F}_q)} |N_y - p_{r-s-1}| = \sum_{y\notin W_L(\mathbb{F}_q)} |N_y - p_{r-s-1}| + \sum_{y\in W_L(\mathbb{F}_q)} |N_y - p_{r-s-1}|\,.$$

Si $y \notin W_L(\mathbb{F}_q)$, por el Teorema 3.3.4 se tiene que V_y es una intersección completa no singular de $\mathbb{P}^{n-s-1}$, definida sobre $\mathbb{F}_q$, de dimensión $r-s-1$, grado δ y multigrado $\boldsymbol{d}$. Aplicando la estimación de Deligne (4.1) a cada V_y se obtiene $|N_y - p_{r-s-1}| \leq b'_{r-s-1}q^{(r-s-1)/2}$, y por lo tanto,

$$\sum_{y\notin W_L(\mathbb{F}_q)} |N_y - p_{r-s-1}| \leq b'_{r-s-1}q^{\frac{r-s-1}{2}}p_{s+1} \leq b'_{r-s-1}q^{\frac{r+s+1}{2}} + 2b'_{r-s-1}q^{r-1}. \tag{4.11}$$

Por otro lado, si $y \in W_L(\mathbb{F}_q)$, entonces $N_y \leq \delta p_{r-s-1}$. Luego, dado que $\delta \geq 2$, obtenemos $|N_y - p_{r-s-1}| \leq (\delta-1)p_{r-s-1}$. De acuerdo a la Proposición 2.3.4 parte

(ii), se tiene $|W_L(\mathbb{F}_q)| \leq \deg W_L \cdot p_s$ y, por lo tanto, deducimos la siguiente estimación:

$$\sum_{y \in W_L(\mathbb{F}_q)} |N_y - p_{r-s-1}| \leq (\delta-1)p_{r-s-1} \cdot \deg W_L \cdot p_s \leq 4(\delta-1)\deg W_L \cdot q^{r-1}. \quad (4.12)$$

Combinando (4.10), (4.11) y (4.12), concluimos que

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_{r-s-1} q^{\frac{r+s+1}{2}} + 2\left(b'_{r-s-1} + (2D^{r-s}\delta+1)(\delta-1)\right) q^{r-1},$$

de donde se deduce fácilmente la afirmación del teorema. □

A continuación damos una estimación de la cantidad de puntos q-racionales regulares de V.

Teorema 4.2.2. *Teniendo en cuenta las notaciones e hipótesis del Teorema 4.2.1, se tiene la siguiente estimación:*

$$\big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| \leq b'_{r-s-1} q^{\frac{r+s+1}{2}} + B(n,s,\boldsymbol{d})\, q^{r-1},$$

donde $B(n,s,\boldsymbol{d}) := 2b'_{r-s-1} + 2\big(2D^{r-s}\delta+1\big)(\delta-1) + 2(s+2)(\delta-1)B_{\boldsymbol{d},s}$.

Demostración. Sea $\mathcal{H} \subset (\mathbb{P}^n)^{s+2}$ la hipersuperficie definida en la Proposición 3.2.6. Recordemos que $\mathcal{H}$ está definida por un polinomio multihomogéneo en $\overline{\mathbb{F}}_q[\boldsymbol{\Lambda}]$ de grado a lo sumo $B_{\boldsymbol{d},s}$ en cada grupo de variables Λ_i. Tenemos entonces

$$\begin{aligned}\big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| &= \frac{1}{p_n^{s+2}}\left(\sum_{\boldsymbol{\lambda} \in ((\mathbb{P}^n)^{s+2} \setminus \mathcal{H})(\mathbb{F}_q)} \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| + \sum_{\boldsymbol{\lambda} \in \mathcal{H}(\mathbb{F}_q)} \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big|\right)\\ &\leq \frac{1}{p_n^{s+2}}\left(\sum_{\boldsymbol{\lambda} \in ((\mathbb{P}^n)^{s+2} \setminus \mathcal{H})(\mathbb{F}_q)} \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| + |\mathcal{H}(\mathbb{F}_q)|(\delta-1)p_r\right).\end{aligned}$$

De (2.7) se sigue que $|\mathcal{H}(\mathbb{F}_q)| \leq p_n^{s+2} - (q^n - \min\{q, B_{\mathbf{d},s}\}q^{n-1})^{s+2}$. Por lo tanto,

$$\frac{|\mathcal{H}(\mathbb{F}_q)|}{(p_n)^{s+2}}(\delta-1)p_r \leq 2(s+2)(\delta-1)B_{\mathbf{d},s}q^{r-1}.$$

Por otro lado, para cada $\boldsymbol{\lambda} \in ((\mathbb{P}^n)^{s+2} \setminus \mathcal{H})(\mathbb{F}_q)$ existe, por el Teorema 3.3.4, una variedad $W_L \subset \mathbb{P}^{s+1}$ de dimensión a lo sumo s y grado a lo sumo $D^{r-s}\delta$ tal que para cada $y \in \mathbb{P}^{s+1} \setminus W_L$, la clausura Zariski V_y de la fibra $\pi^{-1}(y)$ es una intersección completa no singular, y por la Observación 3.3.5 $V_y \subset V_{\mathrm{sm}}$. Argumentando entonces de la misma manera que en la demostración del Teorema 4.2.1, obtenemos

$$\frac{1}{p_n^{s+2}} \sum_{\boldsymbol{\lambda} \notin \mathcal{H}(\mathbb{F}_q)} \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| \leq b'_{r-s-1} q^{\frac{r+s+1}{2}} + 2\left(b'_{r-s-1} + (2D^{r-s}\delta+1)(\delta-1)\right) q^{r-1},$$

de donde se deduce fácilmente el teorema. □

4.2.1. Intersecciones completas normales

Si $V \subset \mathbb{P}^n$ es una intersección completa normal de dimensión r, entonces el lugar singular de V tiene dimensión a lo sumo $r-2$. Por lo tanto, considerando el caso $s := r-2$ de los Teoremas 4.2.1 y 4.2.2 obtenemos el siguiente resultado.

Corolario 4.2.3. *Sea $V \subset \mathbb{P}^n$ una intersección completa normal definida sobre $\mathbb{F}_q$, de dimensión $r \geq 2$, grado δ y multigrado $\boldsymbol{d}$. Entonces*

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta(D-2)+2)q^{r-1/2} + 14D^2\delta^2 q^{r-1}, \tag{4.13}$$
$$\big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| \leq (\delta(D-2)+2)q^{r-1/2} + 11(r+1)D^2\delta^2 q^{r-1}. \tag{4.14}$$

Demostración. Aplicando los Teoremas 4.2.1 y 4.2.2 para el caso $s = r-2$ obtenemos

$$\begin{aligned}\big||V(\mathbb{F}_q)| - p_r\big| &\leq b_1' q^{r-1/2} + A(n, r-2, \boldsymbol{d})\, q^{r-1},\\ \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| &\leq b_1' q^{r-1/2} + B(n, r-2, \boldsymbol{d})\, q^{r-1},\end{aligned}$$

donde $b_1' := b_1'(n-r+1, \boldsymbol{d})$,

$$\begin{aligned}A(n, r-2, \boldsymbol{d}) &:= 2b_1' + 2\big(7D^2\delta + 1\big)(\delta - 1) \text{ y}\\ B(n, r-2, \boldsymbol{d}) &:= 2b_1' + 2\big(2D^2\delta + 1\big)(\delta - 1) + 2r(\delta-1)B_{\mathbf{d},r-2}.\end{aligned}$$

La estimación (4.13) se deduce fácilmente teniendo en cuenta la identidad $b_1' = \delta(D-2)+2$. Por otro lado, la estimación (4.14) es consecuencia de la desigualdad $n - r \leq D$. □

En el caso de intersecciones completas normales, las estimaciones más precisas que se conocen son las de S. Ghorpade y G. Lachaud [GL02a] y A. Cafure y G. Matera [CM07a]. Por un lado, en [GL02a, Corollary 6.2] se obtiene la siguiente estimación:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta(D-2)+2)q^{r-1/2} + 9 \cdot 2^{n-r}((n-r)d+3)^{n+1} q^{r-1}, \tag{4.15}$$

donde $d := \max_{1 \leq i \leq n-r} d_i$. Por otro lado, para $q > 2(n-r)d\delta + 1$, en [CM07a, Corollary 6.2] se demuestra que

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta(D-2)+2)q^{r-1/2} + 2\big((n-r)d\delta\big)^2 q^{r-1}. \tag{4.16}$$

Teniendo en cuenta los lados derechos de (4.13), (4.15) y (4.16), notamos que el primer término es el mismo en todos los casos mientras que la diferencia se encuentra en los segundos términos. Respecto de (4.16), notemos que el segundo término del lado derecho es levemente más chico que el correspondiente término de (4.13) cuando d_1 y d_{n-r} son "similares", en tanto que éste último es significativamente menor cuando d_1 y d_{n-r} difieren de forma importante. Asimismo, cabe destacar que la estimación (4.16) vale bajo la condición $q > 2(n-r)d\delta + 1$, mientras que (4.13) es

válida sin imponer condiciones sobre q. Para facilitar la comparación de (4.15) con (4.13) y (4.16), observamos que

$$\begin{aligned} 2^{n-r}((n-r)d+3)^{n+1} &\geq \big(2(n-r)\big)^{n-r}\left(\sum_{i=1}^{n-r}\frac{d_i}{n-r}\right)^{n-r}\left(\sum_{i=1}^{n-r}d_i\right)^{r+1} \\ &\geq \big(2(n-r)\big)^{n-r}\prod_{i=1}^{n-r}d_i\left(\sum_{i=1}^{n-r}d_i\right)^{r+1} \\ &\geq \big(2(n-r)\big)^{n-r}D^2\delta\left(\sum_{i=1}^{n-r}d_i\right)^{r-1}, \end{aligned}$$

donde la desigualdad del medio se obtiene como consecuencia de la desigualdad entre la media aritmética y la media geométrica. Notemos en primer lugar que para variedades de dimensión alta, por ejemplo $r > (n+1)/2$, las estimaciones (4.13) y (4.16) son claramente mejores que (4.15). En particular, en el caso de hipersuperficies el segundo término del lado derecho de (4.13) y (4.16) es cuadrático en δ, mientras que en (4.15) el exponente de δ es $n+1$. Otro caso en el que las estimaciones (4.13) y (4.16) mejoran (4.15) es el de variedades de grado bajo; por ejemplo, si $\delta \leq (2(n-r))^{n-r}$. Sin embargo, para variedades de dimensión baja el segundo término del lado derecho de (4.15) puede resultar más chico que el correspondiente término en (4.13) y (4.16). Por ejemplo, para curvas dicho término es lineal en δ en (4.15), mientras que en (4.13) y (4.16) es cuadrático en δ. Por lo tanto, la estimación (4.15) resulta mejor para variedades de dimensión baja y grado alto. En conclusión, nuestra estimación complementa la estimación (4.15) y mejora (4.16) en el sentido de que es válida sin imponer condiciones sobre q.

4.2.2. Intersecciones completa regulares en codimensión 2

Sea $V \subset \mathbb{P}^n$ una intersección completa de dimensión r, regular en codimensión 2, es decir, la dimensión del lugar singular es a lo sumo $r-3$. Consideramos entonces el caso $s := r-3$ de los Teoremas 4.2.1 y 4.2.2 y obtenemos el siguiente resultado.

Corolario 4.2.4. *Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión $r \geq 3$, grado δ y multigrado $\boldsymbol{d}$, cuyo lugar singular tiene dimensión a lo sumo $r-3$. Se tiene entonces la siguiente estimación:*

$$\begin{aligned} \big||V(\mathbb{F}_q)| - p_r\big| &\leq 14D^3\delta^2 q^{r-1}, \\ \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| &\leq (34r-20)D^3\delta^2 q^{r-1}. \end{aligned} \tag{4.17}$$

Demostración. Teniendo en cuenta los Teoremas 4.2.1 y 4.2.2, se tiene

$$\begin{aligned} \big||V(\mathbb{F}_q)| - p_r\big| &\leq A(n,r-3,\boldsymbol{d})q^{r-1}, \\ \big||V_{\mathrm{sm}}(\mathbb{F}_q)| - p_r\big| &\leq B(n,r-3,\boldsymbol{d})q^{r-1}, \end{aligned}$$

donde

$$\begin{aligned} A(n,r-3,\boldsymbol{d}) &:= 3b_2' + 2\big(7D^3\delta+1\big)(\delta-1), \\ B(n,r-3,\boldsymbol{d}) &:= 3b_2' + 2\big(2D^3\delta+1\big)(\delta-1) + 2(r-1)(\delta-1)B_{\mathbf{d},r-3} \end{aligned}$$

y $b_2' := b_2'(n-r+2, \boldsymbol{d})$. Por la Observación 4.1.1 se tiene $b_2' \leq (n-r+1)D^2\delta \leq (D+1)D^2\delta$. Las estimaciones del corolario se siguen ahora de cálculos elementales. □

Bajo las hipótesis del Corolario 4.2.4, Ghorpade y Lachaud obtienen en [GL02a, Theorem 6.1] la siguiente estimación:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b_2'(n-r+2, \boldsymbol{d})q^{r-1} + 9 \cdot 2^{n-r} \cdot ((n-r)d+3)^{n+1}q^{r-3/2}. \quad (4.18)$$

Al igual que en el caso de variedades normales, para variedades de dimensión alta nuestra estimación resulta mejor que (4.18), mientras que en el caso de variedades de dimensión baja (4.18) es preferible. Sin embargo, la presencia de términos exponenciales en el segundo término del lado derecho de (4.18) hacen difícil la aplicación de esta estimación. Como ejemplo de este fenómeno, en el Capítulo 6 estudiaremos el problema de estimar el valor promedio del cardinal del conjunto de valores de una familia de polinomios mónicos de grado d con s coeficientes fijos, el cual requiere de la aplicación de una estimación como en (4.17).

4.2.3. Una versión explícita de la estimación de Hooley

En la sección anterior obtuvimos estimaciones para variedades normales y regulares en codimensión 2. Dado que muchas veces disponemos de cotas más precisas para la dimensión del lugar singular, en esta sección nos proponemos obtener una versión explícita de la estimación de Hooley. Como mencionamos anteriormente, en [Hoo91] Hooley extiende la estimación de Deligne [Del74] a intersecciones completas arbitrarias. Más precisamente, si $V \subset \mathbb{P}^n$ es una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r y lugar singular de dimensión $s \geq 0$, entonces la cantidad de puntos q-racionales de V verifica la siguiente estimación:

$$\big|V(\mathbb{F}_q) - p_r\big| = \mathcal{O}(q^{(r+s+1)/2}). \quad (4.19)$$

La constante involucrada en esta estimación, si bien no depende de q, no es explícita. La demostración de Hooley consiste en considerar sucesivas secciones por hiperplanos de V hasta que se obtienen secciones no singulares. La cantidad de puntos q-racionales de dichas secciones no singulares se estima utilizando [Del74]. Dos herramientas claves en el trabajo de Hooley son una estimación (no explícita) de la cantidad de secciones por hiperplanos de V que tienen lugar singular de dimensión s, $s-1$ y $s+1$, y una cota superior para el segundo momento definido como

$$M := M(V) := \sum_{\boldsymbol{m} \in \mathbb{F}_q^{n+1}} \Big(N - q\, N(\boldsymbol{m})\Big)^2,$$

donde N es la cantidad de puntos q-racionales de V y $N(\boldsymbol{m})$ es la cantidad de puntos q-racionales de la sección lineal de V determinada por el hiperplano que define $\boldsymbol{m}$. Aquí seguiremos las técnicas de Hooley, con la diferencia de que, en vez de intersecar sucesivamente a V con hiperplanos hasta obtener secciones lineales de dimensión $r-s-1$, vamos a considerar directamente el segundo momento que

se obtiene teniendo en cuenta las secciones lineales de V que determinan todas las variedades lineales de codimensión $s+1$.

Comenzamos entonces estimando la cantidad de secciones lineales no singulares de V de dimensión $r-s-1$ definidas sobre $\mathbb{F}_q$. Para esto, consideramos la hipersuperficie $\mathcal{H}$ definida en el Corolario 3.4.4. Recordemos que, si $q > D^{r-s-1}\delta(D+r-s+1)$, entonces existe $\boldsymbol{\gamma} \in (\mathbb{F}_q^{n+1})^{s+1}$ tal que $\mathcal{H}(\boldsymbol{\gamma}) \neq 0$, por lo que la sección lineal de V definida por $\boldsymbol{\gamma}$ es no singular de dimensión $r-s-1$ y está definida sobre $\mathbb{F}_q$.

Lema 4.2.5. *La cantidad de elementos $\boldsymbol{\gamma} \in (\mathbb{F}_q^{n+1})^{s+1}$ tales que $\mathcal{H}(\boldsymbol{\gamma}) \neq 0$ es al menos $(q-d)^{s+1}q^{n(s+1)}$, donde $d := D^{r-s-1}\delta(D+r-s+1)$.*

Demostración. Sea N la cantidad de ceros q-racionales de $\mathcal{H}$. Por la desigualdad (2.9) se tiene que

$$N \leq \sum_{\boldsymbol{\varepsilon} \in \{0,1\}^{s+1}\setminus\{\mathbf{0}\}} (-1)^{|\boldsymbol{\varepsilon}|+1} d^{|\boldsymbol{\varepsilon}|} q^{(n+1)(s+1)-|\boldsymbol{\varepsilon}|}.$$

El lado derecho de esta desigualdad verifica

$$\begin{aligned}\sum_{\boldsymbol{\varepsilon} \in \{0,1\}^{s+1}\setminus\{\mathbf{0}\}} (-1)^{|\boldsymbol{\varepsilon}|+1} d^{|\boldsymbol{\varepsilon}|} q^{(n+1)(s+1)-|\boldsymbol{\varepsilon}|} &= \sum_{i=1}^{s+1} \sum_{\boldsymbol{\varepsilon}:\, |\boldsymbol{\varepsilon}|=i} (-1)^{i+1} d^i q^{(n+1)(s+1)-i} \\ &= q^{n(s+1)} \left(\sum_{i=0}^{s+1} \binom{s+1}{i} (-1)^{i+1} d^i q^{s+1-i} + q^{s+1} \right) \\ &= q^{n(s+1)} \left(q^{s+1} - (q-d)^{s+1} \right).\end{aligned}$$

De esto deducimos fácilmente el enunciado del lema. □

A continuación estudiamos el segundo momento definido como

$$M := M(V) := \sum_{\boldsymbol{\gamma} \in \mathbb{F}_q^{(n+1)(s+1)}} \left(N - q^{s+1} N(\boldsymbol{\gamma}) \right)^2, \tag{4.20}$$

donde $N := |V(\mathbb{F}_q)|$, $N(\boldsymbol{\gamma}) := |V \cap \mathcal{L}(\mathbb{F}_q)|$ y $\mathcal{L}$ es la variedad lineal de dimensión $(n-s-1)$ definida por $\boldsymbol{\gamma} := (\gamma_0, \ldots, \gamma_s)$, es decir,

$$\mathcal{L} := \{x \in \mathbb{P}^n : \gamma_0 \cdot x = \cdots = \gamma_s \cdot x = 0\}. \tag{4.21}$$

Notemos $t := (n+1)(s+1)$. Observamos que

$$M = \sum_{\boldsymbol{\gamma} \in \mathbb{F}_q^t} N^2 - \ (2q^{s+1}N) \sum_{\boldsymbol{\gamma} \in \mathbb{F}_q^t} N(\boldsymbol{\gamma}) + q^{2(s+1)} \sum_{\boldsymbol{\gamma} \in \mathbb{F}_q^t} N(\boldsymbol{\gamma})^2. \tag{4.22}$$

Analizamos el segundo término del lado derecho de (4.22). Tenemos que

$$\sum_{\boldsymbol{\gamma} \in \mathbb{F}_q^t} N(\boldsymbol{\gamma}) = \sum_{\boldsymbol{\gamma} \in \mathbb{F}_q^t} \sum_{\substack{x \in V \\ \boldsymbol{\gamma} \cdot x = 0}} 1 = \sum_{x \in V} \sum_{\substack{\boldsymbol{\gamma} \in \mathbb{F}_q^t \\ \boldsymbol{\gamma} \cdot x = 0}} 1 = q^{n(s+1)}\, N, \tag{4.23}$$

donde $\boldsymbol{\gamma} \cdot x = 0$ denota las igualdades $\gamma_i \cdot x = 0$ para $0 \leq i \leq s$.

Por otro lado, el tercer término del lado derecho de (4.22) verifica

$$\begin{aligned}\sum_{\boldsymbol{\gamma}\in\mathbb{F}_q^t} N(\boldsymbol{\gamma})^2 &= \sum_{\boldsymbol{\gamma}\in\mathbb{F}_q^t} \left(\sum_{\substack{x\in V\\ \boldsymbol{\gamma}\cdot x=0}} 1\right)\left(\sum_{\substack{x'\in V\\ \boldsymbol{\gamma}\cdot x'=0}} 1\right)\\ &= \sum_{\boldsymbol{\gamma}\in\mathbb{F}_q^t}\sum_{\substack{x\in V\\ \boldsymbol{\gamma}\cdot x=0}} 1 + \sum_{\boldsymbol{\gamma}\in\mathbb{F}_q^t}\sum_{\substack{x,x'\in V\\ x\neq x'\\ \boldsymbol{\gamma}\cdot x=\boldsymbol{\gamma}\cdot x'=0}} 1 \\ &= q^{n(s+1)}N + \sum_{\substack{x,x'\in V\\ x\neq x'}}\sum_{\substack{\boldsymbol{\gamma}\in\mathbb{F}_q^t\\ \boldsymbol{\gamma}\cdot x=\boldsymbol{\gamma}\cdot x'=0}} 1\\ &= q^{n(s+1)}N + q^{(n-1)(s+1)}N(N-1).\end{aligned} \tag{4.24}$$

Finalmente, combinando (4.23) y (4.24) obtenemos la siguiente cota superior para el segundo momento M de (4.20):

$$M \leq q^{(n+1)(s+1)}(q^{s+1}-1)N \leq \delta\, p_r\, q^{(n+1)(s+1)}(q^{s+1}-1). \tag{4.25}$$

A partir de esta cota superior deducimos que existen al menos $\frac{1}{2}q^{(n+1)(s+1)}$ elementos $\boldsymbol{\gamma} \in \mathbb{F}_q^{(n+1)(s+1)}$ tales que la correspondiente variedad lineal $\mathcal{L}$ satisface la condición

$$\big||V(\mathbb{F}_q)| - q^{s+1}|(V\cap\mathcal{L})(\mathbb{F}_q)|\big| \leq \sqrt{2\delta p_r(q^{s+1}-1)}.$$

En efecto, si fuera

$$\big||V(\mathbb{F}_q)| - q^{s+1}|(V\cap\mathcal{L})(\mathbb{F}_q)|\big| > \sqrt{2\delta p_r(q^{s+1}-1)}$$

para al menos $\frac{1}{2}q^{(n+1)(s+1)}$ variedades lineales $\mathcal{L}$, entonces resultaría

$$M > \delta\, p_r\, q^{(n+1)(s+1)}(q^{s+1}-1),$$

lo que contradiría (4.25). En conclusión, obtenemos el siguiente resultado.

Proposición 4.2.6. *Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r, grado δ, multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ y lugar singular de dimensión a lo sumo $s \geq 0$. Entonces existen al menos $\frac{1}{2}q^{(n+1)(s+1)}$ elementos $\boldsymbol{\gamma}$ en $\mathbb{F}_q^{(n+1)(s+1)}$ tales que la correspondiente variedad lineal $\mathcal{L}$ definida como en (4.21) satisface la siguiente condición:*

$$\big||V(\mathbb{F}_q)| - q^{s+1}|(V\cap\mathcal{L})(\mathbb{F}_q)|\big| \leq \sqrt{2\delta p_r(q^{s+1}-1)}. \tag{4.26}$$

El Lema 4.2.5 establece que, notando $d := \big(D^{r-s-1}(D+r-s)+1\big)\delta$, existen al menos $(q-d)^{s+1}q^{n(s+1)}$ elementos $\boldsymbol{\gamma} \in (\mathbb{F}_q^{n+1})^{s+1}$ tales que la sección lineal de V

definida por $\boldsymbol{\gamma}$ es no singular de dimensión $r-s-1$ y está definida sobre $\mathbb{F}_q$. En particular, si

$$(q-d)^{s+1}q^{n(s+1)} > \frac{1}{2}q^{(n+1)(s+1)}, \tag{4.27}$$

entonces existe al menos una sección lineal no singular de V de dimensión $r-s-1$ definida sobre $\mathbb{F}_q$ que satisface la condición (4.26). Observemos que la desigualdad (4.27) es equivalente a $(1-\frac{d}{q})^{s+1} > \frac{1}{2}$. Por la desigualdad de Bernoulli se tiene que $(1-\frac{d}{q})^{s+1} \geq 1-(s+1)\frac{d}{q}$; luego, pidiendo que $1-(s+1)\frac{d}{q} > \frac{1}{2}$, obtenemos el siguiente resultado.

Corolario 4.2.7. *Sea $q > 2(s+1)\delta\big(D^{r-s-1}(D+r-s)+1\big)$. Bajo las hipótesis de la Proposición 4.2.6, existe una sección lineal no singular de V de dimensión $r-s-1$, definida sobre $\mathbb{F}_q$ que satisface la condición (4.26).*

Finalmente, proporcionamos una estimación *explícita* de la cantidad de puntos q-racionales de una intersección completa singular cuyo lugar singular es de dimensión $0 \leq s \leq r-2$ arbitrario, que es válida bajo una cierta condición sobre q. Decimos que esta estimación es explícita ya que, a diferencia de la estimación (4.19) de Hooley, exhibimos una cota superior explícita en términos de $n, s, r, \boldsymbol{d}$ para la constante involucrada en la misma.

Teorema 4.2.8. *Sea $q > 2(s+1)D^{r-s-1}\delta(D+r-s+1)$ y $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión r, grado δ, multigrado $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ y lugar singular de dimensión a lo sumo s con $0 \leq s \leq r-2$. Tenemos entonces la siguiente estimación:*

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \big(b'_{r-s-1}(n-s-1, \boldsymbol{d}) + 2\sqrt{\delta}+1\big)\, q^{\frac{r+s+1}{2}}. \tag{4.28}$$

Demostración. Como $q > 2(s+1)D^{r-s-1}\delta(D+r-s+1)$, por el Corolario 4.2.7 existe $\boldsymbol{\gamma} \in \mathbb{F}_q^{(n+1)(s+1)}$ tal que la sección lineal $\mathcal{L}$ definida por $\gamma_i \cdot X = 0$, $0 \leq i \leq s$, es no singular de dimensión $r-s-1$, está definida sobre $\mathbb{F}_q$ y se cumple la condición

$$\big||V(\mathbb{F}_q)| - q^{s+1}|(V \cap \mathcal{L})(\mathbb{F}_q)|\big| \leq \sqrt{2\delta p_r(q^{s+1}-1)}.$$

Para dicho $\boldsymbol{\gamma} \in \mathbb{F}_q^{(n+1)(s+1)}$, se tiene

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \big||V(\mathbb{F}_q)| - q^{s+1}N(\boldsymbol{\gamma})\big| + \big|p_r - q^{s+1}N(\boldsymbol{\gamma})\big|,$$

donde $N(\boldsymbol{\gamma}) = |V \cap \mathcal{L}(\mathbb{F}_q)|$. Por (4.26) y la identidad $p_r = q^{s+1}p_{r-s-1} + p_s$, obtenemos

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \sqrt{2\delta p_r(q^{s+1}-1)} + q^{s+1}\big|p_{r-s-1} - N(\boldsymbol{\gamma})\big| + p_s.$$

Como $V \cap \mathcal{L}$ es una sección no singular de V, podemos aplicar (4.1) para estimar la cantidad $|p_{r-s-1} - N(\boldsymbol{\gamma})|$. Más precisamente, tenemos que

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \sqrt{2\delta p_r(q^{s+1}-1)} + b'_{r-s-1}(n-s-1, \boldsymbol{d})\, q^{\frac{r+s+1}{2}} + p_s.$$

Dado que $p_r \leq 2q^r$ y $p_s \leq q^{\frac{r+s+1}{2}}$, deducimos el enunciado del teorema. □

Para finalizar este capítulo, exhibimos las estimaciones que se obtienen a partir del Teorema 4.2.8 en los casos en que el lugar singular de V tiene codimensión al menos 2 o al menos 3.

Sea $V \subset \mathbb{P}^n$ una intersección completa de dimensión r, grado δ, multigrado $\boldsymbol{d}$ y lugar singular de codimensión al menos 2. Considerando el caso $s = r-2$ del Teorema 4.2.8 se tiene que, si $q > 2(r-1)\delta D(D+3)$, entonces

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \big(b_1(n-r+1,\boldsymbol{d})' + 2\sqrt{\delta}+1\big)\, q^{r-\frac{1}{2}}.$$

Por otro lado, de acuerdo a la Proposición 2.3.4 (ii), $|V(\mathbb{F}_q)|$ satisface la siguiente estimación:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta-1)p_r \leq 2\delta q^r.$$

Dado que $b_1'(n-r+1,\boldsymbol{d}) = \delta(D-2)+2$, entonces

$$2\delta q^r \leq (b_1'(n-r+1,\boldsymbol{d}) + 2\sqrt{\delta}+1)q^{r-\frac{1}{2}}$$

si $q \leq D^2$. En resumen obtenemos el siguiente resultado.

Corolario 4.2.9. *Sea $V \subset \mathbb{P}^n$ una intersección completa normal definida sobre $\mathbb{F}_q$, de dimensión $r \geq 2$, grado δ y multigrado $\boldsymbol{d}$. Si $q \leq D^2$ o $q > 2(r-1)\delta D(D+3)$, se satisface la siguiente estimación:*

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \big(b_1(n-r+1,\boldsymbol{d})' + 2\sqrt{\delta}+1\big)\, q^{r-\frac{1}{2}}.$$

Supongamos ahora que el lugar singular de V tiene codimensión al menos 3. Por el caso $s = r-3$ del Teorema 4.2.8, si $q > 2(r-2)\delta D^2(D+4)$, entonces $|V(\mathbb{F}_q)|$ verifica la estimación

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \big(b_2'(n-r+2,\boldsymbol{d}) + 2\sqrt{\delta}+1\big)\, q^{r-1}.$$

Dado que $b_2'(n-r+2,\boldsymbol{d}) \leq (n-r+1)\delta D^2$, entonces

$$2\delta q^r \leq (b_2'(n-r+2,\boldsymbol{d}) + 2\sqrt{\delta}+1)q^{r-1}$$

si $q \leq (n-r+1)D^2$. Tenemos entonces el siguiente resultado.

Corolario 4.2.10. *Sea $V \subset \mathbb{P}^n$ una intersección completa definida sobre $\mathbb{F}_q$, de dimensión $r \geq 3$, grado δ y multigrado $\boldsymbol{d}$, cuyo lugar singular tiene codimensión al menos 3. Si $q \leq (n-r+1)D^2$ o $q > 2(r-2)\delta D^2(D+4)$, se satisface la siguiente estimación:*

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \big(b_2'(n-r+2,\boldsymbol{d}) + 2\sqrt{\delta}+1\big)\, q^{r-1}.$$

Cabe señalar que las estimaciones obtenidas en los Corolarios 4.2.9 y 4.2.10 tienen un término de error que es notablemente mejor que las obtenidas en los Corolarios 4.2.3 y 4.2.4 respectivamente, pero son válidas bajo una cierta condición sobre q. En este sentido, decimos que todas las estimaciones que presentamos se complementan; dependiendo de las características del problema en consideración puede resultar más conveniente una u otra.

Capítulo 5

Intersecciones completas definidas por polinomios simétricos

En los capítulos anteriores obtuvimos estimaciones para intersecciones completas singulares. Nos interesa ahora poder aplicar dichas estimaciones a problemas concretos de teoría de códigos y combinatoria. Más concretamente, en esta tesis estudiamos el problema de determinar deep holes en códigos de Reed-Solomon y el problema del cálculo del valor promedio del cardinal del conjunto de valores de una familia de polinomios univariados mónicos definidos sobre $\mathbb{F}_q$. Para ambos casos ocurre que las variedades involucradas están definidas por polinomios simétricos. Esto nos lleva a pensar que, aprovechando esta característica particular, podemos obtener mejores resultados. Es por eso que dedicamos este capítulo a estudiar las propiedades geométricas de $\mathbb{F}_q$-variedades intersección completa definidas por polinomios invariantes bajo la acción del grupo simétrico de permutaciones de sus coordenadas. Cabe mencionar que este tipo de variedades aparecen con frecuencia en combinatoria, teoría de códigos y criptografía. Por ejemplo, en el estudio de los polinomios "*almost perfect nonlinear*" o de los "*differentially uniform mappings*" (ver [AR10] y [Rod09]).

5.1. Una familia de intersecciones completas

Fijamos enteros positivos s, r, m que verifican $m \leq s \leq r - m$ y consideramos $Y_1, \ldots, Y_s$ indeterminadas sobre $\overline{\mathbb{F}}_q$ y polinomios $S_i \in \mathbb{F}_q[Y_1, \ldots, Y_s]$ con $1 \leq i \leq m$. Sea $(\partial \boldsymbol{S}/\partial \boldsymbol{Y}) := (\partial S_i/\partial Y_j)_{1\leq i\leq m, 1\leq j\leq s}$ la matriz Jacobiana de $S_1, \ldots, S_m$ con respecto a $Y_1, \ldots, Y_s$. Supongamos además que $S_1, \ldots, S_m$ verifican las siguientes condiciones:

(H1) $S_1, \ldots, S_m$ forman una sucesión regular de $\mathbb{F}_q[Y_1, \ldots, Y_s]$;

(H2) $(\partial \boldsymbol{S}/\partial \boldsymbol{Y})(y) := (\partial S_i/\partial Y_j)_{1\leq i\leq m, 1\leq j\leq s}$ tiene rango máximo m para cada $y \in \mathbb{A}^s$.

A partir de (H_1) y (H_2) se tiene que la variedad $W_s \subset \mathbb{A}^s$ definida por $S_1, \ldots, S_m$ es una intersección completa conjuntista de dimensión $s - m$. Más aún, por [Eis95,

Theorem 18.15] se tiene que $S_1, \ldots, S_m$ definen un ideal radical y, por lo tanto, W_s resulta una intersección completa.

Sean $\Pi_1, \ldots, \Pi_s$ los primeros s polinomios simétricos elementales en $\mathbb{F}_q[X_1, \ldots, X_r]$ y sean $R_1, \ldots, R_m \in \mathbb{F}_q[X_1, \ldots, X_r]$ los polinomios definidos como $R_i := S_i(\Pi_1, \ldots, \Pi_s)$ para $1 \leq i \leq m$. Llamamos $V_r \subset \mathbb{A}^r$ a la $\mathbb{F}_q$-variedad afín definida por $R_1, \ldots, R_m$. En lo que sigue probaremos diversas propiedades sobre la geometría de V_r. Con este objetivo, consideramos el siguiente morfismo suryectivo de $\mathbb{F}_q$-variedades:

$$\begin{aligned} \Pi_r : \mathbb{A}^r &\to \mathbb{A}^r \\ x &\mapsto (\Pi_1(x), \ldots, \Pi_r(x)). \end{aligned}$$

Es fácil verificar que Π_r es un morfismo finito (ver [Sha94, §5.3, Example 1]). En particular, la preimagen $(\Pi_r)^{-1}(Z)$ de una variedad afín irreducible $Z \subset \mathbb{A}^r$ de dimensión k es equidimensional de dimensión k (ver [Dan94, §4.2, Proposition]).

Consideremos los polinomios $S_1, \ldots, S_m$ como elementos de $\mathbb{F}_q[Y_1, \ldots, Y_r]$ y llamemos $W_r \subset \mathbb{A}^r$ a la variedad afín correspondiente $W_r := V(S_1, \ldots, S_m)$. Notemos que $V_r = \Pi_r^{-1}(W_r)$. Dado que $S_1, \ldots, S_m$ forman una sucesión regular en $\mathbb{F}_q[Y_1, \ldots, Y_r]$, la variedad W_r es equidimensional de dimensión $r - m$. Esto implica que V_r es equidimensional de dimensión $r - m$. Por otro lado, notemos que, si para $1 \leq j \leq m$ definimos la variedad afín $W_r^j := V(S_1, \ldots, S_j) \subset \mathbb{A}^r$, entonces W_r^j es equidimensional de dimensión $r - j$. Esto implica que la variedad afín $V_r^j := \Pi_r^{-1}(W_r^j)$ definida por los polinomios $R_1, \ldots, R_j$ es equidimensional de dimensión $r - j$ para todo j $(1 \leq j \leq m)$. Por lo tanto, los polinomios $R_1, \ldots, R_m$ forman una sucesión regular en $\mathbb{F}_q[X_1, \ldots, X_r]$ y hemos probado el siguiente resultado.

Lema 5.1.1. *Sea $V_r \subset \mathbb{A}^r$ la $\mathbb{F}_q$–variedad definida por $R_1, \ldots, R_m$. Entonces V_r es una intersección completa conjuntista de dimensión $r - m$.*

5.2. La dimensión del lugar singular

Con el objetivo de aplicar nuestras estimaciones a este tipo de variedades, estudiamos la dimensión del lugar singular de V_r. Para esto, consideramos el siguiente morfismo de $\mathbb{F}_q$-variedades:

$$\begin{aligned} \Pi : V_r &\to W_s \\ x &\mapsto (\Pi_1(x), \ldots, \Pi_s(x)). \end{aligned}$$

Para $x \in V_r$ e $y := \Pi(x)$, denotamos por $\mathcal{T}_x V_r$ y $\mathcal{T}_y W_s$ los espacios tangentes de V_r en x y de W_s en y respectivamente. También consideramos la diferencial de Π en x, es decir,

$$\begin{aligned} \mathrm{d}_x\Pi : \mathcal{T}_x V_r &\to \mathcal{T}_y W_s \\ \boldsymbol{v} &\mapsto A(x) \cdot \boldsymbol{v}, \end{aligned}$$

donde $A(x)$ es la siguiente matriz de tamaño $s \times r$:

$$A(x) := \left(\frac{\partial \Pi}{\partial \boldsymbol{X}}\right)(x) := \left(\frac{\partial \Pi_i}{\partial X_j}(x)\right)_{1 \leq i \leq s,\, 1 \leq j \leq r}. \tag{5.1}$$

Hacemos a continuación algunas observaciones acerca de la matriz Jacobiana de los polinomios simétricos elementales. En primer lugar, es sabido que las derivadas parciales de los polinomios simétricos elementales Π_i satisfacen las siguientes igualdades para $1 \leq i, j \leq r$ (ver [LP02]):

$$\frac{\partial \Pi_i}{\partial X_j} = \Pi_{i-1} - X_j \Pi_{i-2} + X_j^2 \Pi_{i-3} + \cdots + (-1)^{i-1} X_j^{i-1}. \tag{5.2}$$

En consecuencia, si denotamos como $A_r := (X_j^{i-1})_{1 \leq i,j \leq r}$ la matriz de Vandermonde de tamaño $r \times r$, deducimos que la matriz Jacobiana de $\Pi_1, \ldots, \Pi_r$ con respecto a $X_1, \ldots, X_r$ se puede expresar de la siguiente manera:

$$\left(\frac{\partial \Pi_i}{\partial X_j}\right)_{1 \leq i,j \leq r} := B_r \cdot A_r := \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ \Pi_1 & -1 & 0 & & \\ \Pi_2 & -\Pi_1 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ \Pi_{r-1} & -\Pi_{r-2} & \Pi_{r-3} & \cdots & (-1)^{r-1} \end{pmatrix} \cdot A_r. \tag{5.3}$$

Observemos que B_r es una matriz cuadrada y triangular inferior cuyo determinante es igual a $(-1)^{(r-1)r/2}$. Esto implica que el determinante de la matriz $(\partial \Pi_i / \partial X_j)_{1 \leq i,j \leq r}$ es igual, salvo el signo, al determinante de A_r, es decir,

$$\det \left(\frac{\partial \Pi_i}{\partial X_j}\right)_{1 \leq i,j \leq r} = (-1)^{(r-1)r/2} \prod_{1 \leq i < j \leq r} (X_j - X_i).$$

Notemos por $(\partial \boldsymbol{R} / \partial \boldsymbol{X}) := (\partial R_i / \partial X_j)_{1 \leq i \leq m, 1 \leq j \leq r}$ a la matriz Jacobiana de los polinomios $R_1, \ldots, R_m$ con respecto a $X_1, \ldots, X_r$.

Teorema 5.2.1. *El conjunto de puntos $x \in \mathbb{A}^r$ para los cuales $(\partial \boldsymbol{R} / \partial \boldsymbol{X})(x)$ no tiene rango completo tiene dimensión a lo sumo $s-1$. En particular, el lugar singular Σ_r de V_r tiene dimensión a lo sumo $s-1$.*

Demostración. De acuerdo a la regla de la cadena, las derivadas parciales de los polinomios R_i satisfacen la siguiente igualdad:

$$\left(\frac{\partial \boldsymbol{R}}{\partial \boldsymbol{X}}\right) = \left(\frac{\partial \boldsymbol{S}}{\partial \boldsymbol{Y}} \circ \Pi\right) \cdot \left(\frac{\partial \Pi}{\partial \boldsymbol{X}}\right).$$

Fijemos un punto arbitrario x para el cual $(\partial \boldsymbol{R} / \partial \boldsymbol{X})(x)$ no tiene rango completo. Sea $\boldsymbol{v} \in \mathbb{A}^m$ un vector no nulo en el núcleo a izquierda de $(\partial \boldsymbol{R} / \partial \boldsymbol{X})(x)$. Entonces,

$$\boldsymbol{0} = \boldsymbol{v} \cdot \left(\frac{\partial \boldsymbol{R}}{\partial \boldsymbol{X}}\right)(x) = \boldsymbol{v} \cdot \left(\frac{\partial \boldsymbol{S}}{\partial \boldsymbol{Y}}\right)\big(\Pi(x)\big) \cdot A(x),$$

donde $A(x)$ es la matriz definida en (5.1). Por la hipótesis (H2), la matriz Jacobiana $(\partial \boldsymbol{S} / \partial \boldsymbol{Y})\big(\Pi(x)\big)$ tiene rango máximo; por lo tanto, el vector $\boldsymbol{w} := \boldsymbol{v} \cdot$

$(\partial \boldsymbol{S}/\partial \boldsymbol{Y})\big(\Pi(x)\big) \in \mathbb{A}^s$ es no nulo y se verifica $\boldsymbol{w} \cdot A(x) = \mathbf{0}$. De aquí se deduce que todos los menores maximales de la matriz $A(x)$ deben ser cero.

Observemos que $A(x)$ es la submatriz de $(\partial \Pi_i/\partial X_j)_{1\leq i,j\leq r}(x)$ de tamaño $s \times r$ que se obtiene al considerar las primeras s filas de $(\partial \Pi_i/\partial X_j)_{1\leq i,j\leq r}(x)$. Por lo tanto, de (5.3) concluimos que

$$A(x) = B_{s,r}(x) \cdot A_r(x),$$

donde $B_{s,r}(x)$ es la submatriz de $B_r(x)$ de tamaño $s \times r$ que consiste en las primeras s filas de $B_r(x)$. Dado que las últimas $r - s$ columnas de $B_{s,r}(x)$ son nulas, podemos reescribir la identidad anterior de la siguiente manera:

$$A(x) = B_s(x) \cdot (x_j^{i-1})_{1\leq i\leq s,\, 1\leq j\leq r} \tag{5.4}$$

donde $B_s(x)$ es la submatriz $B_r(x)$ de tamaño $s \times s$, que se obtiene al considerar las primeras s filas y las primeras s columnas de $B_r(x)$.

Para $1 \leq l_1 < \cdots < l_s \leq r$, sea $I := (l_1, \ldots, l_s)$ y consideremos la submatriz $M_I(x)$ de $A(x)$ de tamaño $s\times s$ que se obtiene al elegir las columnas $l_1, \ldots, l_s$ de $A(x)$, es decir, $M_I(x) := (\partial \Pi_i/\partial X_{l_j})_{1\leq i,j\leq s}(x)$. De (5.3) y (5.4) deducimos que $M_I(x) = B_s(x) \cdot A_{s,I}(x)$, donde $A_{s,I}(x)$ es la matriz de Vandermonde $A_{s,I}(x) := (x_{l_j}^{i-1})_{1\leq i,j\leq s}$. En consecuencia,

$$\det\big(M_I(x)\big) = (-1)^{\frac{(s-1)s}{2}} \det A_{s,I}(x) = (-1)^{\frac{(s-1)s}{2}} \prod_{1\leq m<n\leq s} (x_{l_n} - x_{l_m}) = 0. \tag{5.5}$$

Como (5.5) es válido para todo $I := (l_1, \ldots, l_s)$ elegido como arriba, concluimos que x tiene a lo sumo $s - 1$ coordenadas distintas. En particular, el conjunto de puntos x para los cuales $\operatorname{rg}(\partial \boldsymbol{R}/\partial \boldsymbol{X})(x) < m$ está contenido en una unión finita de subespacios de $\mathbb{A}^r$ de dimensión $s - 1$, y por lo tanto resulta ser una variedad afín de dimensión a lo sumo $s - 1$.

Finalmente, sea x un punto arbitrario de Σ_r. Por el Lema 5.1.1 se tiene $\dim \mathcal{T}_x V_r > r - m$. Esto implica que $\operatorname{rg}\left(\partial \boldsymbol{R}/\partial \boldsymbol{X}\right)(x) < m$, pues de otra forma $\dim \mathcal{T}_x V_r = r - m$, lo que contradiría que x es un punto singular de V_r. □

Observemos que en la demostración del Teorema 5.2.1 se da la siguiente descripción más precisa del lugar singular de V_r.

Observación 5.2.2. *Bajo las mismas hipótesis del Teorema 5.2.1, se tiene*

$$\Sigma_r \subset \bigcup_{\mathcal{I}} \mathcal{L}_{\mathcal{I}},$$

donde $\mathcal{I} := \{I_1, \ldots, I_{s-1}\}$ *recorre todas las particiones de* $\{1, \ldots, r\}$ *en* $s - 1$ *subconjuntos no vacíos* $I_j \subset \{1, \ldots, r\}$ *y* $\mathcal{L}_{\mathcal{I}}$ *es el subespacio*

$$\mathcal{L}_{\mathcal{I}} := \operatorname{span}(\mathbf{v}^{(I_1)}, \ldots, \mathbf{v}^{(I_{s-1})})$$

generada por los vectores $\mathbf{v}^{(I_j)} := (v_1^{(I_j)}, \ldots, v_r^{(I_j)})$ *definidos por* $v_m^{(I_j)} := 1$ *para* $m \in I_j$ *y* $v_m^{(I_j)} := 0$ *para* $m \notin I_j$.

A partir del Lema 5.1.1 y el Teorema 5.2.1 se obtienen más propiedades algebraicas y geométricas de los polinomios R_i y de la variedad V_r. Por el Teorema 5.2.1 se tiene que el conjunto de puntos $x \in \mathbb{A}^r$ para los cuales la matriz $(\partial \boldsymbol{R}/\partial \boldsymbol{X})(x)$ no tiene rango completo tiene dimensión a lo sumo $s-1$. Como $R_1, \ldots, R_m$ forman una sucesión regular y $s-1 \leq r-m-1$ concluimos, de acuerdo a [Eis95, Theorem 18.15], que $R_1, \ldots, R_m$ definen un ideal radical de $\mathbb{F}_q[X_1, \ldots, X_r]$. Finalmente, por la desigualdad de Bézout (2.2), se tiene que $\deg V_r \leq \prod_{i=1}^m \deg R_i$. En otras palabras, obtenemos el siguiente resultado.

Corolario 5.2.3. *Los polinomios $R_1, \ldots, R_m$ definen un ideal radical y la variedad V_r tiene grado a lo sumo* $\deg V_r \leq \prod_{i=1}^m \deg R_i$.

Capítulo 6

Una aplicación a la teoría de códigos

En este capítulo combinaremos los resultados geométricos obtenidos en el Capítulo 5 sobre intersecciones completas simétricas con las estimaciones para intersecciones completas singulares del Capítulo 3 a fin de resolver un problema concreto de teoría de códigos. El problema que estudiaremos consiste en determinar condiciones bajo las cuales una palabra recibida es un *deep hole* en códigos de Reed-Solomon. El interés en el estudio de los *deep holes* se debe a la dificultad que éstos presentan para su decodificación.

6.1. Códigos de Reed-Solomon

En esta sección haremos una revisión de los conceptos básicos de la teoría de códigos de Reed-Solomon que nos permiten entender el contexto del problema a estudiar. Para una exposición más detallada sobre teoría de códigos en general, y códigos de Reed-Solomon en particular, referimos al lector a [LN83, Chapter 9], [CLO98, Chapter 9] y [HP03].

Existen diversos motivos para querer codificar un mensaje: almacenamiento de datos, ocultar su contenido a terceras personas (criptografía), transmitir información a través de un canal ruidoso que puede introducir errores en el mensaje. En este último caso, uno codifica el mensaje para poder detectar y/o corregir errores que eventualmente pueden producirse en la transmisión. La teoría de códigos autocorrectores se ocupa de la codificación de mensajes para hacer más confiable y eficiente su transmisión por un canal ruidoso, así como también de la decodificación y del problema de detectar y corregir errores. Uno de los más importantes códigos autocorrectores son los códigos de Reed-Solomon.

En teoría de códigos, típicamente se tiene un conjunto finito de símbolos llamado alfabeto y un método de codificación de palabras (de longitud finita) en dicho alfabeto. Una palabra codificada se llama una palabra del código y el conjunto de estas palabras es lo que llamamos el código. En la teoría algebraica de códigos es común considerar al alfabeto como un cuerpo finito $\mathbb{F}_q$ y las palabras a codificar

como sucesiones de elementos de $\mathbb{F}_q$ de longitud fija k. El proceso de codificación se traduce matemáticamente como una función inyectiva $\alpha : \mathbb{F}_q^k \to \mathbb{F}_q^n$ con $k \leq n$ y el código es el conjunto imagen de α. Si bien en principio el código es un subconjunto de $\mathbb{F}_q^n$, en general se suelen estudiar aquellos códigos que posean alguna estructura algebraica que facilite la codificación y la decodificación. Un código lineal es uno que tiene estructura de $\mathbb{F}_q$-espacio vectorial sobre $\mathbb{F}_q^n$. Los códigos de Reed-Solomon son un tipo especial de códigos lineales.

Dado un subconjunto $\mathsf{D} := \{x_1, \ldots, x_n\} \subset \mathbb{F}_q$ y un entero positivo $k \leq n$, el código de Reed–Solomon de longitud n y dimensión k sobre $\mathbb{F}_q$ es el siguiente subespacio de $\mathbb{F}_q^n$:

$$C(\mathsf{D}, k) := \{(f(x_1), \ldots, f(x_n)) : f \in \mathbb{F}_q[T], \deg f \leq k-1\}.$$

El conjunto D se llama el conjunto de evaluación. Cuando $\mathsf{D} = \mathbb{F}_q^*$, el grupo de unidades de $\mathbb{F}_q$, $C(\mathsf{D}, k)$ se llama el código de Reed–Solomon estándar.

Las siguientes definiciones son estándar en teoría de códigos. Sea $C \subset \mathbb{F}_q^n$ un código. Dados $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, la distancia de Hamming entre $\mathbf{x}$ e $\mathbf{y}$ se define como

$$\mathsf{d}(\mathbf{x}, \mathbf{y}) = \mid \{j : x_j \neq y_j,\ 1 \leq j \leq n\} \mid,$$

es decir, como la cantidad de coordenadas en las que $\mathbf{x}$ e $\mathbf{y}$ difieren. Para $\mathbf{w} \in \mathbb{F}_q^n$, la distancia de $\mathbf{w}$ al código C es

$$\mathsf{d}(\mathbf{w}, C) := \min_{\mathbf{c} \in C} \mathsf{d}(\mathbf{w}, \mathbf{c}).$$

La distancia mínima $\mathsf{d}(C)$ de C es la distancia más pequeña entre dos palabras código distintas. El radio de recubrimiento de C se define como

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

Con esta terminología, decimos que una palabra $\mathbf{w} \in \mathbb{F}_q^n$ es un deep hole si $\mathsf{d}(\mathbf{w}, C) = \rho$, es decir, la palabra recibida es un deep hole si en la transmisión se produjo la mayor cantidad de errores posibles. En el caso del código de Reed-Solomon de longitud n y dimensión k sobre $\mathbb{F}_q$, es fácil ver que $\mathsf{d}(C) = n - k + 1$ y $\rho = n - k$.

Uno de los problemas algorítmicos más importantes en la teoría de códigos es el de la decodificación por "mayor cercanía" (*maximum–likelihood decoding*, MLD), que consiste en calcular la palabra del código más cercana a una palabra recibida $\mathbf{w} \in \mathbb{F}_q^n$. En el caso de códigos de Reed-Solomon, M. Sudan por un lado [Sud97], y V. Guruswami y Sudan por el otro [GS99], dan un algoritmo que en tiempo polinomial calcula la palabra del código más cercana a $\mathbf{w}$ cuando $d(\mathbf{w}, C) \leq n - \sqrt{nk}$. Cuando la distancia $d(\mathbf{w}, C)$ aumenta, la decodificación se complica; de hecho, es sabido que el problema MLD es NP-completo ([GV05]; ver también [CM07b]).

Para códigos de Reed-Solomon, resolver el problema MLD para $\mathbf{w} := (w_1, \ldots, w_n) \in \mathbb{F}_q^n$ consiste en encontrar un polinomio $f \in \mathbb{F}_q[T]$ de grado a lo sumo $k-1$ que cumpla la mayor cantidad posible de condiciones $f(x_i) = w_i$ para $1 \leq i \leq n$. Es claro que, por interpolación, existe un único polinomio $f_{\mathbf{w}}$ de grado a lo sumo $n-1$

que verifica $f_{\mathbf{w}}(x_i) = w_i$ para $1 \leq i \leq n$. En este caso, decimos que la palabra $\mathbf{w}$ es generada por $f_{\mathbf{w}}$. Notar que si el grado de $f_{\mathbf{w}}$ es menor o igual a $k-1$ entonces $\mathbf{w}$ es una palabra del código.

Un problema abierto en teoría de códigos de Reed-Solomon es el de caracterizar todos los deep holes. En este contexto, un deep hole está generado por un polinomio $f \in \mathbb{F}_q[T]$ con $k \leq \deg f \leq n-1$. Más aún, se tiene el siguiente resultado.

Proposición 6.1.1 ([CM07b, Corollary 1])**.** *Los polinomios de grado k generan deep holes. Luego, hay al menos $(q-1)q^k$ deep holes (llamados deep holes triviales).*

En 2007, Q. Cheng y E. Murray [CM07b] conjeturaron que los únicos deep holes en el código de Reed–Solomon estándar son los generados por polinomios de grado k. Sin embargo, R. Wu y S. Hong [WH12] probaron 5 años más tarde que esta conjetura es falsa. Concretamente, muestran que en el caso $q > 4$ y $k \leq q-2$, existen deep holes generados por polinomios de grado $q-2$ en el código $C(\mathbb{F}_q^*, k)$. Más ejemplos de deep holes generados por polinomios de grado mayor a k se pueden encontrar en [ZFL12].

Una caracterización más precisa del conjunto de polinomios $f \in \mathbb{F}_q[T]$ que son candidatos a generar deep holes es la siguiente. Supongamos que recibimos una palabra $\mathbf{w} \in \mathbb{F}_q^n$, generada por un polinomio $f_{\mathbf{w}} \in \mathbb{F}_q[T]$ de grado mayor a k, y queremos saber si $\mathbf{w}$ es un deep hole. Descompongamos a $f_{\mathbf{w}}$ como $f_{\mathbf{w}} = g + h$, donde g es la suma de los monomios de $f_{\mathbf{w}}$ de grado mayor o igual a k y h es la suma de los monomios de grado menor o igual a $k-1$, y consideremos las palabras $\mathbf{w}_g$ y $\mathbf{w}_h$ generadas por g y h respectivamente. Observemos que $\mathbf{w}_h$ es una palabra del código. Sea $\mathbf{u} \in C$ la palabra del código que verifica que $\mathsf{d}(\mathbf{w}, \mathbf{u}) = \mathsf{d}(\mathbf{w}, C)$. Teniendo en cuenta las identidades

$$\mathsf{d}(\mathbf{w}, C) = \mathsf{d}(\mathbf{w}, \mathbf{u}) = \mathsf{d}(\mathbf{w} - \mathbf{w}_h, \mathbf{u} - \mathbf{w}_h) = \mathsf{d}(\mathbf{w}_g, \mathbf{u} - \mathbf{w}_h)$$

y el hecho de que $\mathbf{u} - \mathbf{w}_h \in C$, concluimos que

$$\mathsf{d}(\mathbf{w}_g, C) \leq \mathsf{d}(\mathbf{w}, C).$$

Por otro lado, para $\mathbf{u}' \in C$ con $\mathsf{d}(\mathbf{w}_g, C) = \mathsf{d}(\mathbf{w}_g, \mathbf{u}')$, obtenemos

$$\mathsf{d}(\mathbf{w}_g, C) = \mathsf{d}(\mathbf{w}_g, \mathbf{u}') = \mathsf{d}(\mathbf{w}_g + \mathbf{w}_h, \mathbf{u}' + \mathbf{w}_h) = \mathsf{d}(\mathbf{w}, \mathbf{u}' + \mathbf{w}_h) \geq \mathsf{d}(\mathbf{w}, C).$$

Por lo tanto deducimos que $\mathsf{d}(\mathbf{w}, C) = \mathsf{d}(\mathbf{w}_g, C)$. Esto implica que $\mathbf{w}$ es un deep hole si y sólo si $\mathbf{w}_g$ es un deep hole. De este razonamiento se sigue que un deep hole del código de Reed-Solomon C es obtenido como la palabra $\mathbf{w}_f$ generada por un polinomio $f \in \mathbb{F}_q[T]$ de la forma

$$f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0 T^k, \tag{6.1}$$

donde d es un entero no negativo con $k + d < q - 1$. Notar que, de acuerdo a la Proposición 6.1.1, podemos suponer $d \geq 1$.

Sea de ahora en más $C := C(\mathbb{F}_q^*, k)$. Cheng y Murray abordan el problema de caracterizar los deep holes de C relacionando su existencia con la inexistencia de

puntos q-racionales de una cierta familia de hipersuperficies. Su razonamiento es el siguiente. Fijemos un polinomio $f \in \mathbb{F}_q[T]$ como en (6.1) y sea $\mathbf{w}_f$ la palabra que éste genera. Sean $X_1, \ldots, X_{k+1}$ indeterminadas sobre $\overline{\mathbb{F}}_q$ y $Q \in \mathbb{F}_q[X_1, \ldots, X_{k+1}][T]$ el polinomio

$$Q = (T - X_1) \cdots (T - X_{k+1}).$$

Existe un polinomio $R_f \in \mathbb{F}_q[X_1, \ldots, X_{k+1}][T]$ con $\deg_T R_f \leq k$ que verifica la siguiente condición:

$$f \equiv R_f \mod Q. \tag{6.2}$$

Supongamos que R_f tiene grado k y denotemos por $H_f \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ a su coeficiente principal. Supongamos que existe un vector $\mathbf{x} \in (\mathbb{F}_q^*)^{k+1}$ con coordenadas distintas dos a dos tal que $H_f(\mathbf{x}) = 0$. Esto implica que $r := R_f(\mathbf{x}, T)$ tiene grado a lo sumo $k-1$ y, por lo tanto, genera una palabra del código $\mathbf{w}_r$. De (6.2) deducimos que

$$d(\mathbf{w}_f, C) \leq d(\mathbf{w}_f, \mathbf{w}_r) \leq q - k - 2,$$

y, por lo tanto, $\mathbf{w}_f$ no es un deep hole.

En consecuencia, un polinomio f no genera un deep hole de C si y sólo si existe un cero $\mathbf{x} := (x_1, \ldots, x_{k+1}) \in \mathbb{F}_q^{k+1}$ de H_f con coordenadas no nulas, distintas dos a dos, es decir, si existe una solución $\mathbf{x} \in \mathbb{F}_q^{k+1}$ del siguiente sistema de igualdades y desigualdades:

$$H_f(X_1, \ldots, X_{k+1}) = 0, \quad \prod_{1 \leq i < j \leq k+1} (X_i - X_j) \neq 0, \quad \prod_{1 \leq i \leq k+1} X_i \neq 0.$$

Para cada $f \in \mathbb{F}_q[T]$ definido como en (6.1), notamos por V_f a la hipersuperficie dada por el polinomio H_f. Cheng y Murray probaron que cada hipersuperficie V_f es absolutamente irreducible. Esto les permitió obtener condiciones suficientes para la inexistencia de deep holes de C utilizando la estimación de [CM06]. Más precisamente, obtuvieron el siguiente resultado.

Teorema 6.1.2 ([CM07b, Theorem 1]). *Sean k, d enteros positivos, q un número primo y ϵ una constante positiva. Si $q > \max\{k^{4+\epsilon}, d^{13/3+\epsilon}\}$ entonces una palabra $\mathbf{w}_f$ generada por un polinomio $f \in \mathbb{F}_q[T]$ de grado $k + d < q - 1$ no es un deep hole del código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$.*

Por otro lado, Y.-J. Li y D. Wan [LW08b] probaron el siguiente resultado utilizando la estimación de Weil para ciertas sumas de caracteres.

Teorema 6.1.3 ([LW08b, Theorem 1.4]). *Sean k, d enteros positivos, q es una potencia de un primo y ϵ una constante positiva. Si $q > \max\{d^{2+\epsilon}, (k+1)^2\}$ y $k > (\frac{2}{\epsilon} + 1)d + \frac{8}{\epsilon} + 2$, entonces una palabra $\mathbf{w}_f$ generada por un polinomio $f \in \mathbb{F}_q[T]$ de la forma (6.1) y de grado $k + d < q - 1$ no es un deep hole en el código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$.*

En esta tesis retomaremos el enfoque de Cheng y Murray, estudiando en detalle la geometría de las hipersuperficies V_f. Mostraremos que los polinomios $H_f \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ se pueden expresar como polinomios en los primeros d polinomios

simétricos elementales, lo que nos permitirá aplicar los resultados del Capítulo 5 y obtener información relevante sobre la dimensión del lugar singular de V_f. Finalmente, combinaremos este resultado con la estimación de puntos q-racionales de Ghorpade y Lachaud [GL02a] y obtendremos condiciones suficientes para la inexistencia de deep holes en códigos de Reed-Solomon estándar que mejoran [CM07b] y [LW08b].

6.2. H_f en términos de los polinomios simétricos elementales

Consideramos enteros positivos d y k tales que $d < k$ y los primeros d polinomios simétricos elementales $\Pi_1, \ldots, \Pi_d$ en $\mathbb{F}_q[X_1, \ldots, X_{k+1}]$. Notamos $\Pi_0 := 1$. En la sección anterior asociamos un polinomio $H_f \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ a cada polinomio $f \in \mathbb{F}_q[T]$ de grado $k+d$ definido como en (6.1) y llamamos $V_f \subset \mathbb{A}^{k+1}$ a la $\mathbb{F}_q$-hipersuperficie definida por H_f. Recordemos que la palabra $\mathbf{w}_f$ generada por el polinomio f no es un deep hole del código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$ si H_f tiene un cero q-racional con coordenadas no nulas distintas dos a dos. Con el objetivo de aplicar a V_f los resultados obtenidos en el Capítulo 5, vamos a mostrar cómo los polinomios H_f pueden ser expresados en términos de los polinomios simétricos elementales $\Pi_1, \ldots, \Pi_d$. Para esto, primero obtenemos una expresión recursiva del polinomio H_d asociado al monomio T^{k+d}.

Lema 6.2.1. *Si $1 \leq r \leq d$, vale la siguiente igualdad:*

$$H_r = \Pi_1 H_{r-1} - \Pi_2 H_{d-2} + \cdots + (-1)^{r-1} \Pi_r H_0, \tag{6.3}$$

siendo $H_0 := 1$.

Demostración. Consideramos nuevamente el polinomio $Q := (T - X_1) \cdots (T - X_{k+1})$. Se tiene que

$$T^{k+1} \equiv \Pi_1 T^k - \Pi_2 T^{k-1} + \cdots + (-1)^{d-1} \Pi_d T^{k-(d-1)} + \cdots + (-1)^k \Pi_{k+1} \mod Q.$$

Multiplicando esta relación de congruencia por T^{r-1} obtenemos

$$T^{k+r} \equiv \Pi_1 T^{k+r-1} - \Pi_2 T^{k+r-2} + \cdots + (-1)^{r-1} \Pi_r T^k + \mathcal{O}(T^{k-1}) \mod Q,$$

donde $\mathcal{O}(T^{k-1})$ representa la suma de los términos de $\mathbb{F}_q[X_1, \ldots, X_{k+1}][T]$ de grado a lo sumo $k-1$ en T. Tenemos que H_{r-j} es el único polinomio de $\mathbb{F}_q[X_1, \ldots, X_{k+1}]$ que satisface la relación de congruencia

$$T^{k+r-j} \equiv H_{r-j} T^k + \mathcal{O}(T^{k-1}) \mod Q$$

para $1 \leq j \leq r-1$. Por lo tanto, obtenemos la igualdad

$$H_r = \Pi_1 H_{r-1} - \Pi_2 H_{r-2} + \cdots + (-1)^{r-1} \Pi_r,$$

concluyendo así la demostración del lema. □

Nuestro próximo objetivo es obtener una expresión explícita del polinomio H_d en términos de los polinomios simétricos elementales. A partir de esto podremos conseguir rápidamente una expresión para el polinomio H_f, asociado al polinomio f definido en (6.1).

Proposición 6.2.2. *Sea $H_r \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ el polinomio asociado al monomio T^{k+r}, $1 \leq r \leq d$. Entonces se tiene la siguiente igualdad:*

$$H_r = \sum_{i_1+2i_2+\cdots+ri_r=r} (-1)^{\Delta(i_1,\ldots,i_r)} \frac{(i_1+\cdots+i_r)!}{i_1!\cdots i_r!} \Pi_1^{i_1} \cdots \Pi_r^{i_r}, \tag{6.4}$$

con $0 \leq i_j \leq r$ para $1 \leq j \leq r$, siendo $\Delta(i_1, \ldots, i_r) := i_2 + i_4 + \cdots + i_{2\lfloor r/2 \rfloor}$ la suma de los índices i_j para los cuales j es un número par.

Demostración. Hacemos inducción en r. El caso $r = 1$ se sigue de (6.3). Supongamos que $r > 1$ y que la fórmula (6.4) es válida para $1 \leq j \leq r-1$. De (6.4) concluimos que $H_j \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ es un polinomio homogéneo y simétrico de grado j para $1 \leq j \leq r-1$. Más aún, del Lema 6.2.1 deducimos que H_r es un polinomio homogéneo y simétrico de grado r. Asimismo, combinando la hipótesis inductiva y el Lema 6.2.1 se obtiene que H_r se puede expresar de la siguiente manera:

$$H_r = \sum_{i_1+\cdots+ri_r=r} a_{i_1,\ldots,i_r} \Pi_1^{i_1} \cdots \Pi_r^{i_r},$$

para ciertos elementos $a_{i_1,\ldots,i_r} \in \mathbb{F}_q$. Resta entonces demostrar que los términos $a_{i_1,\ldots,i_r}$ verifican la siguiente igualdad:

$$a_{i_1,\ldots,i_r} = (-1)^{\Delta(i_1,\ldots,i_r)} \frac{(i_1+\cdots+i_r)!}{i_1!\cdots i_r!}.$$

Sea $(i_1, \ldots, i_r) \in (\mathbb{Z}_{\geq 0})^r$ con $i_1 + 2i_2 + \cdots + ri_r = r$. Por el Lema 6.2.1 se tiene

$$a_{i_1,\ldots,i_r} = \sum_{j=1}^{r} (-1)^{j-1} (H_{r-j})_{i_1,\ldots,i_j-1,\ldots,i_r},$$

donde $(H_{r-j})_{i_1,\ldots,i_j-1,\ldots,i_r}$ es el coeficiente del monomio $\Pi_1^{i_1} \cdots \Pi_j^{i_j-1} \cdots \Pi_r^{i_r}$ en la expresión de H_{r-j} como polinomio en $\mathbb{F}_q[\Pi_1, \ldots, \Pi_r]$. Aplicando la hipótesis inductiva, obtenemos:

$$a_{i_1,\ldots,i_r} = \sum_{j=1}^{d} (-1)^{j-1} (-1)^{\Delta(i_1,\ldots,i_j-1,\ldots,i_r)} \frac{(i_1+\cdots+i_r-1)!}{i_1!\cdots(i_j-1)!\cdots i_r!}.$$

Si j es un número impar, entonces $\Delta(i_1, \ldots, i_j - 1, \ldots, i_r) = \Delta(i_1, \ldots, i_j, \ldots, i_r)$ y $(-1)^{j-1} = 1$, lo cual implica que $(-1)^{j-1+\Delta(i_1,\ldots,i_j-1,\ldots,i_r)} = (-1)^{\Delta(i_1,\ldots,i_j,\ldots,i_r)}$. Por otro lado, si j es un número par, se tiene que $(-1)^{j-1} = -1$ y $(-1)^{\Delta(i_1,\ldots,i_j,\ldots,i_r)} = (-1)^{j-1}(-1)^{\Delta(i_1,\ldots,i_j-1,\ldots,i_d)}$. Por lo tanto,

$$\begin{aligned} a_{i_1,\ldots,i_r} &= (-1)^{\Delta(i_1,\ldots,i_r)} (i_1+\cdots+i_r-1)! \frac{(i_1+\cdots+i_r)}{i_1!\ldots i_r!} \\ &= (-1)^{\Delta(i_1,\ldots,i_r)} \frac{(i_1+\cdots+i_r)!}{i_1!\ldots i_r!}. \end{aligned}$$

Esto concluye la demostración. □

Es interesante remarcar la similitud de la expresión para H_d con la fórmula de Waring que expresa la suma de potencias en términos de los polinomios simétricos elementales (ver, por ejemplo, [LN83, Theorem 1.76]).

Finalmente, obtenemos una expresión del polinomio H_f, asociado a un polinomio arbitrario $f \in \mathbb{F}_q[T]$ como (6.1), en términos de los polinomios simétricos elementales $\Pi_1, \ldots, \Pi_d$.

Proposición 6.2.3. *Sean* $f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0T^k \in \mathbb{F}_q[T]$ *y* $H_f \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ *el polinomio asociado a* f*. Se tiene entonces que*

$$H_f = H_d + f_{d-1}H_{d-1} + \cdots + f_1H_1 + f_0. \tag{6.5}$$

Demostración. En la demostración del Lema 6.2.1 obtenemos la siguiente relación de congruencia:

$$T^{k+d} \equiv \Pi_1 T^{k+d-1} - \Pi_2 T^{k+d-2} + \cdots + (-1)^{d-1}\Pi_d T^k + \mathcal{O}(T^{k-1}) \mod Q.$$

Luego, se tiene

$$T^{k+d} + \sum_{j=0}^{d-1} f_j T^{k+j} \equiv \sum_{j=0}^{d-1} \big((-1)^{d-1+j}\Pi_{d-j} + f_j\big)T^{k+j} + \mathcal{O}(T^{k-1}) \mod Q.$$

Por lo tanto, teniendo en cuenta que $T^{k+j} \equiv H_jT^k + \mathcal{O}(T^{k-1}) \mod Q$ para $1 \le j \le d-1$, obtenemos

$$\begin{aligned} f := T^{k+d} + \sum_{j=0}^{d-1} f_j T^{k+j} &\equiv \sum_{j=0}^{d-1} \big((-1)^{d-1+j}\Pi_{d-j} + f_j\big)H_jT^k + \mathcal{O}(T^{k-1}) \mod Q \\ &= \left(\sum_{j=0}^{d-1}(-1)^{d-1+j}\Pi_{d-j}H_j + \sum_{j=0}^{d-1} f_jH_j\right)T^k + \mathcal{O}(T^{k-1}) \\ &= \left(H_d + \sum_{j=0}^{d-1} f_jH_j\right)T^k + \mathcal{O}(T^{k-1}), \end{aligned}$$

donde la última igualdad es consecuencia del Lema 6.2.1. Esto prueba la validez de (6.5) y concluye la demostración. □

Observación 6.2.4. *Del Lema 6.2.1 y la Proposición 6.2.2 se sigue que* H_d *es un polinomio homogéneo de* $\mathbb{F}_q[X_1, \ldots, X_{k+1}]$ *de grado* d*, que puede ser expresado como un polinomio en los polinomios simétricos elementales* $\Pi_1, \ldots, \Pi_d$*. Además* H_d *tiene grado* 1 *en* Π_d *con coeficiente* $(-1)^{d-1}$*. Combinando estas observaciones y la Proposición 6.2.3 se tiene que, para un polinomio arbitrario* $f := T^{k+d} + f_{d-1}T^{k+d-1} + \cdots + f_0T^k \in \mathbb{F}_q[T]$*, el polinomio asociado* $H_f \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ *tiene grado* d *y es un elemento mónico de* $\mathbb{F}_q[\Pi_1, \ldots, \Pi_{d-1}][\Pi_d]$ *de la forma* $H_f = (-1)^{d-1}\Pi_d + \widehat{H}_f(\Pi_1, \ldots, \Pi_{d-1})$*.*

6.3. Propiedades de las hipersuperficies V_f

De acuerdo a la Observación 6.2.4, podemos escribir $H_f = G_f(\Pi_1, \ldots, \Pi_d)$, donde $G_f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ es un polinomio de grado d y es mónico de grado 1 en la variable Y_d y coeficiente $(-1)^{d-1}$. Más aún, se tiene

$$\nabla G_f(\mathbf{y}) = \left(\frac{\partial G_f}{\partial Y_1}(\mathbf{y}), \ldots, \frac{\partial G_f}{\partial Y_{d-1}}(\mathbf{y}), (-1)^{d-1} \right) \neq \mathbf{0}$$

para todo $\mathbf{y} \in \mathbb{A}^d$. Por lo tanto, el polinomio G_f define una hipersuperficie $W \subset \mathbb{A}^d$ no singular. En particular, G_f verifica las hipótesis (H_1) y (H_2) del comienzo del Capítulo 5, y podemos aplicar por ende los resultados geométricos de dicho capítulo al polinomio H_f. Más precisamente, de acuerdo al Teorema 5.2.1, obtenemos el siguiente resultado.

Corolario 6.3.1. *El lugar singular $\Sigma_f \subset \mathbb{A}^{k+1}$ de V_f tiene dimensión a lo sumo $d-1$. Más aún, Σ_f está contenido en una unión de variedades lineales de dimensión $d-1$.*

Con el objetivo de obtener estimaciones sobre la cantidad de puntos q-racionales de V_f necesitamos información del comportamiento de V_f "en el infinito". Consideremos entonces la clausura proyectiva $\mathrm{pcl}(V_f) \subset \mathbb{P}^{k+1}$ de V_f. Notar que $\mathrm{pcl}(V_f)$ es una $\mathbb{F}_q$-hipersuperficie de $\mathbb{P}^{k+1}$ definida por la homogeneización $H_f^h \in \mathbb{F}_q[X_0, \ldots, X_{k+1}]$ del polinomio H_f (ver, por ejemplo, [Kun85, §I.5, Exercise 6]).

Proposición 6.3.2. *El lugar singular de* $\mathrm{pcl}(V_f)$ *en el hiperplano del infinito tiene dimensión a lo sumo $d-2$.*

Demostración. Por la Proposición 6.2.3, se tiene

$$H_f = H_d + f_{d-1}H_{d-1} + \cdots + f_1 H_1 + f_0,$$

donde cada H_j es un polinomio homogéneo de grado j para $1 \leq j \leq d$. Luego, la homogeneización de H_f es el siguiente polinomio de $\mathbb{F}_q[X_0, \ldots, X_{k+1}]$:

$$H_f^h = H_d + f_{d-1}H_{d-1}X_0 + \cdots + f_1 H_1 X_0^{d-1} + f_0 X_0^d. \tag{6.6}$$

Sea $\Sigma_f^\infty \subset \mathbb{P}^{k+1}$ el lugar singular de $\mathrm{pcl}(V_f)$ en el hiperplano del infinito, es decir, el conjunto de puntos singulares de $\mathrm{pcl}(V_f)$ que pertenecen al hiperplano $\{X_0 = 0\}$. Dado $\mathbf{x} \in \Sigma_f^\infty$, se satisfacen las igualdades $H_f^h(\mathbf{x}) = 0$ y $\partial H_f^h/\partial X_i(\mathbf{x}) = 0$ para $0 \leq i \leq k+1$. Por lo tanto, de acuerdo a la fórmula (6.6) se tiene que un punto $\mathbf{x} := (0 : x_1 : \cdots : x_{k+1}) \in \Sigma_f^\infty$ satisface las igualdades

$$\begin{cases} H_d(x_1, \ldots, x_{k+1}) & = & 0 \\ f_{d-1}H_{d-1}(x_1, \ldots, x_{k+1}) & = & 0 \\ \dfrac{\partial H_d}{\partial X_i}(x_1, \ldots, x_{k+1}) & = & 0 \quad (1 \leq i \leq k+1). \end{cases} \tag{6.7}$$

Por la Proposición 6.2.2 y la Observación 6.2.4 se tiene que $H_d \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ es un polinomio homogéneo de grado d que puede expresarse en la forma $H_d = G_d(\Pi_1, \ldots, \Pi_d)$, donde $G_d \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ tiene grado d, con coeficiente $(-1)^{d-1}$ en la variable Y_d. Luego, por el Teorema 5.2.1 concluimos que el conjunto de soluciones del sistema (6.7) es un cono afín contenido en $\mathbb{A}^{k+1}$ de dimensión a lo sumo $d-1$, y en consecuencia, resulta una variedad proyectiva contenida en $\mathbb{P}^k$ de dimensión a lo sumo $d-2$. □

Corolario 6.3.3. *La hipersuperficie V_f es absolutamente irreducible.*

Demostración. En primer lugar, notemos que V_f es absolutamente irreducible si y sólo si $\mathrm{pcl}(V_f)$ lo es (ver, por ejemplo, [Kun85, Chapter I, Proposition 5.17]). Si $\mathrm{pcl}(V_f)$ no es absolutamente irreducible, entonces tiene una descomposición no trivial en componentes absolutamente irreducibles

$$\mathrm{pcl}(V_f) = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_s,$$

donde $\mathcal{C}_1, \ldots, \mathcal{C}_s$ son hipersuperficies proyectivas contenidas en $\mathbb{P}^{k+1}$. Como $\mathcal{C}_i \cap \mathcal{C}_j \neq \emptyset$ y $\mathcal{C}_i$, $\mathcal{C}_j$ son absolutamente irreducibles, se tiene $\dim(\mathcal{C}_i \cap \mathcal{C}_j) = k-1$. Sea Σ_f^h el lugar singular de $\mathrm{pcl}(V_f)$. De acuerdo al Corolario 6.3.1 y la Proposición 6.3.2 se tiene $\dim \Sigma_f^h \leq d-1$. Por otro lado, $\mathcal{C}_i \cap \mathcal{C}_j \subset \Sigma_f^h$ para $i \neq j$, lo cual implica que $\dim \Sigma_f^h \geq k-1$. Esto contradice el hecho de que $\dim \Sigma_f^h \leq d-1$, pues $d < k$ por hipótesis. Vemos entonces que V_f es absolutamente irreducible. □

6.3.1. Cuando la dimensión del lugar singular de V_f es $d-1$

En esta sección daremos una caracterización del conjunto de polinomios $f \in \mathbb{F}_q[T]$ para los cuales el lugar singular de V_f tiene dimensión $d-1$. Esta caracterización nos permitirá dar condiciones bajo las cuales dichos polinomios no generan deep holes del código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$.

En primer lugar obtenemos una fórmula para las derivadas parciales del polinomio H_d asociado a T^{k+d}.

Lema 6.3.4. *Dado $j \geq 2$, las derivadas parciales de los polinomios H_j satisfacen la siguiente igualdad para $1 \leq i \leq k+1$:*

$$\frac{\partial H_j}{\partial X_i} = H_{j-1} + H_{j-2}X_i + \cdots + H_{j-3}X_i^2 + \cdots + X_i^{j-1}.$$

Demostración. Hacemos inducción en j. Por el Lema 6.2.1 se tiene que $H_1 = \Pi_1$ y $H_2 = \Pi_1 H_1 - \Pi_2$. Combinando estas igualdades con la fórmula (5.2) se deduce fácilmente nuestra afirmación para $j = 2$. Supongamos ahora que la afirmación del lema es válida para $2 \leq j \leq l-1$. De acuerdo al Lema 6.2.1, se tiene

$$\frac{\partial H_l}{\partial X_i} = \sum_{m=1}^{l} (-1)^{m-1} \frac{\partial(\Pi_m H_{l-m})}{\partial X_i}. \tag{6.8}$$

Teniendo en cuenta la hipótesis inductiva y la expresión (5.2) para las derivadas parciales de los polinomios simétricos elementales, cada término del lado derecho de (6.8) puede ser expresado de la siguiente manera:

$$\frac{\partial(\Pi_m H_{l-m})}{\partial X_i} = H_{l-m}\sum_{n=1}^{m}(-1)^{n-1}\Pi_{m-n}X_i^{n-1} + \Pi_m\sum_{n=1}^{l-m}H_{l-(m+n)}X_i^{n-1}. \tag{6.9}$$

Determinemos el coeficiente de H_{l-m} en el lado derecho de (6.8). A partir de la fórmula (6.9) observamos que los únicos términos que aportan al coeficiente de H_{l-m} son $\partial(\Pi_n H_{l-n})/\partial X_i$ para $1 \leq n \leq m$. En particular, deducimos que H_{l-1} es igual a 1. Para $1 \leq n < m$, el sumando $(-1)^{n-1}\partial(\Pi_n H_{l-n})/\partial X_i$ aporta el término $(-1)^{n-1}X_i^{m-n-1}\Pi_n$. Por otro lado, el sumando $(-1)^{m-1}\partial(\Pi_m H_{l-m})/\partial X_i$ en el lado derecho de (6.8) contribuye con la suma $(-1)^{m-1}\sum_{n=0}^{m-1}(-1)^{m-n-1}\Pi_n X_i^{m-n-1}$. Si agrupamos todos estos términos, concluimos que el coeficiente de H_{l-m} en (6.8) es

$$(-1)^{m-1}\sum_{n=0}^{m-1}(-1)^{m-n-1}\Pi_n X_i^{m-n-1} + \sum_{n=1}^{m-1}(-1)^{n-1}\Pi_n X_i^{m-n-1} = X_i^{m-1}.$$

Esto concluye la demostración del lema. □

Notemos que, de manera similar a la factorización (5.3) de la matriz Jacobiana de los polinomios simétricos elementales, el Lema 6.3.4 nos permite factorizar la matriz Jacobiana de los polinomios $H_1, \ldots, H_{k+1}$ con respecto a las variables $X_1, \ldots, X_{k+1}$ de la siguiente manera:

$$\left(\frac{\partial H_i}{\partial X_j}\right)_{1\leq i,j\leq k+1} = \begin{pmatrix} H_0 & 0 & \cdots & 0 \\ H_1 & H_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ H_k & H_{k-1} & \ldots & H_0 \end{pmatrix} \cdot A_{k+1}, \tag{6.10}$$

donde A_{k+1} es la matriz de Vandermonde de tamaño $(k+1)\times(k+1)$ en las variables $X_1, \ldots, X_{k+1}$.

En el Corolario 6.3.1 probamos que el lugar singular Σ_f de V_f tiene dimensión a lo sumo $d-1$. Supongamos ahora que la dimensión de Σ_f es igual a $d-1$. De acuerdo a la Observación 5.2.2 existe una partición $\mathcal{I} := \{I_1, \ldots, I_{d-1}\}$ del conjunto $\{1, \ldots, k+1\}$ en $d-1$ subconjuntos no vacíos $I_j \subset \{1, \ldots, k+1\}$ con la propiedad de que, si $\mathcal{L}_\mathcal{I} \subset \mathbb{A}^{k+1}$ es la variedad lineal

$$\mathcal{L}_\mathcal{I} := \operatorname{span}(\mathbf{v}^{(I_1)}, \ldots, \mathbf{v}^{(I_{d-1})})$$

generada por los vectores $\mathbf{v}^{(I_j)} := (v_1^{(I_j)}, \ldots, v_{k+1}^{(I_j)})$ definidos por $v_l^{(I_j)} := 1$ para $l \in I_j$ y $v_l^{(I_j)} := 0$ para $l \notin I_j$, $1 \leq j \leq d-1$, entonces $\mathcal{L}_\mathcal{I} \subset \Sigma_f$. Sean $\lambda := (\lambda_1, \ldots, \lambda_{d-1}) \in \mathbb{A}^{d-1}$ y $\mathbf{x} := \sum_{j=1}^{d-1}\lambda_j \mathbf{v}^{(I_j)}$ un punto arbitrario de $\mathcal{L}_\mathcal{I}$. Como $\mathbf{x}$ es un punto singular de V_f se tiene que

$$0 = \frac{\partial H_f}{\partial X_i}(\mathbf{x}) = \frac{\partial H_d}{\partial X_i}(\mathbf{x}) + \sum_{j=1}^{d-1} f_{d-j}\frac{\partial H_{d-j}}{\partial X_i}(\mathbf{x})$$

para $1 \leq i \leq k+1$. A partir de esta última identidad obtenemos la siguiente igualdad de matrices:

$$-\begin{pmatrix} \dfrac{\partial H_1}{\partial X_1}(\mathbf{x}) & \cdots & \dfrac{\partial H_{d-1}}{\partial X_1}(\mathbf{x}) \\ \vdots & & \vdots \\ \dfrac{\partial H_1}{\partial X_{k+1}}(\mathbf{x}) & \cdots & \dfrac{\partial H_{d-1}}{\partial X_{k+1}}(\mathbf{x}) \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_{d-1} \end{pmatrix} = \begin{pmatrix} \dfrac{\partial H_d}{\partial X_1}(\mathbf{x}) \\ \vdots \\ \dfrac{\partial H_d}{\partial X_{k+1}}(\mathbf{x}) \end{pmatrix}. \tag{6.11}$$

Por simetría, podemos suponer que $x_i = \lambda_i$ para $1 \leq i \leq d-1$. Más aún, podemos suponer que $\lambda_i \neq \lambda_j$ si $i \neq j$. Considerando las primeras $d-1$ ecuaciones de (6.11) obtenemos el siguiente sistema de $d-1$ ecuaciones y $d-1$ incógnitas $f_1, \ldots, f_{d-1}$

$$-B(\mathbf{x}) \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{d-1} \end{pmatrix} = \begin{pmatrix} \dfrac{\partial H_d}{\partial X_1}(\mathbf{x}) \\ \vdots \\ \dfrac{\partial H_d}{\partial X_{d-1}}(\mathbf{x}) \end{pmatrix}, \tag{6.12}$$

donde $B(\mathbf{x}) \in \mathbb{A}^{(d-1)\times(d-1)}$ es la matriz

$$B(\mathbf{x}) := \begin{pmatrix} \dfrac{\partial H_1}{\partial X_1}(\mathbf{x}) & \cdots & \dfrac{\partial H_{d-1}}{\partial X_1}(\mathbf{x}) \\ \vdots & & \vdots \\ \dfrac{\partial H_1}{\partial X_{d-1}}(\mathbf{x}) & \cdots & \dfrac{\partial H_{d-1}}{\partial X_{d-1}}(\mathbf{x}) \end{pmatrix}.$$

Teniendo en cuenta (6.10) vemos que la matriz $B(\mathbf{x})$ se puede factorizar de la siguiente manera:

$$B(\mathbf{x}) = A_{d-1}(\mathbf{x})^t \cdot \begin{pmatrix} H_0 & H_1(\mathbf{x}) \ldots & H_{d-2}(\mathbf{x}) \\ 0 & H_0 & \ldots & H_{d-3}(\mathbf{x}) \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & H_0 \end{pmatrix}, \tag{6.13}$$

donde $A_{d-1}(\mathbf{x}) := (x_j^{i-1})_{1\leq i,j\leq d-1}$ es una matriz de Vandermonde. Como consecuencia, la matriz $B(\mathbf{x})$ es no singular y

$$\det B(\mathbf{x}) = \prod_{1\leq i<j\leq d-1} (x_j - x_i). \tag{6.14}$$

Por lo tanto, $(f_1, \ldots, f_{d-1})$ es la única solución del sistema (6.12). Más aún, por la regla de Cramer obtenemos

$$f_j = \frac{\det B^{(j)}(\mathbf{x})}{\det B(\mathbf{x})},\ 1 \leq j \leq d-1,$$

donde $B^{(j)}(\mathbf{x}) \in \mathbb{A}^{(d-1)\times(d-1)}$ es la matriz que se obtiene al reemplazar la j-ésima columna de $B(\mathbf{x})$ por el vector $b(\mathbf{x}) := \big((\partial H_d/\partial X_1)(\mathbf{x}), \ldots, (\partial H_d/\partial X_{d-1})(\mathbf{x})\big)$.

Consideramos ahora las versiones "genéricas" $B, B^{(j)} \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]^{(d-1)\times(d-1)}$ de las matrices $B(\mathbf{x})$ y $B^{(j)}(\mathbf{x})$ para $1 \leq j \leq d-1$. Afirmamos que $\det B = \prod_{1\leq i<j\leq d-1}(X_j - X_i)$ divide a $\det B^{(j)}$ en $\mathbb{F}_q[X_1, \ldots, X_{k+1}]$. Para probar esto, sea $C \in \mathbb{F}_q[X_1, \ldots, X_{d-1}]^{(d-1)\times d}$ la siguiente matriz:

$$C := \begin{pmatrix} 1 & X_1 & \cdots & X_1^{d-2} & X_1^{d-1} \\ 1 & X_2 & \cdots & X_2^{d-2} & X_2^{d-1} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & X_{d-1} & \cdots & X_{d-1}^{d-2} & X_{d-1}^{d-1} \end{pmatrix}.$$

Si notamos como $A_{d-1} \in \mathbb{F}_q[X_1, \ldots, X_{d-1}]^{(d-1)\times(d-1)}$ a la versión genérica de la matriz de Vandermonde $A_{d-1}(\mathbf{x})$, entonces la matriz C se obtiene agregando el vector columna $(X_j^{d-1})_{1\leq j\leq d-1}$ a la matriz traspuesta A_{d-1}^t. Por otro lado, para $1 \leq j \leq d-1$ definimos una matriz $H^{(j)} \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]^{d\times(d-1)}$ de la siguiente manera:

$$H^{(j)} := \begin{pmatrix} H_0 & H_1 & \cdots & H_{j-2} & H_{d-1} & H_j & \cdots & H_{d-2} \\ 0 & H_0 & \cdots & H_{j-1} & H_{d-2} & H_{j-1} & \cdots & H_{d-3} \\ \vdots & 0 & \ddots & \vdots & \vdots & \vdots & & \vdots \\ & & \ddots & H_0 & H_{d-j+1} & H_2 & \cdots & H_{j-1} \\ \vdots & \vdots & & 0 & H_{d-j} & H_1 & & \vdots \\ & & & & H_{d-j-1} & H_0 & \ddots & \\ \vdots & \vdots & & \vdots & \vdots & 0 & \ddots & H_1 \\ & & & & H_1 & \vdots & \ddots & H_0 \\ 0 & 0 & \cdots & 0 & H_0 & 0 & \cdots & 0 \end{pmatrix}.$$

En otras palabras, $H^{(j)}$ se obtiene agregando una d-ésima fila nula al segundo factor del lado derecho de la igualdad (6.13) y reemplazando la j-ésima columna de la matriz que obtenemos por el vector columna $(H_{d-j}, 1 \leq j \leq d) \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]^{d\times 1}$. De esta manera, la matriz $B^{(j)}$ se puede factorizar como

$$B^{(j)} = C \cdot H^{(j)}. \tag{6.15}$$

En efecto, para $l \neq j$, las l-ésimas columnas de B y $B^{(j)}$ coinciden y de (6.13) se deduce fácilmente que la l-ésima columna de ambos lados de (6.15) son iguales. Por otro lado, a partir del Lema 6.3.4 se deduce fácilmente que la columna j-ésima de $B^{(j)}$ y $C \cdot H^{(j)}$ coinciden. En particular, el determinante de $B^{(j)}$ se puede obtener a partir de (6.15) utilizando la fórmula de Cauchy–Binet. Dado que cualquier menor maximal de C es un múltiplo de $\det B$ (ver, por ejemplo, [Ern00, Lemma 2.1] o [FS65, Exercise 281]), concluimos que $\det B$ divide a $\det B^{(j)}$ en $\mathbb{F}_q[X_1, \ldots, X_{k+1}]$.

A partir de esto se obtiene que, para cada $1 \leq j \leq d-1$, existe un polinomio homogéneo $P^{(j)} \in \mathbb{F}_q[X_1, \ldots, X_{d-1}]$ de grado $d-j$ o nulo tal que

$$f_{d-j} = P^{(j)}(\lambda_1, \ldots, \lambda_{d-1}) \tag{6.16}$$

para $1 \leq j \leq d-1$ y $(\lambda_1, \ldots, \lambda_{d-1}) \in \mathbb{A}^{d-1}$ con $\lambda_i \neq \lambda_j$ si $i \neq j$. Como (6.16) es válido en un abierto Zariski denso de $\mathbb{A}^{d-1}$, concluimos que (6.16) es válido para todo $(\lambda_1, \ldots, \lambda_{d-1}) \in \mathbb{A}^{d-1}$. Sustituyendo 0 por λ_i en (6.16) deducimos que $f_{d-j} = 0$ para $1 \leq j \leq d-1$. Por último, teniendo en cuenta que $(0, \ldots, 0)$ pertenece a $\mathcal{L}_{\mathcal{I}} \subset \Sigma_f \subset V_f$, deducimos que $f_0 = 0$. De esta forma, podemos dar la siguiente caracterización de los polinomios $f \in \mathbb{F}_q[T]$ para los cuales el lugar singular de V_f tiene dimensión $d-1$.

Teorema 6.3.5. *Teniendo en cuenta las notaciones dadas anteriormente, si el lugar singular Σ_f de V_f tiene dimensión $d-1$, entonces $f_0 = \cdots = f_{d-1} = 0$.*

En la Sección 6.5 vamos a probar que, si la característica p de $\mathbb{F}_q$ verifica que $p > d+1$, entonces el polinomio T^{k+d} no genera un deep hole del código de Reed-Solomon estándar. Por lo tanto, cuando la característica es suficientemente grande, podemos restringir nuestra atención a los casos en que la dimensión del lugar singular de V_f es a lo sumo $d-2$.

6.4. Una estimación de la cantidad de puntos q-racionales de V_f

Al igual que antes, consideramos enteros positivos d y k con $k > d$ y $q-1 > k+d$ y el código de Reed-Solomon estándar C de dimensión k sobre $\mathbb{F}_q$. Recordemos que nuestro objetivo es obtener condiciones sobre q, d y k que implican que C no tiene deep holes. Vimos en la Sección 6.1 que si existe un punto q-racional de V_f con coordenadas no nulas y distintas dos a dos, entonces la palabra generada por f no es un deep hole de C. Utilizando los resultados de la Sección 6.3 obtendremos una cota inferior para la cantidad de puntos q-racionales de V_f y una cota superior para la cantidad de puntos q-racionales de V_f con alguna coordenada nula o con al menos dos coordenadas iguales. Esto nos permitirá obtener una cota inferior para la cantidad de puntos q-racionales de V_f que son de nuestro interés y conseguir las condiciones sobre q, d y k para que C no posea deep holes.

Para esto, vamos a aplicar la siguiente estimación de Ghorpade y Lachaud para $\mathbb{F}_q$-hipersuperficies (ver [GL02a, Theorem 6.1]). Sea $V \subset \mathbb{P}^{m+1}$ una hipersuperficie de grado $d \geq 2$ y lugar singular de dimensión a lo sumo $s \geq 0$. Entonces, el número $|V(\mathbb{F}_q)|$ de puntos q-racionales de V verifica

$$\big||V(\mathbb{F}_q)| - p_m\big| \leq b_{m-s-1,d}\, q^{\frac{m+s+1}{2}} + C_{s,m}(V) q^{\frac{m+s}{2}}, \tag{6.17}$$

donde $b_{m-s-1,d}$ es el $(m-s-1)$-ésimo número primitivo de Betti de una hipersuperficie no singular en $\mathbb{P}^{m-s}$ de grado d, que se encuentra acotado superiormente por

$$b_{m-s-1,d} \leq \frac{d-1}{d}\big((d-1)^{m-s} - (-1)^{m-s}\big) \leq (d-1)^{m-s}, \tag{6.18}$$

y $C_{s,m}(V)$ es la suma

$$C_{s,m}(V) := \sum_{i=m}^{m+s} b_{i,\ell}(V) + \varepsilon_i,$$

donde $b_{i,\ell}(V)$ denota el i-ésimo ℓ-ádico número de Betti de V con ℓ un número primo diferente de $p := \mathrm{char}(\mathbb{F}_q)$, $\varepsilon_i := 1$ si i es par y $\varepsilon_i := 0$ si i es impar. En [GL02a, Proposition 5.1] se prueba que

$$C_{s,m}(V) \leq 18(d+3)^{m+2}. \tag{6.19}$$

Esta última cota es un caso particular de una cota para variedades proyectivas intersección completa singulares. A continuación damos una pequeña mejora de (6.19) para el caso de hipersuperficies.

Lema 6.4.1. *Si $V \subset \mathbb{P}^{m+1}$ es una hipersuperficie absolutamente irreducible de grado $d \geq 2$ y lugar singular de dimensión a lo sumo $s \geq 0$, se tiene entonces*

$$C_{s,m}(V) \leq 6(d+2)^{m+2}.$$

Demostración. Sea $E(n,d)$ una cota universal para la característica de Euler de una hipersuperficie afín $\mathcal{V} \subset \mathbb{A}^n$ definida por un polinomio $F_{\mathcal{V}} \in \overline{\mathbb{F}}_q[X_1,\ldots,X_n]$ de grado a lo sumo d y sea $A(n,d)$ el siguiente número:

$$A(n,d) := E(n,d) + 2 + 2\sum_{j=1}^{n-1} E(j,d).$$

Por la desigualdad de Katz [Kat01, Theorem 3], se tiene que

$$C_{s,m}(V) \leq s + 2 + \sum_{n=1}^{m+1} \big(1 + A(n+1, d+1)\big). \tag{6.20}$$

Como consecuencia de [AS88, Theorem 5.27] podemos elegir

$$E(n,d) := \frac{2}{d}\big((d+1)^{n+1} - 1\big).$$

A partir de esta elección y haciendo cálculos elementales, obtenemos

$$\begin{aligned} A(n,d) &= 2 + \frac{2}{d^2}\big((d+1)^{n+1}(d+2) - (2d^2 + d(2n+3) + 2)\big) \\ &\leq 2 + 2\frac{(d+2)}{d^2}\big((d+1)^{n+1} - 2d - 2n + 1\big). \end{aligned}$$

Combinando esta desigualdad con (6.20) se tiene

$$C_{s,m}(V) \leq m + 1 + \sum_{n=1}^{m+1}\left(3 + 2\frac{(d+3)}{(d+1)^2}\big((d+2)^{n+2} - 2d - 3\big)\right) \leq 6(d+2)^{m+2}. \quad \square$$

Combinando (6.17) con (6.18) y el Lema 6.4.1 obtenemos la siguiente estimación: si $V \subset \mathbb{P}^{m+1}$ es una $\mathbb{F}_q$-hipersuperficie absolutamente irreducible de grado $d \geq 2$ y lugar singular de dimensión a lo sumo $s \geq 0$, entonces el número de puntos q-racionales de V satisface la estimación

$$\big||V(\mathbb{F}_q)| - p_m\big| \leq (d-1)^{m-s}\, q^{\frac{m+s+1}{2}} + 6(d+2)^{m+2} q^{\frac{m+s}{2}}. \tag{6.21}$$

Combinando el Corolario 6.3.3 y [Kun85, Chapter I, Proposition 5.17] se tiene que la clausura proyectiva $\mathrm{pcl}(V_f) \subset \mathbb{P}^{k+1}$ de V_f es una $\mathbb{F}_q$-hipersuperficie absolutamente irreducible. Más aún, por el Corolario 6.3.1 y la Proposición 6.3.2 deducimos que la dimensión del lugar singular de $\mathrm{pcl}(V_f)$ es a lo sumo $d-1$. Por lo tanto, de (6.21), deducimos la siguiente estimación:

$$||\mathrm{pcl}(V_f)(\mathbb{F}_q)| - p_k| \leq (d-1)^{k-d+1}\, q^{\frac{k+d}{2}} + 6(d+2)^{k+2} q^{\frac{k+d-1}{2}}. \tag{6.22}$$

A partir de esta última estimación obtenemos la siguiente cota inferior para la cantidad de puntos q-racionales de V_f.

Proposición 6.4.2. *Sean d y k enteros positivos con $k > d \geq 2$ y $q-1 > k+d$. Entonces el número de puntos q-racionales de la hipersuperficie V_f satisface la siguiente desigualdad:*

$$|V_f(\mathbb{F}_q)| \geq q^k - 2(d-1)^{k-d+1} q^{\frac{k+d}{2}} - 7(d+2)^{k+2} q^{\frac{k+d-1}{2}}.$$

Demostración. Como estamos interesados en puntos q-racionales de V_f, necesitamos descartar los puntos de $\mathrm{pcl}(V_f)(\mathbb{F}_q)$ que pertenecen al hiperplano del infinito $\{X_0 = 0\}$. Como $\mathrm{pcl}(V_f)$ es la hipersuperficie definida por el polinomio $H_f^h = H_d + f_{d-1}H_{d-1}X_0 + \cdots + f_0 X_0^d \in \mathbb{F}_q[X_0, \ldots, X_{k+1}]$, tenemos que

$$\mathrm{pcl}(V_f)(\mathbb{F}_q) \cap \{X_0 = 0\} = \{\mathbf{x} \in \mathbb{P}^k(\mathbb{F}_q) : H_d(\mathbf{x}) = 0\}.$$

Por la Proposición 6.3.2, el lugar singular de la $\mathbb{F}_q$-hipersuperficie $V_f^\infty \subset \mathbb{P}^k$ definida por H_d tiene dimensión a lo sumo $d-2$. Luego, aplicando la estimación (6.21) obtenemos

$$||V_f^\infty(\mathbb{F}_q)| - p_{k-1}| \leq (d-1)^{k-d+1}\, q^{\frac{k+d-2}{2}} + 6(d+2)^{k+1}\, q^{\frac{k+d-3}{2}}. \tag{6.23}$$

Finalmente, combinando (6.22) y (6.23) se tiene la siguiente cota inferior para $|V_f(\mathbb{F}_q)|$:

$$\begin{aligned} |V_f(\mathbb{F}_q)| - q^k &= \big(|\mathrm{pcl}(V_f)(\mathbb{F}_q)| - p_k\big) - \big(|V_f^\infty(\mathbb{F}_q)| - p_{k-1}\big) \\ &\geq -(d-1)^{k-d+1} q^{\frac{k+d}{2}}(1+q^{-1}) - 6(d+2)^{k+2} q^{\frac{k+d-1}{2}}\big(1+(q(d+2))^{-1}\big). \end{aligned}$$

A partir de esta última desigualdad se obtiene fácilmente la afirmación de la proposición. □

A continuación obtenemos una cota superior para la cantidad de puntos q-racionales de V_f que no resultan útiles a los efectos de determinar la existencia de deep holes en el código de Reed-Solomon estándar, es decir, aquellos puntos de $V_f(\mathbb{F}_q)$ que poseen alguna coordenada nula o algún par de coordenadas iguales. Comenzamos estimando la cantidad de puntos que tienen alguna coordenada nula.

Proposición 6.4.3. *Con las hipótesis de la Proposición 6.4.2, el número N_1 de puntos q-racionales de V_f con alguna coordenada nula satisface la siguiente desigualdad:*

$$N_1 \leq (k+1)\left(q^{k-1} + 2(d-1)^{k-d} q^{\frac{k+d-1}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-2}{2}}\right).$$

Demostración. Sea $\mathbf{x} := (x_1, \ldots, x_{k+1})$ un punto de V_f con una coordenada nula. Sin pérdida generalidad podemos suponer que $x_{k+1} = 0$. Por lo tanto, $\mathbf{x}$ es un punto q-racional de la intersección $W_{k+1} := V_f \cap \{X_{k+1} = 0\}$. Observemos que W_{k+1} es la $\mathbb{F}_q$-hipersuperficie contenida en el espacio lineal $\{X_{k+1} = 0\}$ definida por el polinomio $G_f(\Pi_1^k, \ldots, \Pi_d^k)$, donde $\Pi_1^k, \ldots, \Pi_d^k$ son los primeros d polinomios simétricos elementales en $\mathbb{F}_q[X_1, \ldots, X_k]$. De acuerdo al Teorema 5.2.1, el lugar singular de W_{k+1} tiene dimensión a lo sumo $d-1$. Más aún, por la Proposición 6.3.2 el lugar singular de W_{k+1} en el hiperplano del infinito tiene dimensión a lo sumo $d-2$. Como consecuencia, argumentando como en la Proposición 6.4.2, obtenemos

$$\begin{aligned} |W_{k+1}(\mathbb{F}_q)| - q^{k-1} &= \big(|\mathrm{pcl}(W_{k+1})(\mathbb{F}_q)| - p_{k-1}\big) - \big(|W_{k+1}^{\infty}(\mathbb{F}_q)| - p_{k-2}\big) \\ &\leq (d-1)^{k-d} q^{\frac{k+d-1}{2}} + 6(d+2)^{k+1} q^{\frac{k+d-2}{2}} \\ &\quad + (d-1)^{k-d} q^{\frac{k+d-3}{2}} + 6(d+2)^{k} q^{\frac{k+d-4}{2}}, \end{aligned}$$

de donde

$$|W_{k+1}(\mathbb{F}_q)| \leq q^{k-1} + 2(d-1)^{k-d} q^{\frac{k+d-1}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-2}{2}}.$$

Finalmente, la demostración se sigue teniendo en cuenta las cotas superiores para la cantidad de puntos q-racionales de cada una de las variedades $W_i := V_f \cap \{X_i = 0\}$ con $1 \leq i \leq k+1$. □

Analizamos ahora el caso de los puntos q-racionales de V_f con dos coordenadas iguales.

Proposición 6.4.4. *Con las hipótesis de la Proposición 6.4.2, el número N_2 de puntos q-racionales de V_f con al menos dos coordenadas iguales satisface la siguiente desigualdad:*

$$N_2 \leq \frac{(k+1)k}{2}\Big(q^{k-1} + 2(d-1)^{k-d} q^{\frac{k+d-1}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-2}{2}}\Big).$$

Demostración. Sea $\mathbf{x} := (x_1, \ldots, x_{k+1}) \in V_f(\mathbb{F}_q)$ un punto con dos coordenadas iguales. Sin pérdida de generalidad, podemos suponer que $x_k = x_{k+1}$. Entonces $\mathbf{x}$ es un punto q-racional de la hipersuperficie $W_{k,k+1} \subset \{X_k = X_{k+1}\}$ definida por el polinomio $G_f(\Pi_1^*, \ldots, \Pi_d^*) \in \mathbb{F}_q[X_1, \ldots, X_k]$, donde $\Pi_i^* := \Pi_i(X_1, \ldots, X_k, X_k) \in \mathbb{F}_q[X_1, \ldots, X_k]$ es el polinomio que se obtiene sustituyendo X_k por X_{k+1} en el i-ésimo polinomio simétrico elemental de $\mathbb{F}_q[X_1, \ldots, X_{k+1}]$. Observemos que

$$\Pi_i^* = \Pi_i^{k-1} + 2X_k \cdot \Pi_{i-1}^{k-1} + X_k^2 \cdot \Pi_{i-2}^{k-1}, \tag{6.24}$$

donde Π_j^l denota el j-ésimo polinomio simétrico elemental de $\mathbb{F}_q[X_1, \ldots, X_l]$ para $1 \leq j \leq d$ y $1 \leq l \leq k+1$. Afirmamos que el lugar singular de $\mathrm{pcl}(W_{k,k+1})$ y el lugar singular de $W_{k,k+1}$ en el hiperplano del infinito tienen dimensión a lo sumo $d-1$ y $d-2$, respectivamente. Para probar esta afirmación, supongamos en primer lugar que la característica p de $\mathbb{F}_q$ es mayor a 2. Entonces, por la fórmula

(6.24) se puede demostrar que todos los menores maximales de la matriz Jacobiana $(\partial\Pi_i^*/\partial X_j)_{1\le i\le d,1\le j\le k}$ coinciden, salvo una constante no nula, con los correspondientes menores de la matriz Jacobiana $(\partial\Pi_i^k/\partial X_j)_{1\le i\le d,1\le j\le k}$. Así, argumentos similares a los hechos en las demostraciones del Teorema 5.2.1 y la Proposición 6.3.2 prueban nuestra afirmación.

Supongamos que $p = 2$. Teniendo en cuenta la fórmula (6.24), notamos que la primera derivada parcial de Π_j^* con respecto a X_k es igual a cero. Más aún, es fácil ver que el menor maximal no nulo de la matriz Jacobiana $(\partial\Pi_i^*/\partial X_j)_{1\le i\le d,1\le j\le k}$ que se obtiene al considerar las columnas $1 \le i_1 < i_2 < \cdots < i_d \le k-1$ es igual al correspondiente menor no nulo de $(\partial\Pi_i^{k-1}/\partial X_j)_{1\le i\le d,1\le j\le k}$. Esto prueba que cada menor maximal no nulo de $(\partial\Pi_i^*/\partial X_j)_{1\le i\le d,1\le j\le k}$ es un determinante de Vandermonde que depende de d y de las indeterminadas $X_1,\ldots,X_{k-1}$. En particular, al pedir que todos estos menores se anulen no imponemos ninguna condición en la variable X_k. Notemos por $\Sigma_{k,k+1}$ el lugar singular de $W_{k,k+1}$. Observemos que, con los mismos argumentos de la demostración del Teorema 5.2.1, se obtiene

$$\Sigma_{k,k+1} \subset \bigcup_{\mathcal{I}} \mathcal{L}_{\mathcal{I}}, \tag{6.25}$$

donde $\mathcal{I} := \{I_1,\ldots,I_d\}$ recorre todas las particiones de $\{1,\ldots,k+1\}$ en d subconjuntos no vacíos $I_j \subset \{1,\ldots,k+1\}$ tales que $I_j \subset \{1,\ldots,k-1\}$ para $1 \le j \le d-1$ e $I_d := \{k,k+1\}$, y $\mathcal{L}_{\mathcal{I}}$ es la variedad lineal

$$\mathcal{L}_{\mathcal{I}} := \operatorname{span}(\mathbf{v}^{(I_1)},\ldots,\mathbf{v}^{(I_d)})$$

generada por los vectores $\mathbf{v}^{(I_j)} := (v_1^{(I_j)},\ldots,v_{k+1}^{(I_j)})$ definidos por $v_m^{(I_j)} := 1$ para $m \in I_j$ y $v_m^{(I_j)} := 0$ para $m \notin I_j$ (ver la Observación 5.2.2). Luego, si $\Sigma_{k,k+1}$ tiene dimensión d, entonces contiene una variedad lineal $\mathcal{L}_{\mathcal{I}}$. Asumamos que $\Sigma_{k,k+1}$ tiene dimensión d y lleguemos a una contradicción. Siguiendo la demostración del Teorema 6.3.5 se tiene que f es el monomio T^{k+d} y que $H_f = H_d$. Fijemos $\mathcal{I} := \{I_1,\ldots,I_d\}$ y sea $\mathcal{L}_{\mathcal{I}}$ la correspondiente variedad lineal de dimensión d. Afirmamos que $\mathcal{L}_{\mathcal{I}}$ interseca $\Sigma_{k,k+1}$ propiamente. En efecto, consideremos la variedad lineal $\ell_\lambda := \{\mathbf{v}_\lambda := (0,\ldots,0,\lambda,\lambda) \in \mathbb{A}^{k+1} : \lambda \in \mathbb{A}^1\} \subset \mathcal{L}_{\mathcal{I}}$. Observemos que

$$\ell_\lambda \cap \Sigma_{k,k+1} = \{\mathbf{v}_\lambda \in \mathbb{A}^{k+1} : H_d(\mathbf{v}_\lambda) = 0, \nabla H_d(\mathbf{v}_\lambda) = \mathbf{0}\}.$$

Por la Proposición 6.2.2 y las igualdades $\Pi_j(\mathbf{v}_\lambda) = 0$ si $j \notin \{0,2\}$ y $\Pi_2(\mathbf{v}_\lambda) = \lambda^2$ se obtiene que, si d es par, entonces $H_d(\mathbf{v}_\lambda) = \pm\lambda^d$ y, si d es impar, $H_{d-1}(\mathbf{v}_\lambda) = \pm\lambda^{d-1}$. Más aún, por el Lema 6.3.4 se tiene que $(\partial H_d/\partial X_1)(\mathbf{v}_\lambda) = H_{d-1}(\mathbf{v}_\lambda) = \pm\lambda^{d-1}$ si d es impar. En ambos casos, las identidades $H_d(\mathbf{v}_\lambda) = (\partial H_d/\partial X_1)(\mathbf{v}_\lambda) = 0$ implican que $\lambda = 0$, lo que prueba que $\ell_\lambda \subset \mathcal{L}_{\mathcal{I}}$ interseca propiamente a $\Sigma_{k,k+1}$. Finalmente, teniendo en cuenta (6.25) y que cada $\mathcal{L}_{\mathcal{I}}$ interseca propiamente a $\Sigma_{k,k+1}$, deducimos que $\dim \Sigma_{k,k+1} \le d-1$, pues cada variedad $\mathcal{L}_{\mathcal{I}}$ es absolutamente irreducible y cada componente irreducible de $\Sigma_{k,k+1}$ es una subvariedad propia de alguna variedad $\mathcal{L}_{\mathcal{I}}$. Esto contradice el hecho de que $\dim \Sigma_{k,k+1} = d$, con lo cual obtenemos que $\dim \Sigma_{k,k+1} \le d-1$. Con los mismos argumentos de la Proposición 6.3.2 concluimos

que el lugar singular de $W_{k,k+1}$ en el hiperplano del infinito tiene dimensión a lo sumo $d-2$.

En conclusión, probamos que, independientemente de la característica p de $\mathbb{F}_q$, el lugar singular de $\mathrm{pcl}(W_{k,k+1})$ y el lugar singular de $W_{k,k+1}$ en el hiperplano del infinito tienen dimensión a lo sumo $d-1$ y $d-2$. Por lo tanto, siguiendo la demostración de la Proposición 6.4.3 obtenemos

$$|W_{k,k+1}(\mathbb{F}_q)| \leq q^{k-1} + 2(d-1)^{k-d} q^{\frac{k+d-1}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-2}{2}}.$$

La proposición se sigue fácilmente de esta desigualdad. □

Finalmente, combinando las Proposiciones 6.4.2, 6.4.3 y 6.4.4 obtenemos que el número N de puntos q-racionales de V_f con coordenadas no nulas y distintas satisface la siguiente desigualdad:

$$\begin{aligned} N \geq q^k - \frac{(k+1)(k+2)}{2} q^{k-1} - 2(d-1)^{k-d} q^{\frac{k+d}{2}} \left(d - 1 + \frac{(k+1)(k+2)}{2q^{\frac{1}{2}}} \right) \\ -7(d+2)^{k+1} q^{\frac{k+d-1}{2}} \left(d + 2 + \frac{(k+1)(k+2)}{2q^{\frac{1}{2}}} \right). \end{aligned} \tag{6.26}$$

6.5. Resultados sobre la existencia de deep holes

Recordemos que d y k son enteros positivos con $k > d$ y $q - 1 > k + d$, C es el código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$ y f es un polinomio arbitrario como en (6.1). Teniendo en cuenta los resultados de la sección anterior, se tiene que f no genera un deep hole de C si el lado derecho de (6.26) es un número positivo.

Supongamos que q, k y $d \geq 3$ satisfacen las condiciones:

$$q > (k+1)^2, \quad k > 3d. \tag{6.27}$$

Como $k \geq 10$, entonces $\frac{3}{4}(k+1)(k+2) \leq (k+1)^2 < q$. Por lo tanto, se tiene $q - \frac{1}{2}(k+1)(k+2) > q/3$, lo que implica

$$q^k - \frac{(k+1)(k+2)}{2} q^{k-1} = q^{k-1} \left(q - \frac{(k+1)(k+2)}{2} \right) > \frac{q^k}{3}.$$

Concluimos que el lado derecho de (6.26) es positivo si

$$\begin{aligned} \frac{q^k}{3} \quad \geq \quad & 2(d-1)^{k-d} q^{\frac{k+d}{2}} \left(d - 1 + \frac{(k+1)(k+2)}{2q^{\frac{1}{2}}} \right) \\ & + 7(d+2)^{k+1} q^{\frac{k+d-1}{2}} \left(d + 2 + \frac{(k+1)(k+2)}{2q^{\frac{1}{2}}} \right). \end{aligned} \tag{6.28}$$

Teniendo en cuenta que $k + 1 < q^{\frac{1}{2}}$, se tiene que (6.28) puede ser reemplazado por la siguiente condición:

$$\frac{q^k}{3} \geq 2(d-1)^{k-d} q^{\frac{k+d}{2}} \left(d - 1 + \tfrac{k+2}{2} \right) + 7(d+2)^{k+1} q^{\frac{k+d-1}{2}} \left(d + 2 + \tfrac{k+2}{2} \right).$$

Como $d \leq \frac{k-1}{3}$, tenemos que $d+2+\frac{k+2}{2} \leq k+1$, y por lo tanto el lado derecho de (6.26) es positivo si

$$\frac{q^k}{3} \geq 2(d-1)^{k-d}(k-2)q^{\frac{k+d}{2}} + 7(d+2)^{k+1}(k+1)q^{\frac{k+d-1}{2}},$$

o equivalentemente, si

$$q^k \geq 6(d-1)^{k-d}(k-2)q^{\frac{k+d}{2}} + 21(d+2)^{k+1}(k+1)q^{\frac{k+d-1}{2}}.$$

Más aún, esta condición se cumple si

$$\frac{q^k}{8} \geq 6(d-1)^{k-d}(k-2)q^{\frac{k+d}{2}}, \quad \frac{7q^k}{8} \geq 21(d+2)^{k+1}(k+1)q^{\frac{k+d-1}{2}},$$

estas condiciones podemos reescribirlas de la siguiente manera:

$$q^k \geq 48(d-1)^{k-d}(k-2)q^{\frac{k+d}{2}}, \quad q^k \geq 24(d+2)^{k+1}(k+1)q^{\frac{k+d-1}{2}}. \tag{6.29}$$

La primer desigualdad es equivalente a que

$$q \geq (48(k-2))^{\frac{2}{k-d}}(d-1)^2.$$

A partir de (6.27) podemos concluir que $3(k-d) \geq 2k+1$. Como la función $k \mapsto \big(48(k-2)\big)^{6/(2k+1)}$ es decreciente y $k \geq 10$, deducimos que una condición suficiente para que sea válida la desigualdad de arriba es

$$q > 6d^2. \tag{6.30}$$

A continuación consideramos la segunda desigualdad (6.29). Observemos que esta desigualdad puede ser expresada de la siguiente manera:

$$q > (24(k+1))^{\frac{2}{k-d+1}}\Big(\frac{d+2}{d}\Big)^{2+\frac{2d}{k-d+1}} d^{2+\frac{2d}{k-d+1}}. \tag{6.31}$$

A partir de (6.27) deducimos que $3(k-d+1) \geq 2k+4$. Teniendo en cuenta que la función $k \mapsto \big(24(k+1)\big)^{3/(k+2)}$ es decreciente, en particular para $k \geq 12$ (y por lo tanto, para $d \geq 4$), vemos que se cumple (6.31) si vale la siguiente condición:

$$q > 14\, d^{2+2d/(k-d)}. \tag{6.32}$$

Combinando (6.27), (6.30) y (6.32) concluimos que (6.27) y (6.32) proporcionan una condición suficiente para la no existencia de deep holes. Finalmente, a partir de (6.26) fácilmente se concluye que (6.27) y (6.32) proveen una condición suficiente para la inexistencia de deep holes en el caso $d = 3$. En resumen, tenemos el siguiente resultado.

Teorema 6.5.1. *Sean k y d enteros positivos con $k > d \geq 3$ y ϵ una constante positiva. Sea $\mathbf{w}_f$ la palabra generada por un polinomio $f \in \mathbb{F}_q[T]$ de grado $k+d < q-1$. Si se valen las condiciones*

$$q > \text{máx}\{(k+1)^2, 14\, d^{2+\epsilon}\}, \quad k \geq d\Big(\frac{2}{\epsilon}+1\Big),$$

entonces $\mathbf{w}_f$ no es un deep hole del código deReed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$.

Observamos que en [LW08a] se prueba que, para $d = 1$, $k > 2$ y $q > k + 3$, los polinomios de grado $k + 1$ no generan deep holes del código de Reed-Solomon estándar C. Por otro lado, siguiendo nuestro enfoque, se puede obtener un resultado similar al Teorema 6.5.1 para $d = 2$, es decir, para una constante $M_1 > 14$, si se cumplen las condiciones $q > \max\{(k+1)^2, M_1\, 2^{2+\epsilon}\}$ y $k \geq 2(2/\epsilon + 1)$, entonces los polinomios de grado $k + 2$ no generan deep holes del código C.

6.5.1. El caso $\mathbf{char}(\mathbb{F}_q) > d + 1$

A lo largo de toda esta sección suponemos que la característica p de $\mathbb{F}_q$ es mayor a $d + 1$. Si la dimensión del lugar singular de V_f es $d - 1$, el Teorema 6.3.5 asegura que el polinomio f de (6.1) es el monomio $f = T^{k+d}$. Nuestro primer objetivo es mostrar que T^{k+d} no genera un deep hole del código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$. Esto implica que, a los efectos de determinar la existencia de deep holes, podemos suponer que la dimensión del lugar singular de V_f es a lo sumo $d - 2$. Comenzamos probando el siguiente resultado.

Lema 6.5.2. *Sean k y d enteros positivos con $k > d$. Si el lugar singular de la hipersuperficie $V_d \subset \mathbb{A}^{k+1}$ asociada a T^{k+d} tiene dimensión $d - 1$, entonces $p|k + d$.*

Demostración. En la demostración del Teorema 6.3.5 vimos que si el lugar singular Σ_d de V_d tiene dimensión $d - 1$, entonces existe una variedad lineal de dimensión $d - 1$ contenida en Σ_d

$$\mathcal{L}_{\mathcal{I}} := \operatorname{span}(\mathbf{v}^{(I_1)}, \ldots, \mathbf{v}^{(I_{d-1})}),$$

donde $\{I_1, \ldots, I_{d-1}\}$ es una partición de $\{1, \ldots, k+1\}$, luego $|I_1|+\cdots+|I_{d-1}| = k+1$, $v_i^{I_j} \in \{0, 1\}$ para $1 \leq i \leq k + 1$ y $1 \leq j \leq d - 1$, y se tiene que $\mathbf{v}^{(I_1)} + \cdots + \mathbf{v}^{(I_{d-1})} = (1, \ldots, 1)$. Sean $\lambda := (\lambda_1, \ldots, \lambda_{d-1}) \in \mathbb{A}^{d-1}$ y $\mathbf{x} := \sum_{j=1}^{d-1} \lambda_j \mathbf{v}^{(I_j)}$ un punto arbitrario de $\mathcal{L}_{\mathcal{I}}$. Al igual que en la demostración del Teorema 6.3.5, suponemos que $x_i = \lambda_i$, $1 \leq i \leq d - 1$ y $\lambda_i \neq \lambda_j$, $1 \leq i < j \leq k + 1$. De acuerdo a (6.14) se tiene que la matriz $B(\mathbf{x})$ es no singular y, por lo tanto, $\mathbf{0} \in \mathbb{A}^d$ es la única solución del sistema lineal (6.12), es decir,

$$-B(\mathbf{x}) \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{d-1} \end{pmatrix} = \begin{pmatrix} \dfrac{\partial H_d}{\partial X_1}(\mathbf{x}) \\ \vdots \\ \dfrac{\partial H_d}{\partial X_{d-1}}(\mathbf{x}) \end{pmatrix}.$$

En particular, por la regla de Cramer, obtenemos

$$\det B^{(d-1)}(\mathbf{x}) = 0, \tag{6.33}$$

donde $B^{(d-1)}(\mathbf{x}) \in \mathbb{A}^{(d-1)\times(d-1)}$ es la matriz que se obtiene reemplazando la $(d-1)$-ésima columna de $B(\mathbf{x})$ por el vector $b(\mathbf{x}) := \big((\partial H_d/\partial X_j)(\mathbf{x}) : 1 \leq j \leq d - 1\big)$. Recordemos que la matriz $B^{(d-1)}(\mathbf{x})$ se puede factorizar como en (6.15), es decir,

$$B^{(d-1)}(\mathbf{x}) = C(\mathbf{x}) \cdot H^{(d-1)}(\mathbf{x}),$$

donde $C(\mathbf{x})$ se define como en (6.3.1) y $H^{(d-1)}(\mathbf{x}) \in \mathbb{A}^{d\times(d-1)}$ es la matriz

$$H^{(d-1)}(\mathbf{x}) := \begin{pmatrix} 1 & H_1(\mathbf{x}) & \cdots & H_{d-3}(\mathbf{x}) & H_{d-1}(\mathbf{x}) \\ 0 & 1 & \cdots & H_{d-4}(\mathbf{x}) & H_{d-2}(\mathbf{x}) \\ & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 1 & H_2(\mathbf{x}) \\ & & & 0 & H_1(\mathbf{x}) \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Vamos a obtener una expresión explícita de $\det B^{(d-1)}(\mathbf{x})$ aplicando la fórmula de Cauchy–Binet a la factorización de $B^{(d-1)}(\mathbf{x})$. Para esto, observemos que $H^{(d-1)}(\mathbf{x})$ tiene sólo dos menores no nulos de tamaño $(d-1)\times(d-1)$: el que corresponde a la submatriz formada por las primeras $d-1$ filas de $H^{(d-1)}(\mathbf{x})$, cuyo valor es igual a $H_1(\mathbf{x})$, y el determinado por las filas $\{1,\dots,d-2,d\}$ de $H^{(d-1)}(\mathbf{x})$, que es igual a 1. Luego, por la fórmula de Cauchy–Binet obtenemos que

$$\det B^{(d-1)}(\mathbf{x}) = H_1(\mathbf{x})\cdot\det B(\mathbf{x}) + \det\begin{pmatrix} 1 & x_1 & \cdots & x_1^{d-3} & x_1^{d-1} \\ 1 & x_2 & \cdots & x_2^{d-3} & x_2^{d-1} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{d-1} & \cdots & x_{d-1}^{d-3} & x_{d-1}^{d-1} \end{pmatrix}.$$

Combinando (6.33) con, por ejemplo, [Ern00, Lemma 2.1] o [FS65, Exercise 280], se deduce la siguiente identidad:

$$\begin{aligned} 0 &= H_1(\mathbf{x})\cdot\det B(\mathbf{x}) + (x_1+\cdots+x_{d-1})\det B(\mathbf{x}) \\ &= \det B(\mathbf{x})\cdot\big((|I_1|+1)\lambda_1+\cdots+(|I_{d-1}|+1)\lambda_{d-1}\big). \end{aligned}$$

De (6.14) deducimos que $B(\mathbf{x})$ es una matriz no singular. Luego, se tiene que

$$(|I_1|+1)\lambda_1+\cdots+(|I_{d-1}|+1)\lambda_{d-1} = 0 \tag{6.34}$$

para todo $\lambda \in \mathbb{A}^{d-1}$ con $\lambda_i \neq \lambda_j$ si $i \neq j$, y por lo tanto, para todo $\lambda \in \mathbb{A}^{d-1}$. Sustituyendo 1 por λ_i en (6.34), el lema queda demostrado, dado que $(|I_1|+1)+\cdots+(|I_{d-1}|+1) = k+d$. □

Observación 6.5.3. *Notemos que la igualdad (6.34) establece una fuerte restricción sobre las particiones $\mathcal{I}$ de las variedades lineales $\mathcal{L}_\mathcal{I}$ contenidas en el lugar singular Σ_f de una hipersuperficie V_f con $\dim\Sigma_f = d-1$. En particular, fijando $i \in \{1,\dots,d-1\}$ y sustituyendo 1 por λ_i y 0 por λ_j con $j \neq i$, (6.34) implica que $|I_i| \equiv -1 \mod p$.*

A continuación probamos que si el lugar singular de la hipersuperficies V_f tiene dimensión $d-1$, entonces la palabra generada por f no es un deep hole del código de Reed-Solomon estándar C.

Proposición 6.5.4. *Sean k y d enteros positivos con $k > d$, $p > d+1$ y $q > k+d$. Supongamos que $p|k+d$. Sea $\mathbf{w}_d \in \mathbb{F}_q^{q-1}$ la palabra generada por el polinomio $T^{k+d} \in \mathbb{F}_q[T]$. Entonces $\mathbf{w}_d$ no es un deep hole del código de Reed-Solomon estándar C de dimension k sobre $\mathbb{F}_q$.*

Demostración. Sea $q := p^s$. En primer lugar, notemos que la desigualdad $q > k+d \geq p$ implica $s > 1$. Recordemos que la traza $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$, definida por $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) := \sum_{i=0}^{s-1} \alpha^{p^i}$, es un morfismo $\mathbb{F}_p$-lineal suryectivo. Esto, en particular, implica que existen p^{s-1} elementos en $\mathbb{F}_q$ cuya traza es igual a cero. Sea $k+d = pl$. De la condición $q > k+d$ se deduce que $p^{s-1} > l$ y, por lo tanto, existen l elementos distintos $b_1 \ldots, b_l \in \mathbb{F}_q^*$ con $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(b_i) = 0$. Por lo tanto, de [CH04, Theorem 3] concluimos que el polinomio de Artin–Schreier $g_{b_i} := T^p - T - b_i \in \mathbb{F}_q[T]$ tiene p raíces distintas en $\mathbb{F}_q^*$ para $1 \leq i \leq l$. Más aún, como $b_i \neq b_j$ si $i \neq j$, los polinomios g_{b_i} y g_{b_j} no tienen raíces en común. Luego, el polinomio

$$g := \prod_{i=1}^{l} g_{b_i} = \prod_{i=1}^{l} (T^p - T - b_i) \tag{6.35}$$

tiene pl raíces distintas en $\mathbb{F}_q^*$. Por otro lado,

$$g = T^{k+d} - lT^{p(l-1)+1} + \mathcal{O}(T^{p(l-1)}) = T^{k+d} + h(T),$$

donde $h := lT^{p(l-1)+1} + \mathcal{O}(T^{p(l-1)})$ tiene grado a lo sumo $p(l-1)+1$. Sea $\mathbf{w}_h \in \mathbb{F}_q^{q-1}$ la palabra generada por el polinomio h. Como

$$p(l-1)+1 = k+d-p+1 \leq k+d-(d+2)+1 = k-1,$$

$\mathbf{w}_h$ es una palabra del código. Como el polinomio g definido en (6.35) tiene $pl > k$ raíces distintas en $\mathbb{F}_q^*$, se tiene que $\mathsf{d}(\mathbf{w}_d, \mathbf{w}_h) < q-1-k$, donde d denota la distancia de Hamming de $\mathbb{F}_q^{q-1}$. Concluimos entonces que $\mathbf{w}_d$ no es un deep hole del código C. □

Resumiendo, si $\mathbf{w}_f$ es una palabra generada por un polinomio $f \in \mathbb{F}_q[T]$ tal que el lugar singular de la hipersuperficie asociada V_f tiene dimensión $d-1$, entonces el Teorema 6.3.5 muestra que $f = T^{k+d}$. Asimismo, del Lema 6.5.2 y la Proposición 6.5.4 deducimos que $\mathbf{w}_f$ no genera un deep hole del código de Reed-Solomon estándar C.

Para finalizar el análisis de la existencia de deep holes del código de Reed-Solomon C en el caso en que $p > d+1$, nos resta estudiar el conjunto de palabras generadas por polinomios $f \in \mathbb{F}_q[T]$ para las cuales el lugar singular de la correspondiente hipersuperficie V_f tiene dimensión a lo sumo $d-2$.

Fijamos q, k y $d \geq 3$ con $q-1 > k+d$, $k > d$ y $p > d+1$. Supongamos que el polinomio $f \in \mathbb{F}_q[T]$ verifica que el lugar singular de la correspondiente hipersuperficie V_f tiene dimensión a lo sumo $d-2$. Con los argumentos de las demostraciones de la Proposiciones 6.4.2, 6.4.3 y 6.4.4 obtenemos las siguientes cotas:

$$|V_f(\mathbb{F}_q)| \geq q^k - 2(d-1)^{k-d+2} q^{\frac{k+d-1}{2}} - 7(d+2)^{k+2} q^{\frac{k+d-2}{2}},$$

$$N' \leq \frac{(k+1)(k+2)}{2}\left(q^{k-1} + 2(d-1)^{k-d+1} q^{\frac{k+d-2}{2}} + 7(d+2)^{k+1} q^{\frac{k+d-3}{2}}\right),$$

donde N' denota el número de puntos q-racionales de V_f que tienen alguna coordenada nula o al menos dos coordenadas iguales. Por lo tanto, el número de puntos q-racionales N de V_f con coordenadas no nulas y distintas dos a dos satisface la siguiente desigualdad:

$$\begin{aligned} N \geq q^k - \frac{(k+1)(k+2)}{2} q^{k-1} - 2(d-1)^{k-d+1} q^{\frac{k+d-1}{2}} \left(d - 1 + \frac{(k+1)(k+2)}{2q^{\frac{1}{2}}} \right) \\ -7(d+2)^{k+1} q^{\frac{k+d-2}{2}} \left(d + 2 + \frac{(k+1)(k+2)}{2q^{\frac{1}{2}}} \right). \end{aligned} \tag{6.36}$$

Supongamos que q, k y $d \geq 4$ satisfacen las siguientes condiciones:

$$q > (k+1)^2, \quad k > 3(d-1).$$

Entonces, el lado derecho de (6.36) es positivo si

$$q^k \geq \text{máx}\left\{ 48(d-1)^{k-d+1}(k-1) q^{\frac{k+d-1}{2}},\ 24(d+2)^{k+1}(k+2) q^{\frac{k+d-2}{2}} \right\}. \tag{6.37}$$

Argumentando de la misma manera que en la demostración del Teorema 6.5.1 concluimos que se satisface (6.37) si cumple la condición

$$q > 14\, d^{2+(2d-2)/(k-d+2)}. \tag{6.38}$$

Por otro lado, a partir de (6.36) deducimos que (6.38) es una condición suficiente para la no existencia de deep holes en el caso $d = 3$. En resumen, obtenemos el siguiente resultado:

Teorema 6.5.5. *Sean k y d enteros positivos con $k > d \geq 3$ y ϵ una constante positiva. Sea $\mathbf{w}_f$ la palabra generada por un polinomio $f \in \mathbb{F}_q[T]$ de grado $k + d < q - 1$. Si $\text{char}(\mathbb{F}_q) > d + 1$ y*

$$q > \text{máx}\{(k+1)^2, 14\, d^{2+\epsilon}\}, \quad k \geq (d-1)\left(\frac{2}{\epsilon} + 1\right),$$

entonces $\mathbf{w}_f$ no es un deep hole del código de Reed-Solomon estándar de dimensión k sobre $\mathbb{F}_q$.

Capítulo 7

Una aplicación a la Combinatoria

El objetivo de este capítulo es el de obtener una estimación del comportamiento promedio del "conjunto de valores" de familias de polinomios univariados definidos sobre $\mathbb{F}_q$ con coeficientes prescriptos. Se trata de un problema clásico de combinatoria que tiene aplicaciones a la teoría de códigos, a problemas de interpolación y al análisis de algoritmos de búsqueda de soluciones en $\mathbb{F}_q$ de sistemas de ecuaciones polinomiales, entre otras.

De manera similar a lo hecho en el capítulo anterior, traduciremos el problema original al de determinar la cantidad de puntos q-racionales con coordenadas distintas de intersecciones completas definidas por polinomios simétricos. De esta forma, podremos combinar nuestros resultados para este tipo de variedades con las estimaciones para intersecciones completas regulares en codimensión 2 del Capítulo 4.

7.1. Conjunto de valores de polinomios sobre cuerpos finitos

A continuación haremos una breve revisión de los resultados básicos relacionados con el estudio del conjunto de valores de polinomios univariados sobre un cuerpo finito. Para una exposición más detallada ver, por ejemplo, [LN83].

Para un polinomio $f \in \mathbb{F}_q[T]$ definimos el conjunto de valores de f (*value set*) en $\mathbb{F}_q$ como el conjunto imagen de la función polinomial de $\mathbb{F}_q$ en $\mathbb{F}_q$ que define f. Denotamos como $\mathcal{V}(f)$ al cardinal de dicho conjunto, es decir,

$$\mathcal{V}(f) := |\{f(c) \,|\, c \in \mathbb{F}_q\}|.$$

Para todo $f \in \mathbb{F}_q[T]$ se verifica trivialmente que $\mathcal{V}(f) \leq q$. Cuando vale la igualdad, el polinomio correspondiente se denomina un polinomio de permutación. Por otro lado, si f tiene grado d, entonces $\mathcal{V}(f) \geq \lceil q/d \rceil$. Los polinomios para los cuales vale la igualdad se llaman polinomios de conjunto de valores mínimo. El problema de calcular $\mathcal{V}(f)$ fue extensamente estudiado. Solo se conocen fórmulas exactas de $\mathcal{V}(f)$ para polinomios especiales; por ejemplo, es sencillo dar fórmulas para polinomios de grado 1 y 2 y se conocen fórmulas para los polinomios de grado 3, para el polinomio

$f := T^d$ y para los polinomios de Dickson, entre otros. Para polinomios generales sólo se tienen fórmulas asintóticas del número $\mathcal{V}(f)$. Los primeros en dar una fórmula de este tipo fueron Birch y Swinnerton–Dyer, quienes obtuvieron el siguiente resultado [BSD59]: si f es un polinomio de grado $d \geq 1$, entonces

$$\mathcal{V}(f) = \mu_d\, q + \mathcal{O}(q^{1/2}),$$

donde $\mu_d := \sum_{r=1}^{d} (-1)^{r-1}/r!$ y la constante que aparece en la notación $\mathcal{O}$ depende sólo de d. Posteriormente, S. Uchiyama [Uch54] prueba que si $\frac{f(x)-f(y)}{x-y}$ es absolutamente irreducible y $d \geq 4$, entonces se verifica

$$\mathcal{V}(f) = \mu_d\, q + \mathcal{O}(1).$$

En cuanto al valor promedio $\mathcal{V}(d,0)$ de $\mathcal{V}(f)$ cuando f recorre todos los polinomios mónicos en $\mathbb{F}_q[T]$ de grado d con $f(0) = 0$, se tiene el siguiente resultado de Cohen [Coh73, §2], que mejora el original de Uchiyama [Uch55a]:

$$\mathcal{V}(d,0) = \sum_{r=1}^{d} (-1)^{r-1} \binom{q}{r} q^{1-r} = \mu_d\, q + \mathcal{O}(1).$$

Sin embargo, si algunos coeficientes de f están fijos, los resultados que se conocen sobre el valor promedio de $\mathcal{V}(f)$ son menos precisos. En efecto, Uchiyama [Uch55b] y Cohen [Coh72] obtienen el siguiente resultado. Sea s un entero con $1 \leq s \leq d-2$ y $\boldsymbol{a} := (a_{d-1}, \ldots, a_{d-s}) \in \mathbb{F}_q^s$. Para cada $\boldsymbol{b} := (b_{d-s-1}, \ldots, b_1)$, sea

$$f_{\boldsymbol{b}} := f_{\boldsymbol{b}}^{\boldsymbol{a}} := T^d + \sum_{i=1}^{s} a_{d-i} T^{d-i} + \sum_{i=s+1}^{d-1} b_{d-i} T^{d-i}.$$

Si $p := \mathrm{char}(\mathbb{F}_q) > d$, entonces

$$\mathcal{V}(d,s,\boldsymbol{a}) := \frac{1}{q^{d-s-1}} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}}) = \mu_d\, q + \mathcal{O}(q^{1/2}), \tag{7.1}$$

donde la constante que aparece en la notación $\mathcal{O}$ depende sólo de d y s. Cabe mencionar que ni Cohen ni Uchiyama dan una expresión explícita del término de error en (7.1).

En esta tesis mejoramos el resultado (7.1). En efecto, probamos que $\mathcal{V}(d,s,\boldsymbol{a}) = \mu_d\, q + \mathcal{O}(1)$, sin imponer condiciones sobre la característica p. Además, damos una expresión explícita del término de error y probamos que este posee un "buen comportamiento", en el sentido de que tiende a cero cuando d tiende a infinito. Más precisamente, obtenemos la siguiente expresión:

$$\mathcal{V}(d,s,\boldsymbol{a}) = \mu_d\, q + \frac{1}{2e} + \mathcal{O}(\rho^{-d}) + \mathcal{O}(q^{-1})$$

para $\frac{1}{2} < \rho < 1$.

7.2. $\mathcal{V}(d,s,a)$ en términos de ciertos conjuntos de polinomios interpolantes

En esta sección vamos a mostrar cómo se puede relacionar el problema de estimar el número $\mathcal{V}(d,s,\boldsymbol{a})$ con un problema de interpolación. Fijamos un entero s con $1 \leq s \leq d-2$, una s-upla $\boldsymbol{a} := (a_{d-1}, \ldots, a_{d-s}) \in \mathbb{F}_q^s$ y consideramos el polinomio

$$f_{\boldsymbol{a}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s}. \tag{7.2}$$

Para cada $\boldsymbol{b} := (b_{d-s-1}, \ldots, b_1) \in \mathbb{F}_q^{d-s-1}$, notamos como $f_{\boldsymbol{b}} := f_{\boldsymbol{b}}^{\boldsymbol{a}} \in \mathbb{F}_q[T]$ al polinomio

$$f_{\boldsymbol{b}} := f_{\boldsymbol{a}} + b_{d-s-1}T^{d-s-1} + \cdots + b_1 T.$$

Dado $\boldsymbol{b} \in \mathbb{F}_q^{d-s-1}$, el conjunto de valores $\mathcal{V}(f_{\boldsymbol{b}})$ de $f_{\boldsymbol{b}}$ es igual a la cantidad de elementos $b_0 \in \mathbb{F}_q$ para los cuales el polinomio $f_{\boldsymbol{b}}+b_0$ tiene al menos una raíz en $\mathbb{F}_q$. Sea $\mathbb{F}_q[T]_d$ el conjunto de polinomios de $\mathbb{F}_q[T]$ de grado a lo sumo d y $\mathcal{N} : \mathbb{F}_q[T]_d \to \mathbb{Z}_{\geq 0}$ la función que a cada polinomio en $\mathbb{F}_q[T]_d$ le asigna la cantidad de raíces que éste posee en $\mathbb{F}_q$. Por último, consideramos la función característica $\mathbf{1}_{\{\mathcal{N}>0\}} : \mathbb{F}_q[T]_d \to \{0,1\}$ del conjunto de elementos de $\mathbb{F}_q[T]_d$ que tienen al menos una raíz en $\mathbb{F}_q$. De acuerdo a las notaciones y observaciones previas, deducimos la siguiente igualdad:

$$\begin{aligned}\sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}}) &= \sum_{b_0\in\mathbb{F}_q} \sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \mathbf{1}_{\{\mathcal{N}>0\}}(f_{\boldsymbol{b}} + b_0) \\ &= \big|\{g \in \mathbb{F}_q[T]_{d-s-1} : \mathcal{N}(f_{\boldsymbol{a}} + g) > 0\}\big|.\end{aligned}$$

Dado un subconjunto $\mathcal{X} \subseteq \mathbb{F}_q$, definimos $\mathcal{S}_{\mathcal{X}}^{\boldsymbol{a}}$ como el conjunto de polinomios de $\mathbb{F}_q[T]_{d-s-1}$ que interpolan al polinomio $-f_{\boldsymbol{a}}$ en todos los puntos de $\mathcal{X}$, es decir,

$$\mathcal{S}_{\mathcal{X}}^{\boldsymbol{a}} := \{g \in \mathbb{F}_q[T]_{d-s-1} : (f_{\boldsymbol{a}} + g)(x) = 0 \text{ para todo } x \in \mathcal{X}\}.$$

Finalmente, dado $r \in \mathbb{N}$ notamos como $\mathcal{X}_r$ a un subconjunto de $\mathbb{F}_q$ de r elementos.

Teorema 7.2.1. *Sean $s, d \in \mathbb{N}$ con $d < q$ y $1 \leq s \leq d-2$. Se verifica la siguiente igualdad:*

$$\mathcal{V}(d,s,\boldsymbol{a}) = \sum_{r=1}^{d-s}(-1)^{r-1}\binom{q}{r}q^{1-r} + \frac{1}{q^{d-s-1}}\sum_{r=d-s+1}^{d}(-1)^{r-1}\chi_r^{\boldsymbol{a}},$$

donde $\mathcal{V}(d,s,\boldsymbol{a})$ se define como en (7.1) y $\chi_r^{\boldsymbol{a}}$ es la cantidad de subconjuntos de r elementos $\mathcal{X}_r$ de $\mathbb{F}_q$ tales que existe un polinomio $g \in \mathbb{F}_q[T]_{d-s-1}$ para el cual se verifica $(f_{\boldsymbol{a}} + g)|_{\mathcal{X}_r} \equiv 0$.

Demostración. Dado un subconjunto $\mathcal{X}_r := \{x_1, \ldots, x_r\} \subset \mathbb{F}_q$, consideramos el correspondiente conjunto $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}} \subset \mathbb{F}_q[T]_{d-s-1}$ definido anteriormente. Es fácil ver que $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}} = \bigcap_{i=1}^{r} \mathcal{S}_{\{x_i\}}^{\boldsymbol{a}}$ y

$$\{g \in \mathbb{F}_q[T]_{d-s-1} : \mathcal{N}(f_{\boldsymbol{a}} + g) > 0\} = \bigcup_{x\in\mathbb{F}_q} \mathcal{S}_{\{x\}}^{\boldsymbol{a}}.$$

Luego, por el principio de inclusión-exclusión, obtenemos

$$\mathcal{V}(d,s,\boldsymbol{a}) = \frac{1}{q^{d-s-1}}\left|\bigcup_{x\in\mathbb{F}_q}\mathcal{S}^{\boldsymbol{a}}_{\{x\}}\right| = \frac{1}{q^{d-s-1}}\sum_{r=1}^{q}(-1)^{r-1}\sum_{\mathcal{X}_r\subseteq\mathbb{F}_q}\left|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}\right|. \tag{7.3}$$

A continuación calculamos $|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}|$ para un cierto conjunto $\mathcal{X}_r = \{x_1,\ldots,x_r\}\subset\mathbb{F}_q$. Notar que si $g := b_{d-s-1}T^{d-s-1}+\cdots+b_1T+b_0$ es un elemento de $\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}$, entonces se tienen las igualdades $f_{\boldsymbol{a}}(x_i)+g(x_i)=0$ para $1\le i\le r$. Estas identidades se pueden expresar en forma matricial de la siguiente manera:

$$\mathcal{M}(\mathcal{X}_r)\cdot\widehat{\boldsymbol{b}} + f_{\boldsymbol{a}}(\mathcal{X}_r) = 0,$$

donde $\mathcal{M}(\mathcal{X}_r) := (m_{i,j})\in\mathbb{F}_q^{r\times(d-s)}$ es la matriz de Vandermonde definida por $m_{i,j} := x_i^{d-s-j}$ para $1\le i\le r$ y $1\le j\le d-s$, $\widehat{\boldsymbol{b}} := (b_{d-s-1},\ldots,b_0)\in\mathbb{F}_q^{d-s}$ y $f_{\boldsymbol{a}}(\mathcal{X}_r) := (f_{\boldsymbol{a}}(x_1),\ldots,f_{\boldsymbol{a}}(x_r))\in\mathbb{F}_q^r$. Notar que, como $x_i\neq x_j$ si $i\neq j$, se sigue que

$$\operatorname{rg}(\mathcal{M}(\mathcal{X}_r)) = \min\{r, d-s\}. \tag{7.4}$$

Por lo tanto, $\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}$ es una $\mathbb{F}_q$-variedad lineal en $\mathbb{F}_q^{d-s}$. Además, o bien $\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}=\emptyset$, o bien

$$\operatorname{rg}(\mathcal{M}(\mathcal{X}_r)) + \dim\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r} = d-s. \tag{7.5}$$

Supongamos $r\le d-s$. Entonces (7.4) implica que $\operatorname{rg}(\mathcal{M}(\mathcal{X}_r)) = r$ y, por lo tanto, $\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}$ es no vacío. Asimismo, de (7.5) deducimos que $\dim\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r} = d-s-r$ y

$$|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}| = q^{d-s-r}. \tag{7.6}$$

Consideremos ahora $r\ge d-s+1$. Si $\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}\neq\emptyset$, entonces (7.5) implica que $\dim\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}=0$ y, por lo tanto, $|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}|=1$. Por otro lado, si $\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}=\emptyset$, entonces $|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}|=0$. En el caso $r>d$ se tiene que, si $g\in\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}$, entonces $g\in\mathbb{F}_q[T]_{d-s-1}$ y $f_{\boldsymbol{a}}(x_i)+g(x_i)=0$ para $1\le i\le r$. En consecuencia, el polinomio no nulo $f_{\boldsymbol{a}}+g$ tiene grado d y r raíces diferentes, lo que contradice el hecho de que $r>d$. Concluimos entonces que $\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}$ es vacío en este caso y, por lo tanto,

$$|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}| = 0. \tag{7.7}$$

En conclusión, si $d-s+1\le r\le d$, entonces $|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}|=0$ o $|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}|=1$.

Finalmente, combinando (7.3), (7.6) y (7.7) obtenemos

$$q^{d-s-1}\mathcal{V}(d,s,\boldsymbol{a}) = \sum_{r=1}^{d-s}(-1)^{r-1}\binom{q}{r}q^{d-s-r} + \sum_{r=d-s+1}^{d}(-1)^{r-1}\sum_{\mathcal{X}_r\subset\mathbb{F}_q}|\mathcal{S}^{\boldsymbol{a}}_{\mathcal{X}_r}|,$$

de donde se deduce el teorema. □

7.2.1. Un enfoque algebraico para estimar $\chi_r^{\boldsymbol{a}}$

De acuerdo al Teorema 7.2.1, para determinar el comportamiento de $\mathcal{V}(d,s,\boldsymbol{a})$ necesitamos estimar el número $\chi_r^{\boldsymbol{a}}$ con $d-s+1 \leq r \leq d$. Para esto, seguimos un enfoque similar al que desarrollamos en la Sección 6.2, es decir, vamos a traducir el problema de estudiar el comportamiento de $\chi_r^{\boldsymbol{a}}$ en el de estimar la cantidad de puntos q-racionales con coordenadas distintas dos a dos de una cierta variedad algebraica. De manera similar al problema de la existencia de deep holes, vamos a probar que dicha variedad algebraica está definida por polinomios invariantes bajo la acción del grupo simétrico de permutaciones de sus coordenadas.

Fijamos un conjunto $\mathcal{X}_r := \{x_1,\ldots,x_r\} \subset \mathbb{F}_q$ de r elementos y un polinomio $g \in \mathbb{F}_q[T]_{d-s-1}$. Entonces g pertenece a $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ si y sólo si $(T-x_1)\cdots(T-x_r)$ divide a $f_{\boldsymbol{a}}+g$ en $\mathbb{F}_q[T]$. Como $\deg g \leq d-s-1 < r$, deducimos que $-g$ es el resto de la división de $f_{\boldsymbol{a}}$ por $(T-x_1)\cdots(T-x_r)$. En otras palabras, el conjunto $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ es no vacío si y sólo si el resto de la división de $f_{\boldsymbol{a}}$ por $(T-x_1)\cdots(T-x_r)$ tiene grado a lo sumo $d-s-1$.

Sean $X_1,\ldots,X_r$ indeterminadas sobre $\overline{\mathbb{F}}_q$, sea $\boldsymbol{X} := (X_1,\ldots,X_r)$ y sea $Q \in \mathbb{F}_q[\boldsymbol{X}][T]$ el polinomio

$$Q = (T-X_1)\cdots(T-X_r).$$

Existe un polinomio $R_{\boldsymbol{a}} \in \mathbb{F}_q[\boldsymbol{X}][T]$ con $\deg R_{\boldsymbol{a}} \leq r-1$ tal que se verifica la siguiente relación:

$$f_{\boldsymbol{a}} \equiv R_{\boldsymbol{a}} \mod Q.$$

Escribimos $R_{\boldsymbol{a}} = R_{r-1}^{\boldsymbol{a}}(\boldsymbol{X})T^{r-1} + \cdots + R_0^{\boldsymbol{a}}(\boldsymbol{X})$. Entonces $R_{\boldsymbol{a}}(x_1,\ldots,x_r,T) \in \mathbb{F}_q[T]$ es el resto de la división de $f_{\boldsymbol{a}}$ por $(T-x_1)\cdots(T-x_r)$. Por lo tanto, el conjunto $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ es no vacío si y sólo si se verifican las siguientes igualdades:

$$R_j^{\boldsymbol{a}}(x_1,\ldots,x_r) = 0 \quad (d-s \leq j \leq r-1). \tag{7.8}$$

Recíprocamente, supongamos que existe $\boldsymbol{x} := (x_1,\ldots,x_r) \in \mathbb{F}_q^r$ con coordenadas distintas dos a dos tal que se verifica (7.8). Consideramos el conjunto $\mathcal{X}_r = \{x_1,\ldots,x_r\}$. Entonces el resto de la división de $f_{\boldsymbol{a}}$ por $Q(\boldsymbol{x},T) = (T-x_1)\cdots(T-x_r)$ es un polinomio $r_{\boldsymbol{a}} := R_{\boldsymbol{a}}(\boldsymbol{x},T)$ de grado a lo sumo $d-s-1$. Esto implica que $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ es no vacío. Como conclusión de estos argumentos, obtenemos el siguiente resultado.

Lema 7.2.2. *Sean $s,d \in \mathbb{N}$ con $1 \leq s \leq d-2$. Consideramos los polinomios $R_j^{\boldsymbol{a}}$, $d-s \leq j \leq r-1$, definidos en (7.8) y un conjunto $\mathcal{X}_r = \{x_1,\ldots,x_r\} \subset \mathbb{F}_q$ de r elementos. Entonces $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ es no vacío si y sólo si se verifica (7.8).*

Por lo tanto, el número $\chi_r^{\boldsymbol{a}}$ de conjuntos $\mathcal{X}_r \subset \mathbb{F}_q$ de r elementos tales que $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ es no vacío coincide con la cantidad de puntos $\boldsymbol{x} := (x_1,\ldots,x_r) \in \mathbb{F}_q^r$ con coordenadas distintas dos a dos que satisfacen (7.8), salvo permutaciones de las coordenadas. Más precisamente, $\chi_r^{\boldsymbol{a}}\, r!$ coincide con la cantidad de soluciones $\boldsymbol{x} \in \mathbb{F}_q^r$ del siguiente sistema de igualdades y desigualdades:

$$R_j^{\boldsymbol{a}}(X_1,\ldots,X_r) = 0 \quad (d-s \leq j \leq r-1), \quad \prod_{1\leq i<j\leq r}(X_i-X_j) \neq 0.$$

7.2.2. R_a en términos de los polinomios simétricos elementales

Sea r con $d-s+1 \leq r \leq d$. Supongamos que $2(s+1) \leq d$ y consideremos los polinomios simétricos elementales $\Pi_1, \ldots, \Pi_s$ de $\mathbb{F}_q[X_1, \ldots, X_r]$. El objetivo de esta sección es mostrar como los polinomios $R_j^{\boldsymbol{a}}$ se pueden expresar en términos de $\Pi_1, \ldots, \Pi_s$. De forma similar al Lema 6.2.1, vamos a obtener una fórmula recursiva para el resto de dividir T^j por $Q := (T-X_1)\cdots(T-X_r)$ para cada $r \leq j \leq d$.

Lema 7.2.3. *Para $r \leq j \leq d$, se verifican las siguientes congruencias:*

$$T^j \equiv H_{r-1,j}T^{r-1} + H_{r-2,j}T^{r-2} + \cdots + H_{0,j} \mod Q, \tag{7.9}$$

donde cada $H_{i,j}$ es igual a cero o es un polinomio homogéneo en $\mathbb{F}_q[X_1, \ldots, X_r]$ de grado $j-i$. Más aún, para $j-i \leq r$, el polinomio $H_{i,j} \in \mathbb{F}_q[\Pi_1, \ldots, \Pi_{j-i-1}][\Pi_{j-i}]$ es de grado 1 en Π_{j-i} con coeficiente principal ± 1.

Demostración. Procedemos por inducción en $j \geq r$. Teniendo en cuenta que

$$T^r \equiv \Pi_1 T^{r-1} - \Pi_2 T^{r-2} + \cdots + (-1)^{r-1}\Pi_r \mod Q, \tag{7.10}$$

deducimos que (7.9) es válido para $j = r$ y $H_{0,r} = (-1)^{r-1}\Pi_r$ es mónico de grado 1 en Π_r. Supongamos que (7.9) vale para j con $r \leq j$. Multiplicando ambos lados de (7.9) por T y combinando este resultado con (7.10), obtenemos:

$$\begin{aligned} T^{j+1} &\equiv H_{r-1,j}T^r + H_{r-2,j}T^{r-1} + \cdots + H_{0,j}T \mod Q \\ &\equiv (\Pi_1 H_{r-1,j} + H_{r-2,j})T^{r-1} + \cdots + ((-1)^{r-2}\Pi_{r-1}H_{r-1,j} + H_{0,j})T \\ &\quad + (-1)^{r-1}\Pi_r H_{r-1,j} \mod Q. \end{aligned}$$

Definiendo

$$\begin{aligned} H_{k,j+1} &:= (-1)^{r-1-k}\Pi_{r-k}H_{r-1,j} + H_{k-1,j} \text{ para } 1 \leq k \leq r-1 \text{ y} \\ H_{0,j+1} &:= (-1)^{r-1}\Pi_r H_{r-1,j}, \end{aligned}$$

tenemos

$$T^{j+1} \equiv H_{r-1,j+1}T^{r-1} + H_{r-2,j+1}T^{r-2} + \cdots + H_{0,j+1} \mod Q.$$

Resta probar que el polinomio $H_{k,j+1}$ verifica las propiedades del enunciado del teorema.

Fijamos k con $1 \leq k \leq r-1$. Entonces $H_{k,j+1} = (-1)^{r-1-k}\Pi_{r-k}H_{r-1,j} + H_{k-1,j}$. Por hipótesis inductiva se tiene que $H_{r-1,j}$ y $H_{k-1,j}$ son polinomios nulos u homogéneos de grados $j-r+1$ y $j-k+1$ respectivamente. Luego, concluimos que $H_{k,j+1}$ es nulo o es un polinomio homogéneo de grado $j-k+1$. Además, para $j+1-k \leq r$, como $\max\{r-k, j-r+1\} \leq j-k < r$, se tiene que $\Pi_{r-k}H_{r-1,j}$ es un elemento del anillo $\mathbb{F}_q[\Pi_1, \ldots, \Pi_{j-k}]$. Por otro lado, $H_{k-1,j} \in \mathbb{F}_q[\Pi_1, \ldots, \Pi_{j-k}][\Pi_{j-k+1}]$ es de grado 1 en Π_{j-k+1} con coeficiente principal ± 1, lo cual implica que $H_{k,j+1}$ también lo es.

Finalmente, para $k = 0$ se tiene que $H_{0,j+1} := (-1)^{r-1}\Pi_r H_{r-1,j}$, lo que muestra que $H_{0,j+1}$ es nulo o es un polinomio homogéneo de $\mathbb{F}_q[X_1, \ldots, X_r]$ de grado $r+j-r+1 = j+1$. Así concluimos la demostración del lema. □

Observamos que, de manera similar a la Proposición 6.2.2, podemos obtener una fórmula explícita para cada polinomio $H_{i,j}$. Sin embargo, dado que no la necesitamos para lo que sigue, no vamos a darla.

Finalmente obtenemos una expresión para los polinomios $R^{\boldsymbol{a}}_j \in \mathbb{F}_q[X_1,\ldots,X_r]$ con $d-s \le j \le r-1$ en términos de los polinomios $H_{i,j}$.

Proposición 7.2.4. *Sean $s,d \in \mathbb{N}$ con $2(s+1) \le d$. Si $d-s \le j \le r-1$, entonces*

$$R^{\boldsymbol{a}}_j = a_j + \sum_{i=r}^{d} a_i H_{j,i}, \tag{7.11}$$

donde los polinomios $H_{j,i}$ son los definidos en el Lema 7.2.3. En particular, $R^{\boldsymbol{a}}_j$ es un polinomio mónico de $\mathbb{F}_q[\Pi_1,\ldots,\Pi_{d-1-j}][\Pi_{d-j}]$, salvo una constante no nula en $\mathbb{F}_q$, de grado $d-j \le s$, para $d-s \le j \le r-1$.

Demostración. Por el Lema 7.2.3, para $r \le j \le d$, se verifica la siguiente relación:

$$T^j \equiv H_{r-1,j}T^{r-1} + H_{r-2,j}T^{r-2} + \cdots + H_{0,j} \mod Q.$$

Luego,

$$\begin{aligned} f_a = \sum_{j=d-s}^{d} a_j T^j &= \sum_{j=d-s}^{r-1} a_j T^j + \sum_{j=r}^{d} a_j T^j \\ &\equiv \sum_{j=d-s}^{r-1} a_j T^j + \sum_{j=r}^{d} a_j \sum_{i=d-s}^{r-1} H_{i,j}T^i + \mathcal{O}(T^{d-s-1}) \mod Q \\ &\equiv \sum_{j=d-s}^{r-1} \left(a_j + \sum_{i=r}^{d} a_i H_{j,i}\right) T^j + \mathcal{O}(T^{d-s-1}) \mod Q, \end{aligned}$$

donde $\mathcal{O}(T^{d-s-1})$ representa la suma de los términos de $\mathbb{F}_q[X_1,\ldots,X_r][T]$ de grado a lo sumo $d-s-1$ en T. Esto muestra que los polinomios $R^{\boldsymbol{a}}_j$ verifican (7.11). Por otro lado, observemos que, para cada $H_{j,i}$ que aparece en la fórmula (7.11), se verifica que $i-j \le s \le d-s-2 \le r$. Esto implica que $H_{j,i} \in \mathbb{F}_q[\Pi_1,\ldots,\Pi_{i-j-1}][\Pi_{i-j}]$ es de grado 1 en Π_{j-i} con coeficiente principal ± 1 y de grado $i-j$ en las variables $X_1,\ldots,X_r$. En consecuencia, para cada $d-s \le j \le r-1$, $R^{\boldsymbol{a}}_j$ es un elemento mónico del anillo $\mathbb{F}_q[\Pi_1,\ldots,\Pi_{d-1-j}][\Pi_{d-j}]$, salvo una constante no nula en $\mathbb{F}_q$, de grado $d-j$ mirado como polinomio en $X_1,\ldots,X_r$. Esto concluye la demostración de la proposición. □

7.3. Propiedades de la variedad definida por $R^{\boldsymbol{a}}_{\boldsymbol{d-s}},\ldots,R^{\boldsymbol{a}}_{\boldsymbol{r-1}}$

Sean s y d enteros positivos con $d < q$ y $2(s+1) \le d$. Fijemos una s-upla $\boldsymbol{a} := (a_{d-1},\ldots,a_{d-s}) \in \mathbb{F}_q^s$ y consideremos el polinomio

$$f_{\boldsymbol{a}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s}.$$

En la Sección 7.2.1, para r fijo asociamos a $f_{\boldsymbol{a}}$ polinomios $R_j^{\boldsymbol{a}} \in \mathbb{F}_q[X_1,\ldots,X_r]$ con $d-s \le j \le r-1$. De acuerdo a la Proposición 7.2.4, podemos expresar cada polinomio $R_j^{\boldsymbol{a}}$ como un polinomio en $\Pi_1,\ldots,\Pi_s \in \mathbb{F}_q[X_1,\ldots,X_r]$. Más precisamente, si $Y_1,\ldots,Y_s$ son nuevas indeterminadas sobre $\overline{\mathbb{F}}_q$, entonces

$$R_j^{\boldsymbol{a}} = S_j^{\boldsymbol{a}}(\Pi_1,\ldots,\Pi_{d-j}) \quad (d-s \le j \le r-1),$$

donde cada $S_j^{\boldsymbol{a}} \in \mathbb{F}_q[Y_1,\ldots,Y_{d-j}]$ es de grado 1 en Y_{d-j} con coeficiente principal ± 1.

Consideremos la $\mathbb{F}_q$-variedad afín $V_r^{\boldsymbol{a}} \subset \mathbb{A}^r$ definida por los polinomios $R_{d-s}^{\boldsymbol{a}}$, $R_{d-s+1}^{\boldsymbol{a}},\ldots,R_{r-1}^{\boldsymbol{a}} \in \mathbb{F}_q[X_1,\ldots X_r]$. Mediante un argumento recursivo, es fácil probar que

$$\overline{\mathbb{F}}_q[Y_1,\ldots,Y_s]/(S_{d-s}^{\boldsymbol{a}},\ldots,S_j^{\boldsymbol{a}}) \simeq \overline{\mathbb{F}}_q[Y_1,\ldots,Y_{d-j-1}] \tag{7.12}$$

para $d-s \le j \le r-1$. Por lo tanto, se tiene que $S_{d-s}^{\boldsymbol{a}},\ldots,S_{r-1}^{\boldsymbol{a}}$ forman una sucesión regular de $\mathbb{F}_q[Y_1,\ldots,Y_s]$, es decir, satisfacen la hipótesis (H1) del comienzo del Capítulo 5. Además, teniendo en cuenta el isomorfismo (7.12) para $j=r-1$, deducimos que $S_{d-s}^{\boldsymbol{a}},\ldots,S_{r-1}^{\boldsymbol{a}}$ definen un ideal radical de $\mathbb{F}_q[Y_1,\ldots,Y_s]$ y la variedad $W_r^{\boldsymbol{a}} \subset \mathbb{A}^s$ definida por $S_{d-s}^{\boldsymbol{a}},\ldots,S_{r-1}^{\boldsymbol{a}}$ resulta isomorfa al espacio afín $\mathbb{A}^{d-r}$. Esto implica que $W_r^{\boldsymbol{a}}$ es una variedad no singular. Luego, la matriz $(\partial \boldsymbol{S}^{\boldsymbol{a}}/\partial \boldsymbol{Y})(\boldsymbol{y})$ tiene rango completo para todo $\boldsymbol{y} \in \mathbb{A}^s$, es decir, $S_{d-s}^{\boldsymbol{a}},\ldots,S_{r-1}^{\boldsymbol{a}}$ satisfacen la hipótesis (H2) del comienzo del Capítulo 5. Finalmente, como las hipótesis sobre los enteros d, r y s implican $r-d+s \le s \le d-s$, estamos en condiciones de aplicar los resultados del Capítulo 5 a la variedad $V_r^{\boldsymbol{a}}$. Combinando el Lema 5.1.1, el Teorema 5.2.1 y el Corolario 5.2.3, obtenemos el siguiente resultado.

Corolario 7.3.1. *Sea $V_r^{\boldsymbol{a}} \subset \mathbb{A}^r$ la $\mathbb{F}_q$-variedad afín definida por los polinomios $R_{d-s}^{\boldsymbol{a}},\ldots,R_{r-1}^{\boldsymbol{a}}$. Entonces $V_r^{\boldsymbol{a}}$ es una intersección completa de dimensión $d-s$, grado a lo sumo $s!/(d-r)!$ y lugar singular $\Sigma_r^{\boldsymbol{a}}$ de dimensión a lo sumo $s-1$.*

7.3.1. La clausura proyectiva de $V_r^{\boldsymbol{a}}$

Consideramos la clausura proyectiva $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \subset \mathbb{P}^r$ de $V_r^{\boldsymbol{a}}$. Vamos a estudiar el comportamiento de $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ en el hiperplano del infinito. Por la Proposición 7.2.4, para $d-s \le j \le r-1$ se tiene que

$$R_j^{\boldsymbol{a}} = a_j + \sum_{i=r}^{d} a_i H_{j,i},$$

donde los polinomios $H_{j,i}$ son homogéneos de grado $i-j$ o nulos. Por lo tanto, la homogeneización $R_j^{\boldsymbol{a},h}$ de cada uno de ellos es el siguiente polinomio de $\mathbb{F}_q[X_0,\ldots,X_r]$:

$$R_j^{\boldsymbol{a},h} = a_j X_0^{d-j} + \sum_{i=r}^{d} a_i H_{j,i} X_0^{d-i}. \tag{7.13}$$

Observación 7.3.2. *De (7.13) se deduce que $R_j^{\boldsymbol{a},h}(0,X_1,\ldots,X_r) = H_{j,d}$ para $d-s \le j \le r-1$, esto es, resultan los polinomios asociados al vector nulo de $\mathbb{F}_q^s$ y al polinomio $f_{\boldsymbol{0}} := T^d \in \mathbb{F}_q[T]$.*

Observación 7.3.3. *Por el Corolario 7.3.1, la variedad de $\mathbb{A}^r$ definida por los polinomios $H_{j,d}$ $(d-s\leq j\leq r-1)$ es un cono afín equidimensional de dimensión $d-s$, grado a lo sumo $s!/(d-r)!$ y lugar singular de dimensión a lo sumo $s-1$. Por lo tanto, la variedad proyectiva de $\mathbb{P}^{r-1}$ que definen estos polinomios es equidimensional de dimensión $d-s-1$, grado a lo sumo $s!/(d-r)!$ y lugar singular de dimensión a lo sumo $s-2$.*

Lema 7.3.4. *El lugar singular de* $\operatorname{pcl}(V^{\boldsymbol{a}}_r)$ *en el hiperplano del infinito tiene dimensión a lo sumo $s-2$.*

Demostración. Sea $\Sigma^{\boldsymbol{a}}_{r,\infty}\subset\mathbb{P}^r$ el lugar singular de $\operatorname{pcl}(V^{\boldsymbol{a}}_r)$ en el hiperplano del infinito y consideremos $\boldsymbol{x}:=(0:x_1:\cdots:x_r)\in\Sigma^{\boldsymbol{a}}_{r,\infty}$. Como los polinomios $R^{\boldsymbol{a},h}_j$ se anulan en $\operatorname{pcl}(V^{\boldsymbol{a}}_r)$, se tiene que $R^{\boldsymbol{a},h}_j(\boldsymbol{x})=H_{j,d}(x_1,\ldots,x_r)=0$ para $d-s\leq j\leq r-1$. Sea $(\partial H_d/\partial\boldsymbol{X})$ la matriz Jacobiana de $\{H_{j,d}:d-s\leq j\leq r-1\}$ con respecto a $X_1,\ldots,X_r$. Afirmamos que

$$\operatorname{rg}\left(\frac{\partial H_d}{\partial\boldsymbol{X}}\right)(\boldsymbol{x})<r-d+s. \tag{7.14}$$

En efecto, si el rango de la matriz $(\partial H_d/\partial\boldsymbol{X})$ es igual a $r-d+s$, entonces se verifica que $\dim\mathcal{T}_{\boldsymbol{x}}(\operatorname{pcl}(V^{\boldsymbol{a}}_r))\leq d-s$, lo cual implica que $\boldsymbol{x}$ es un punto regular de $\operatorname{pcl}(V^{\boldsymbol{a}}_r)$. Esto contradice la hipótesis sobre $\boldsymbol{x}$. Por las Observaciones 7.3.2 y 7.3.3, el conjunto de puntos que verifican (7.14) es un cono afín equidimensional de dimensión a lo sumo $s-1$, de lo que concluimos que la variedad proyectiva $\Sigma^{\boldsymbol{a}}_{r,\infty}$ tiene dimensión a lo sumo $s-2$. □

Teorema 7.3.5. $\operatorname{pcl}(V^{\boldsymbol{a}}_r)\cap\{X_0=0\}\subset\mathbb{P}^{r-1}$ *es una intersección completa absolutamente irreducible de dimensión $d-s-1$, grado $s!/(d-r)!$ y lugar singular de dimensión a lo sumo $s-2$.*

Demostración. Por la Observación 7.3.2 se tiene que la variedad proyectiva $V(H_{j,d}:d-s\leq j\leq r-1)\subset\mathbb{P}^{r-1}$ es una intersección completa conjuntista cuyo lugar singular tiene codimensión al menos $d-s-1-(s-2)\geq 3$. Luego, por el Teorema de Conexión de Hartshorne (ver, por ejemplo, [Kun85, Theorem 4.2]) resulta que $V(H_{j,d}:d-s\leq j\leq r-1)$ es absolutamente irreducible.

Observemos que $\operatorname{pcl}(V^{\boldsymbol{a}}_r)$ es equidimensional de dimensión $d-s$. Por lo tanto, cada componente irreducible de $\operatorname{pcl}(V^{\boldsymbol{a}}_r)\cap\{X_0=0\}$ tiene dimensión al menos $d-s-1$. Además, de (7.13) se deduce que $\operatorname{pcl}(V^{\boldsymbol{a}}_r)\cap\{X_0=0\}$ está contenida en la variedad proyectiva $V(H_{j,d}:d-s\leq j\leq r-1)$. Como $V(H_{j,d}:d-s\leq j\leq r-1)$ es absolutamente irreducible de dimensión $d-s-1$, concluimos que $\operatorname{pcl}(V^{\boldsymbol{a}}_r)\cap\{X_0=0\}$ es también absolutamente irreducible y, por lo tanto,

$$\operatorname{pcl}(V^{\boldsymbol{a}}_r)\cap\{X_0=0\}=V(H_{j,d}:d-s\leq j\leq r-1).$$

Finalmente, por [Eis95, Theorem 18.15] deducimos que los polinomios $H_{j,d}$ $(d-s\leq j\leq r-1)$ definen un ideal radical. En consecuencia, obtenemos que

$$\deg(\operatorname{pcl}(V^{\boldsymbol{a}}_r)\cap\{X_0=0\})=\prod_{j=d-s}^{r-1}\deg H_{j,d}=s!/(d-r)!$$

(ver, por ejemplo, [Har92, Theorem 18.3]). Esto concluye la demostración. □

Finalizamos esta sección con un teorema que recopila todas las propiedades de la clausura proyectiva $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ que necesitamos.

Teorema 7.3.6. *La variedad proyectiva* $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \subset \mathbb{P}^r$ *es una intersección completa, absolutamente irreducible, de dimensión* $d-s$*, grado* $s!/(d-r)!$ *y lugar singular de dimensión a lo sumo* $s-1$*.*

Demostración. Probamos primero que $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ es una variedad equidimensional de dimensión $d-s$ y grado a lo sumo $s!/(d-r)!$. Por el Corolario 6.3.1, el conjunto de puntos singulares de $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ que pertenecen al abierto $\{X_0 \neq 0\}$ tiene dimensión a lo sumo $s-1$, mientras que por el Lema 7.3.4 se tiene que el conjunto de puntos singulares en el infinito tiene dimensión a lo sumo $s-2$. Por lo tanto, el lugar singular de $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ tiene dimensión a lo sumo $s-1$. Por otro lado, observemos que $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ está contenido en la variedad proyectiva $V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$. Además,

$$V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1) \cap \{X_0 \neq 0\} \subset V(R_j^{\boldsymbol{a}} : d-s \leq j \leq r-1),$$
$$V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1) \cap \{X_0 = 0\} \subset V(H_{d,j} : d-s \leq j \leq r-1).$$

Por el Corolario 7.3.1 tenemos que $V(R_j^{\boldsymbol{a}} : d-s \leq j \leq r-1) \subset \mathbb{A}^r$ es equidimensional de dimensión $d-s$ y $V(H_{d,j} : d-s \leq j \leq r-1) \subset \mathbb{P}^{r-1}$ es equidimensional de dimensión $d-s-1$. Por lo tanto, $V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$ tiene dimensión a lo sumo $d-s$. Teniendo en cuenta que está definida por $r-d+s$ polinomios, deducimos que es una intersección completa conjuntista de dimensión $r-(r-d+s) = d-s$. Esto implica que es equidimensional de dimensión $d-s$ y, por lo tanto, ninguna de sus componentes irreducibles está contenida en el hiperplano del infinito. En particular, coincide con su clausura proyectiva restringida al espacio afín $\mathbb{A}^r$ (ver, por ejemplo, [Kun85, Proposition I.5.17]). Como dicha restricción es la variedad afín $V_r^{\boldsymbol{a}} = V(R_j^{\boldsymbol{a}} : \ d-s \leq j \leq r-1)$, obtenemos que

$$\mathrm{pcl}(V_r^{\boldsymbol{a}}) = V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1).$$

Como el lugar singular de $V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$ tiene dimensión a lo sumo $s-1$ y $d-s-(s-1) \geq 3$, deducimos que es absolutamente irreducible por el Teorema de Conexión de Hartshorne (ver, por ejemplo, [Kun85, Theorem 4.2]). Finalmente, con el mismo argumento de la demostración del Teorema 7.3.5, de [Eis95, Theorem 18.15] se sigue que los polinomios $R_j^{\boldsymbol{a},h}$ $(d-s \leq j \leq r-1)$ definen un ideal radical. Esto implica que $\deg \mathrm{pcl}\big(V_r^{\boldsymbol{a}}\big) = \prod_{j=d-s}^{r-1} \deg R_j^{\boldsymbol{a},h} = s!/(d-r)!$ (ver, por ejemplo, [Har92, Theorem 18.3]). □

7.4. Estimación de la cantidad de puntos q-racionales de $V_r^{\boldsymbol{a}}$

Recordemos que nuestro objetivo es estimar el comportamiento del cardinal promedio del conjunto de valores $\mathcal{V}(d,s,\boldsymbol{a})$ (ver (7.1)). De acuerdo al Teorema 7.2.1,

para $d-s+1 \leq r \leq d$ tenemos que determinar el número $\chi_r^{\boldsymbol{a}}$ de subconjuntos de r elementos $\mathcal{X}_r \subset \mathbb{F}_q$ tales que existe un polinomio $g \in \mathbb{F}_q[T]$ de grado a lo sumo $d-s-1$ que interpola al polinomio $-f_{\boldsymbol{a}}$ (ver (7.2)) en $\mathcal{X}_r$. En la Sección 7.2.1 probamos que cada $\boldsymbol{a}$ tiene asociados polinomios $R_j^{\boldsymbol{a}} \in \mathbb{F}_q[X_1,\ldots,X_r]$ con $d-s \leq j \leq r-1$. Luego probamos que el número de puntos q-racionales con coordenadas distintas de la variedad $V_r^{\boldsymbol{a}}$ definida por estos polinomios es igual a $r!\chi_r^{\boldsymbol{a}}$, es decir,

$$\chi_r^{\boldsymbol{a}} = \frac{1}{r!}\left|\left\{\boldsymbol{x} \in \mathbb{F}_q^r : R_j^{\boldsymbol{a}}(\boldsymbol{x}) = 0\,(d-s \leq j \leq r-1), x_k \neq x_l\,(1 \leq k < l \leq r)\right\}\right|.$$

A continuación obtenemos una estimación del número $\chi_r^{\boldsymbol{a}}$.

Teorema 7.4.1. *Sean $\boldsymbol{a} \in \mathbb{F}_q^s$, d, r y s enteros positivos con $d < q$ y $2(s+1) \leq d$. Para $d-s+1 \leq r \leq d$ se verifica que*

$$\left|\chi_r^{\boldsymbol{a}} - \frac{q^{d-s}}{r!}\right| \leq \frac{r(r-1)}{2r!}\,\delta_r q^{d-s-1} + \frac{14}{r!}D_r^3\delta_r^2(q+1)q^{d-s-2},$$

donde $D_r := \sum_{j=d-r+1}^{s}(j-1)$ y $\delta_r := \prod_{j=d-r+1}^{s} j = s!/(d-r)!$.

Demostración. En primer lugar estimamos la cantidad de puntos q-racionales de $V_r^{\boldsymbol{a}}$. Consideramos $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ y sea $V_{r,\infty}^{\boldsymbol{a}} := \mathrm{pcl}(V_r^{\boldsymbol{a}}) \cap \{X_0 = 0\}$. Combinando los Teoremas 7.3.5 y 7.3.6 con la estimación (4.17) obtenemos

$$\begin{aligned}\left||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)| - p_{d-s}\right| &\leq 14D_r^3\delta_r^2 q^{d-s-1},\\ \left||V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)| - p_{d-s-1}\right| &\leq 14D_r^3\delta_r^2 q^{d-s-2}.\end{aligned}$$

Como consecuencia, la cantidad de puntos q-racionales de $V_r^{\boldsymbol{a}}$ satisface la siguiente estimación:

$$\begin{aligned}\left||V_r^{\boldsymbol{a}}(\mathbb{F}_q)| - q^{d-s}\right| &= \left||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)| - |V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)| - p_{d-s} + p_{d-s-1}\right|\\ &\leq \left||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)| - p_{d-s}\right| + \left||V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)| - p_{d-s-1}\right|\\ &\leq 14D_r^3\delta_r^2(q+1)q^{d-s-2}. \qquad (7.15)\end{aligned}$$

En segundo lugar obtenemos una cota superior de la cantidad de puntos q-racionales de $V_r^{\boldsymbol{a}}$ con al menos dos coordenadas que toman el mismo valor. Sea

$$V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q) := \bigcup_{1\leq i<j\leq r} V_r^{\boldsymbol{a}}(\mathbb{F}_q) \cap \{X_i = X_j\},$$

y sea $V_{r,\neq}^{\boldsymbol{a}}(\mathbb{F}_q) := V_r^{\boldsymbol{a}}(\mathbb{F}_q) \setminus V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q)$. Consideremos $\boldsymbol{x} := (x_1,\ldots,x_r) \in V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q)$. Sin pérdida de generalidad podemos suponer que $x_{r-1} = x_r$. Luego $\boldsymbol{x}$ es un punto q-racional de la variedad afín $W_{r-1,r} \subset \{X_{r-1} = X_r\}$ definida por los polinomios $S_{d-s}^{\boldsymbol{a}}(\Pi_1^*,\ldots,\Pi_s^*),\ldots,S_{r-1}^{\boldsymbol{a}}(\Pi_1^*,\ldots,\Pi_s^*) \in \mathbb{F}_q[X_1,\ldots X_{r-1}]$, con $\Pi_i^* \in \mathbb{F}_q[X_1,\ldots,X_{r-1}]$ el polinomio definido por $\Pi_i^* := \Pi_i(X_1,\ldots,X_{r-1},X_{r-1})$, $(1 \leq i \leq s)$, que se obtiene al reemplazar X_{r-1} por X_r en el i-ésimo polinomio simétrico elemental $\Pi_i \in \mathbb{F}_q[X_1,\ldots,X_r]$. Dado que $\Pi_1^*,\ldots,\Pi_s^*$ son algebraicamente independientes en

$\overline{\mathbb{F}}_q[X_1,\dots,X_{r-1}]$, entonces $S^{\boldsymbol{a}}_{d-s}(\Pi^*_1,\dots,\Pi^*_s),\dots,S^{\boldsymbol{a}}_{r-1}(\Pi^*_1,\dots,\Pi^*_s)$ forman una sucesión regular de $\mathbb{F}_q[X_1,\dots X_{r-1}]$. Esto implica que $W_{r-1,r}$ tiene dimensión $d-s-1$. Por otro lado, como $W_{r-1.r}=V^{\boldsymbol{a}}_r\cap\{X_r=X_{r-1}\}$, (2.2) implica que $\deg W_{r-1,r}\le\deg V^{\boldsymbol{a}}_r$. Luego, por la Proposición 2.3.4 (ii) se tiene que

$$|W_{r-1,r}(\mathbb{F}_q)|\le\deg W_{r-1,r}q^{d-s-1}\le\deg V^{\boldsymbol{a}}_r q^{d-s-1}.$$

En consecuencia, obtenemos

$$|V^{\boldsymbol{a}}_{r,=}(\mathbb{F}_q)|\le\frac{r(r-1)}{2}\,\delta_r\,q^{d-s-1}.$$

Combinando (7.15) con esta cota superior, se tiene que

$$\big||V^{\boldsymbol{a}}_{r,\neq}(\mathbb{F}_q)|-q^{d-s}\big|\le\frac{r(r-1)}{2}\,\delta_r\,q^{d-s-1}+14D_r^3\delta_r^2(q+1)q^{d-s-2}.$$

De esta última desigualdad se deduce fácilmente el teorema. □

A partir de la estimación del Teorema 7.4.1 podemos determinar el comportamiento asintótico de $\mathcal{V}(d,s,\boldsymbol{a})$.

Corolario 7.4.2. *Con las hipótesis del Teorema 7.4.1, tenemos la siguiente estimación:*

$$\left|\mathcal{V}(d,s,\boldsymbol{a})-\mu_d\,q-\frac{1}{2e}\right|\le\frac{s^2+1}{(d-s-1)!}+\frac{21}{8}\frac{s^6(s!)^2}{d!}\sum_{k=0}^{s-1}\binom{d}{k}\frac{1}{k!}+\frac{7}{q}.\tag{7.16}$$

Demostración. Por el Teorema 7.2.1, se tiene

$$\begin{aligned}\mathcal{V}(d,s,\boldsymbol{a})-\mu_d\,q=&\sum_{r=1}^{d-s}(-q)^{1-r}\left(\binom{q}{r}-\frac{q^r}{r!}\right)\\&+\frac{1}{q^{d-s-1}}\sum_{r=d-s+1}^{d}(-1)^{r-1}\left(\chi^{\boldsymbol{a}}_r-\frac{q^{d-s}}{r!}\right).\end{aligned}\tag{7.17}$$

En primer lugar acotamos superiormente el valor absoluto $A(d,s)$ del primer término en el lado derecho de (7.17). Para ello, dados enteros positivos k,n con $k\le n$, denotamos como $\left[\begin{smallmatrix}n\\k\end{smallmatrix}\right]$ al número de Stirling de primera clase, es decir, el número de permutaciones de n elementos con k ciclos disjuntos. Las siguientes son propiedades básicas de los números de Stirling (ver, por ejemplo, [FS09, §A.8]):

$$\begin{bmatrix}r\\r\end{bmatrix}=1,\quad\begin{bmatrix}r\\r-1\end{bmatrix}=\binom{r}{2},\quad\sum_{k=0}^{r}\begin{bmatrix}r\\k\end{bmatrix}=r!.$$

Teniendo en cuenta la identidad $\binom{q}{r}=\sum_{k=0}^{r}\frac{(-1)^{r-k}}{r!}\left[\begin{smallmatrix}r\\k\end{smallmatrix}\right]q^k$, obtenemos

$$\begin{aligned}A(d,s):=\sum_{r=2}^{d-s}(-q)^{1-r}\left(\binom{q}{r}-\frac{q^r}{r!}\right)&=\sum_{r=2}^{d-s}q^{1-r}\sum_{k=0}^{r-1}\frac{(-1)^{k+1}}{r!}\begin{bmatrix}r\\k\end{bmatrix}q^k\\&=\sum_{r=0}^{d-s-2}\frac{(-1)^r}{2r!}+\sum_{r=2}^{d-s}q^{1-r}\sum_{k=0}^{r-2}\frac{(-1)^{k+1}}{r!}\begin{bmatrix}r\\k\end{bmatrix}q^k.\end{aligned}$$

El segundo término de lado derecho de esta expresión se puede acotar por

$$\sum_{k=0}^{r-2} \frac{1}{r!} \begin{bmatrix} r \\ k \end{bmatrix} q^k \leq \sum_{k=0}^{r-3} \frac{1}{r!} \begin{bmatrix} r \\ k \end{bmatrix} q^k + \frac{1}{r!} \begin{bmatrix} r \\ r-2 \end{bmatrix} q^{r-2} \leq q^{r-3} + \frac{8}{r^2} q^{r-2} \leq \left(\frac{1}{d} + \frac{8}{r^2} \right) q^{r-2}.$$

Como consecuencia

$$\left| A(d,s) - \frac{1}{2e} \right| \leq \frac{1}{2 \cdot (d-s-1)!} + \sum_{r=2}^{d-s} \left(\frac{1}{d} + \frac{8}{r^2} \right) \frac{1}{q} \leq \frac{1}{2 \cdot (d-s-1)!} + \frac{7}{q}. \quad (7.18)$$

Consideramos ahora el valor absoluto del segundo término del lado derecho de (7.17). Por el Teorema 7.4.1 se tiene

$$\begin{aligned} B(d,s) &:= \frac{1}{q^{d-s-1}} \sum_{r=d-s+1}^{d} \left| \chi_r^{\boldsymbol{a}} - \frac{q^{d-s}}{r!} \right| \\ &\leq \sum_{r=d-s+1}^{d} \frac{r(r-1)}{2r!} \delta_r + \sum_{r=d-s+1}^{d} \frac{14}{r!} D_r^3 \delta_r^2 \left(1 + \frac{1}{q} \right). \end{aligned}$$

Ahora bien, el primer término del lado derecho de esta última desigualdad se puede escribir de la siguiente manera:

$$\begin{aligned} \sum_{r=d-s+1}^{d} \frac{r(r-1)}{2r!} \delta_r &= \frac{s!}{2(d-2)!} \sum_{r=d-s+1}^{d} \binom{d-2}{r-2} \\ &\leq \frac{s \cdot s!}{2(d-2)!} \binom{d-2}{s-1} = \frac{s^2}{2(d-s-1)!}. \end{aligned}$$

Por otro lado,

$$\sum_{r=d-s+1}^{d} \frac{14}{r!} D_r^3 \delta_r^2 \leq \frac{7}{4} \sum_{r=d-s+1}^{d} \frac{s^3 (s-1)^3 (s!)^2}{r!((d-r)!)^2} = \frac{7}{4} \sum_{k=0}^{s-1} \frac{s^6 (s!)^2}{(d-k)!(k!)^2}.$$

Finalmente obtenemos,

$$B(d,s) \leq \frac{s^2}{2(d-s-1)!} + \frac{21}{8} \frac{s^6 (s!)^2}{d!} \sum_{k=0}^{s-1} \binom{d}{k} \frac{1}{k!}.$$

Combinando las cotas superiores de $A(d,s)$ y $B(d,s)$ se deduce el corolario. □

Por último, vamos a analizar el comportamiento del lado derecho de (7.16). Esto nos permitirá mostrar que el término de error tiende a cero cuando d tiende a infinito.

Fijamos k con $0 \leq k \leq s-1$ y consideramos la función $h(k) := \binom{d}{k} \frac{1}{k!}$. Analizando el signo de las diferencias $h(k+1) - h(k)$ para $0 \leq k \leq s-2$, deducimos el siguiente resultado.

Observación 7.4.3. *Sea* $k_0 := -1/2 + \sqrt{5+4d}/2$. *Entonces* h *es una función unimodal en el intervalo de enteros* $[0, s-1]$, *es decir, existe* $c \in (0, s+1)$ *tal que* h *es creciente en* $(0, c)$ *y decreciente en* $(c, s-1)$, *y alcanza su máximo en* $\lfloor k_0 \rfloor$.

A partir de la Observación 7.4.3 vemos que

$$\frac{s^6(s!)^2}{d!}\sum_{k=0}^{s-1}\binom{d}{k}\frac{1}{k!} \leq \frac{s^7(s!)^2}{d!}\binom{d}{\lfloor k_0\rfloor}\frac{1}{\lfloor k_0\rfloor!} = \frac{s^7(s!)^2}{(d-\lfloor k_0\rfloor)!(\lfloor k_0\rfloor!)^2}. \tag{7.19}$$

Para obtener una cota superior del lado derecho de (7.19) utilizamos la fórmula de Stirling (ver, por ejemplo, [FS09, p. 747]): para $m \in \mathbb{N}$, existe θ con $0 \leq \theta < 1$ tal que se verifica $m! = (m/e)^m\sqrt{2\pi m}\, e^{\theta/12m}$. Aplicando esta fórmula y teniendo en cuenta que $2(s+1) \leq d$, vemos que existen θ_i $(i = 1, 2, 3)$ con $0 \leq \theta_i < 1$ tales que

$$C(d,s) := \frac{s^7(s!)^2}{(d-\lfloor k_0\rfloor)!(\lfloor k_0\rfloor!)^2} \leq \frac{(\frac{d}{2}-1)^8(\frac{d}{2}-1)^{d-2}\, e^{2+\lfloor k_0\rfloor+\frac{\theta_1}{3d-6}-\frac{\theta_2}{12(d-\lfloor k_0\rfloor)}-\frac{\theta_3}{6\lfloor k_0\rfloor}}}{\big(d-\lfloor k_0\rfloor\big)^{d-\lfloor k_0\rfloor}\sqrt{2\pi(d-\lfloor k_0\rfloor)}\lfloor k_0\rfloor^{2\lfloor k_0\rfloor+1}}.$$

De cálculos elementales se sigue que

$$\begin{aligned}
(d-\lfloor k_0\rfloor)^{-d+\lfloor k_0\rfloor} &\leq d^{-d+\lfloor k_0\rfloor}e^{\lfloor k_0\rfloor(d-\lfloor k_0\rfloor)/d},\\
\frac{d^{\lfloor k_0\rfloor}}{\lfloor k_0\rfloor^{2\lfloor k_0\rfloor}} &\leq e^{(d-\lfloor k_0\rfloor^2)/\lfloor k_0\rfloor},\\
\left(\frac{d}{2}-1\right)^{d-2} &\leq \left(\frac{d}{2}\right)^{d-2} e^{4/d-2}.
\end{aligned}$$

Luego,

$$C(d,s) \leq \left(\frac{d}{2}-1\right)^8 \frac{e^{\lfloor k_0\rfloor+\frac{1}{3d-6}+\frac{4}{d}+\frac{\lfloor k_0\rfloor}{d}(d-\lfloor k_0\rfloor)+\frac{1}{\lfloor k_0\rfloor}(d-\lfloor k_0\rfloor^2)}}{d^2 2^{d-2}\sqrt{2\pi(d-\lfloor k_0\rfloor)}\lfloor k_0\rfloor}.$$

De acuerdo a la definición de $\lfloor k_0\rfloor$, es fácil ver que

$$\begin{aligned}
\lfloor k_0\rfloor + \frac{\lfloor k_0\rfloor}{d}(d-\lfloor k_0\rfloor) &\leq 2\lfloor k_0\rfloor - \frac{1}{5},\\
\frac{1}{\lfloor k_0\rfloor}(d-\lfloor k_0\rfloor^2) &\leq 4,\\
\frac{(\frac{d}{2}-1)^3}{d^2\lfloor k_0\rfloor\sqrt{d-\lfloor k_0\rfloor}} &\leq \frac{3}{20}.
\end{aligned}$$

Por lo tanto, teniendo en cuenta que $d \geq 2$, concluimos que

$$C(d,s) \leq \frac{3(\frac{d}{2}-1)^5 e^{\frac{1}{3d-6}+\frac{4}{d}-\frac{1}{5}+3+\sqrt{5+4d}}}{5\sqrt{2\pi}\,2^d}. \tag{7.20}$$

Combinando estas cotas con el Corolario 7.4.2 obtenemos el siguiente resultado.

Teorema 7.4.4. *Bajo las hipótesis del Teorema 7.4.1, se verifica*

$$\left|\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d\, q - \frac{1}{2e}\right| \leq \frac{(d-2)^5 e^{2\sqrt{d}}}{2^{d-2}} + \frac{7}{q}.$$

Demostración. Teniendo en cuenta (7.20) y que $\sqrt{5+4d} \leq 4/5 + 2\sqrt{d}$ para $d \geq 2$, concluimos que

$$\frac{21}{8}\frac{s^6(s!)^2}{d!}\sum_{k=0}^{s-1}\binom{d}{k}\frac{1}{k!} \leq 3\,\frac{(d-2)^5 e^{2\sqrt{d}}}{2^d}.$$

Por otro lado, es fácil ver que

$$\frac{s^2+1}{2(d-s-1)!} \leq \frac{(d-2)^5 e^{2\sqrt{d}}}{2^d}.$$

A partir de estas desigualdades se deduce el teorema. □

Para finalizar, hacemos algunos comentarios sobre el comportamiento de la cota de (7.4.4).

Observación 7.4.5. *Consideremos la función $f : \mathbb{Z}_{\geq 4} \to \mathbb{R}$ definida por $f(d) := (d-2)^5 e^{2\sqrt{d}} 2^{-d}$. Se verifica que f es una función unimodal, alcanza su máximo en $d_0 := 14$ y $f(d_0) \approx 1.08 \cdot 10^5$. Es fácil ver que $\lim_{d\to+\infty} f(d) = 0$, de hecho, si $d \geq 51$ entonces $f(d) < 1$.*

7.5. Otra estimación de la cantidad de puntos q-racionales de $V_r^{\boldsymbol{a}}$

A continuación vamos a estimar el cardinal $\mathcal{V}(d,s,\boldsymbol{a})$ aplicando nuestra versión explícita de la estimación de Hooley (Teorema 4.2.8). De acuerdo a la igualdad (7.17), debemos estudiar el comportamiento del número $\chi_r^{\boldsymbol{a}}$. Recordemos que $r!\chi_r^{\boldsymbol{a}}$ coincide con la cantidad de puntos q-racionales con coordenadas distintas de la variedad $V_r^{\boldsymbol{a}}$, por lo que comenzamos estimando dicha cantidad. Para esto, recordemos que $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \subset \mathbb{P}^r$ y $V_{r,\infty}^{\boldsymbol{a}} := \mathrm{pcl}(V_r^{\boldsymbol{a}}) \cap \{X_0 = 0\} \subset \mathbb{P}^{r-1}$ son intersecciones completas absolutamente irreducibles definidas sobre $\mathbb{F}_q$, de dimensión $d-s$ y $d-s-1$ respectivamente, ambas de grado $\delta_r := s!/(d-r)!$. El lugar singular de $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ es de dimensión a lo sumo $s-1$ y el de $V_{r,\infty}^{\boldsymbol{a}}$ es de dimensión a lo sumo $s-2$. Recordemos la notación $D_r := \sum_{j=d-r+1}^{s}(j-1)$. Supongamos que $q > 2s\delta_r(D_r^{d-2s}(D_r+d-2s+1)+1)$. Luego, de acuerdo a la estimación (4.28), tenemos que

$$\big||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)| - p_{d-s}\big| \leq \Big(b'_{d-2s}(r-s,\boldsymbol{d}) + 2\sqrt{\delta_r} + 1\Big)q^{d/2},$$

$$\big||V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)| - p_{d-s-1}\big| \leq \Big(b'_{d-2s}(r-s,\boldsymbol{d}) + 2\sqrt{\delta_r} + 1\Big)q^{d/2-1}.$$

Así, la cantidad de puntos q-racionales de $V_r^{\boldsymbol{a}}$ satisface la estimación

$$\begin{aligned}\big||V_r^{\boldsymbol{a}}(\mathbb{F}_q)| - q^{d-s}\big| &= \big||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)| - |V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)| - p_{d-s} + p_{d-s-1}\big| \\ &\leq \big||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)| - p_{d-s}\big| + \big||V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)| - p_{d-s-1}\big| \\ &\leq \Big(b'_{d-2s}(r-s,\boldsymbol{d}) + 2\sqrt{\delta_r} + 1\Big)q^{d/2-1}(q+1). \qquad (7.21)\end{aligned}$$

Recordemos que la cantidad de puntos q-racionales de $V_r^{\boldsymbol{a}}$ con al menos dos coordenadas que toman el mismo valor se acota superiormente por

$$|V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q)| \leq \frac{r(r-1)}{2}\delta_r q^{d-s-1}.$$

Luego, combinando esta cota superior con (7.21), se tiene que la cantidad de puntos q-racionales de $V_r^{\boldsymbol{a}}$ cuyas coordenadas son distintas dos a dos satisface la estimación

$$\begin{aligned}\big||V_{r,\neq}^{\boldsymbol{a}}(\mathbb{F}_q)| - q^{d-s}\big| \leq\ & \frac{r(r-1)}{2}\delta_r q^{d-s-1} \\ &+ \Big(b'_{d-2s}(r-s,\boldsymbol{d}) + 2\sqrt{\delta_r} + 1\Big)q^{d/2-1}(q+1). \qquad (7.22)\end{aligned}$$

A partir de (7.22) obtenemos el siguiente resultado.

Teorema 7.5.1. *Sean $\boldsymbol{a} \in \mathbb{F}_q^s$, d, r y s enteros positivos con $d < q$ y $2(s+1) \leq d$. Supongamos que $q > 2s\delta_r(D_r^{d-2s}(D_r+d-2s+1)+1)$. Entonces, para $d-s+1 \leq r \leq d$, se verifica que*

$$\begin{aligned}\left|\chi_r^{\boldsymbol{a}} - \frac{q^{d-s}}{r!}\right| \leq\ & \frac{1}{2(r-2)!}\delta_r q^{d-s-1} \\ &+ \frac{1}{r!}\Big(b'_{d-2s}(r-s,\boldsymbol{d}) + 2\sqrt{\delta_r} + 1\Big)q^{d/2-1}(q+1). \qquad (7.23)\end{aligned}$$

donde $D_r := \sum_{j=d-r+1}^{s}(j-1)$ y $\delta_r := \prod_{j=d-r+1}^{s} j = s!/(d-r)!$.

Teniendo en cuenta la igualdad (7.17), vamos a acotar el valor absoluto $B(d,s)$ del segundo término de la misma utilizando la estimación (7.23). Así, resulta

$$\begin{aligned}B(d,s) &:= \frac{1}{q^{d-s-1}}\sum_{r=d-s+1}^{d}\left|\chi_r^{\boldsymbol{a}} - \frac{q^{d-s}}{r!}\right| \\ &\leq \sum_{r=d-s+1}^{d}\frac{1}{2(r-2)!}\delta_r + q^{s-d/2}(q+1)\sum_{r=d-s+1}^{d}\frac{1}{r!}\Big(b'_{d-2s}(r-s,\boldsymbol{d}) + 2\sqrt{\delta_r} + 1\Big).\end{aligned}$$

Recordamos que para el primer término del lado derecho de esta última desigualdad se acota de la siguiente manera:

$$\sum_{r=d-s+1}^{d}\frac{1}{2(r-2)!}\delta_r = \sum_{r=d-s+1}^{d}\frac{r(r-1)}{2r!}\,\delta_r \leq \frac{s^2}{2(d-s-1)!}. \qquad (7.24)$$

A continuación acotamos el segundo término del lado derecho de esta última desigualdad. Por un lado, es fácil ver que se verifica la siguiente cota:

$$\sum_{r=d-s+1}^{d} \frac{1}{r!} \leq \frac{s}{(d-s+1)!}. \tag{7.25}$$

Por otro lado,

$$\sum_{r=d-s+1}^{d} \frac{2\sqrt{\delta_r}}{r!} = \sum_{k=0}^{s-1} \frac{2\sqrt{s!}}{(d-k)!\sqrt{k!}} = \frac{2\sqrt{s!}}{d!} \sum_{k=0}^{s-1} \binom{d}{k} \sqrt{k!}.$$

Dado que la función $f(k) = \binom{d}{k}\sqrt{k!}$ es creciente para $0 \leq k \leq s-1$, obtenemos la siguiente desigualdad:

$$\sum_{r=d-s+1}^{d} \frac{2\sqrt{\delta_r}}{r!} \leq \frac{2\,s^2}{(d-s+1)!}. \tag{7.26}$$

Finalmente acotamos la suma

$$\sum_{r=d-s+1}^{d} \frac{1}{r!} b'_{r-2s}(r-s, \boldsymbol{d}).$$

Para esto, utilizamos la siguiente cota superior de $b'_{d-2s}(r-s, \boldsymbol{d})$ (ver, por ejemplo, [GL02a, Proposition 4.2]):

$$b'_{d-2s}(r-s, \boldsymbol{d}) \leq (-1)^{d-2s+1}(d-2s+1) + \frac{s!}{(d-r)!}\binom{r-s+1}{d-2s}(s+1)^{d-2s}.$$

Así, tenemos que

$$\begin{aligned}\sum_{r=d-s+1}^{d} \frac{1}{r!} b'_{d-2s}(r-s, \boldsymbol{d}) \leq & \sum_{r=d-s+1}^{d} \frac{1}{r!}(d-2s+1) \\ & + \frac{s!}{d!}(s+1)^{d-2s} \sum_{r=d-s+1}^{d} \binom{d}{r}\binom{r-s+1}{d-2s}.\end{aligned}$$

Analizamos ahora el segundo término de la desigualdad precedente, es decir,

$$\frac{s!}{d!}(s+1)^{d-2s} \sum_{r=d-s+1}^{d} \binom{d}{r}\binom{r-s+1}{d-2s}.$$

Dado que la función $h(r) = \binom{d}{r}$ es decreciente para $d-s+1 \leq r \leq d$, y por la identidad $\sum_{k=0}^{n}\binom{k}{m} = \binom{n+1}{m+1}$ (ver, por ejemplo, [GKP89, p. 174]), se obtiene

$$\frac{s!}{d!}(s+1)^{d-2s} \sum_{r=d-s+1}^{d} \binom{d}{r}\binom{r-s+1}{d-2s} \leq \frac{(s+1)^{d-2s-1}(d-s+2)}{(s-1)!(d-2s+1)!}.$$

En consecuencia,

$$\sum_{r=d-s+1}^{d} \frac{1}{r!} b'_{d-2s}(r-s, \boldsymbol{d}) \leq \frac{(d-2s+1)s}{(d-s+1)!} + \frac{(s+1)^{d-2s-1}(d-s+2)}{(s-1)!(d-2s+1)!}.$$

Combinando esta última desigualdad con (7.25) y (7.26), por medio de cálculos elementales obtenemos que

$$\sum_{r=d-s+1}^{d} \frac{1}{r!}(1+2\sqrt{\delta_r}+b'_{d-2s}(r-s,\boldsymbol{d})) \leq \frac{3d}{(d-s)!} + \frac{2^{d-2s}\, s^{d-2s} d}{s!(d-2s+1)!}.$$

Aplicando la fórmula de Stirling (ver, por ejemplo, [FS09, p. 747]), dado que $(d-s)^{-d+s} \leq d^{-d+s} e^{s-s^2/d}$, se deduce que

$$\frac{3d}{(d-s)!} \leq \frac{3e^{d-s^2/d}}{\sqrt{2\pi} d^{d-s-1/2}} \leq \frac{9}{5}\frac{e^d}{d^s}. \tag{7.27}$$

Por otro lado, aplicando nuevamente la fórmula de Stirling, y teniendo en cuenta la desigualdad

$$(d-2s+1)^{-d+2s-1} \leq d^{-d+2s-1} e^{2s-1-(1-2s)^2/d},$$

y que $s \leq d/2-1$ y $\sqrt{s(d-2s+1)} \geq \sqrt{3}$, concluimos que

$$\frac{2^{d-2s} s^{d-2s} d}{s!(d-2s+1)!} \leq \frac{2^{d-2s} s^{d-3s} e^{d+s} d^{-d+2s}}{2\pi\sqrt{s(d-2s+1)}} \leq \frac{2^s e^{d+s}}{2\pi\sqrt{3} d^s} \leq \frac{1}{25}\frac{2^s e^{3d/2}}{d^s}. \tag{7.28}$$

Así, de (7.24), (7.27) y (7.28) se deduce la siguiente cota para $B(d,s)$:

$$B(d,s) \leq \frac{s^2}{2(d-s-1)!} + \frac{4\, e^{2d}}{q^{d/2-s-1} d^s}. \tag{7.29}$$

Estamos en condiciones de estudiar el valor absoluto de $\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d q$. En (7.17) expresamos esta diferencia como la suma de dos términos. El primero de ellos, $A(d,s)$, se estima en (7.18). El valor absoluto de $B(d,s)$ del segundo de ellos se acota en (7.29). Por lo tanto, combinando (7.18) y (7.29) obtenemos el siguiente resultado.

Teorema 7.5.2. *Con las hipótesis del Teorema 7.5.1, se verifica*

$$\left|\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d q - \frac{1}{2e}\right| \leq \frac{7}{q} + \frac{1+s^2}{2(d-s-1)!} + \frac{4\, e^{2d}}{q^{d/2-s-1} d^s}. \tag{7.30}$$

La estimación (7.30) es válida para valores grandes de q, mientras que la estimación del Teorema 7.4.4 es válida para todo q. Asimismo, la estimación (7.30) mejora notablemente la del Teorema 7.4.4 para valores de s pequeños. De hecho, (7.30) es ampliamente mejor que la estimación del Teorema 7.4.4 si $s \leq d/2-3$. Se puede ver que si $s \leq d/2-1$, entonces el lado derecho de (7.30) es menor a 1 para $d \geq 103$, mientras que, si $s \leq d/2-3$, el lado derecho de (7.30) es menor a 1 para $d \geq 8$. En tal sentido, vemos que (7.30) complementa la estimación del Teorema 7.4.4. Más aún, si (7.30) no nos proporciona mejores resultados, esto es debido a que creemos que las cotas para los correspondientes números de Betti no son lo suficientemente precisas.

Bibliografía

[AR10] Y. Aubry y F. Rodier, *Differentially 4-uniform functions*, in "Arithmetic, geometry, cryptography and coding theory 2009", Contemp. Math., vol. 521, Amer. Math. Soc., Providence, RI, 2010, 1–8.

[AS88] A. Adolphson y S. Sperber, *On the degree of the L-function associated with an exponential sum*, Compositio Math. **68** (1988), no. 2, 125–159.

[Bal03] E. Ballico, *An effective Bertini theorem over finite fields*, Adv. Geom. **3** (2003), no. 4, 361–363.

[BGH+10] B. Bank, M. Giusti, J. Heintz, M. Safey El Din y E. Schost, *On the geometry of polar varieties*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 1, 33–83.

[BGH+12] B. Bank, M. Giusti, J. Heintz, L. Lehmann y L. M. Pardo, *Algorithms of intrinsic complexity for point searching in compact real singular hypersurfaces*, Found. Comput. Math. **12** (2012), no. 1, 75–122.

[BGHM97] B. Bank, M. Giusti, J. Heintz y G. M. Mbakop, *Polar varieties, real equation solving, and data structures: the hypersurface case*, J. Complexity **13** (1997), no. 1, 5–27.

[BGHM01] _____, *Polar varieties and efficient real elimination*, Math. Z. **238** (2001), no. 1, 115–144.

[BGHP05] B. Bank, M. Giusti, J. Heintz y L. M. Pardo, *Generalized polar varieties: geometry and algorithms*, J. Complexity **21** (2005), no. 4, 377–412.

[BSD59] B. J. Birch y H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla*, Acta Arith. **5** (1959), 417–423.

[BV88] W. Bruns y U. Vetter, *Determinantal rings*, Lecture Notes in Mathematics, vol. 1327, Springer-Verlag, Berlin, 1988.

[Car55] L. Carlitz, *On the number of distinct values of a polynomial with coefficients in a finite field*, Proc. Japan Acad. **31** (1955), 119–120.

[CGH91] L. Caniglia, A. Galligo y J. Heintz, *Equations for the projective closure and effective Nullstellensatz*, Discrete Appl. Math. **33** (1991), no. 1-3, 11–23.

[CH04] R. Coulter y M. Henderson, *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc. **69** (2004), no. 3, 429–432.

[CLO98] D. Cox, J. Little y D. O'Shea, *Using algebraic geometry*, Graduate Texts in Mathematics, vol. 185, Springer-Verlag, New York, 1998.

[CM06] A. Cafure y G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. **12** (2006), no. 2, 155–185.

[CM07a] ———, *An effective Bertini theorem and the number of rational points of a normal complete intersection over a finite field*, Acta Arith. **130** (2007), no. 1, 19–35.

[CM07b] Q. Cheng y E. Murray, *On deciding deep holes of Reed-Solomon codes*, in "Theory and applications of models of computation", Lecture Notes in Comput. Sci., vol. 4484, Springer, Berlin, 2007, 296–305.

[CMP12] A. Cafure, G. Matera y M. Privitelli, *Singularities of symmetric hypersurfaces and Reed-Solomon codes*, Adv. Math. Commun. **6** (2012), no. 1, 69–94.

[CMP14] ———, *Polar varieties, Bertini's theorems and number of points of singular complete intersections over a finite field*, 2014, Disponible en arXiv:1209.4938.

[CMPP14] E. Cesaratto, G. Matera, M. Pérez y M. Privitelli, *On the value set of small families of polynomials over a finite field, I*, J. Combin. Theory Ser. A **124** (2014), 203–227.

[Coh72] S. D. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. (2) **6** (1972), 93–102.

[Coh73] S. D. Cohen, *The values of a polynomial over a finite field*, Glasgow Math. J. **14** (1973), 205–208.

[CU57] L. Carlitz y S. Uchiyama, *Bounds for exponential sums*, Duke Math. J. **24** (1957), 37–41.

[Dan94] V. I. Danilov, *Algebraic varieties and schemes*, Algebraic geometry, I, Encyclopaedia Math. Sci., vol. 23, Springer, Berlin, 1994, 167–297.

[Del74] P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.

[DGS06] J. Ding, J. E. Gower y D. Schmidt, *Multivariate public key cryptosystems*, Advances in Information Security, vol. 25, Springer, 2006.

[DKS13] C. D'Andrea, T. Krick y M. Sombra, *Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze*, Ann. Sci. Éc. Norm. Supér. (4) **46** (2013), no. 4, 549–627.

[Eis95] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.

[ELX09] F. A. B. Edoukou, S. Ling y C. Xing, *Intersection of two quadrics with no common hyperplane in* $\mathbb{P}^n(\mathbb{F}_q)$, 2009, Disponible en arXiv:0907.4556.

[Ern00] T. Ernst, *Generalized Vandermonde determinants*, Report 2000:6 Matematiska Institutionen, Uppsala Universitet, 2000, Disponible en http://www2.math.uu.se/research/pub/Ernst1.pdf.

[FHJ94] M. D. Fried, D. Haran y M. Jarden, *Effective counting of the points of definable sets over finite fields*, Israel J. Math. **85** (1994), no. 1-3, 103–133.

[FS65] D. K. Faddeev y I. S. Sominskii, *Problems in higher algebra*, W. H. Freeman and Co., San Francisco-London, 1965.

[FS09] P. Flajolet y R. Sedgewick, *Analytic combinatorics*, Cambridge University Press, Cambridge, 2009.

[Ful84] W. Fulton, *Intersection theory*, Springer-Verlag, Berlin, 1984.

[GHP99] S. Gao, J. Howell y D. Panario, *Irreducible polynomials of given forms*, Contemp. Math. **255** (1999), 43–53.

[GKP89] R. L. Graham, D. E. Knuth y O. Patashnik, *Concrete mathematics*, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1989.

[GL02a] S. R. Ghorpade y G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, Mosc. Math. J. **2** (2002), no. 3, 589–631.

[GL02b] ———, *Number of solutions of equations over finite fields and a conjecture of Lang and Weil*, Number theory and discrete mathematics (Chandigarh, 2000), Trends Math., Birkhäuser, Basel, 2002, 269–291.

[GS99] V. Guruswami y M. Sudan, *Improved decoding of Reed-Solomon and algebraic-geometry codes*, IEEE Trans. Inform. Theory **45** (1999), no. 6, 1757–1767.

[GV05] V. Guruswami y A. Vardy, *Maximum-likelihood decoding of Reed-Solomon codes is NP-hard*, IEEE Trans. Inform. Theory **51** (2005), no. 7, 2249–2256.

[Har92] J. Harris, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 133, Springer-Verlag, New York, 1992.

[Hei83] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), no. 3, 239–277.

[HLT05] E. W. Howe, K. E. Lauter y J. Top, *Pointless curves of genus three and four*, Arithmetic, geometry and coding theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, 125–141.

[Hoo91] C. Hooley, *On the number of points on a complete intersection over a finite field*, J. Number Theory **38** (1991), no. 3, 338–358.

[HP94a] W. V. D. Hodge y D. Pedoe, *Methods of algebraic geometry. Vol. I*, Cambridge Math. Lib., Cambridge Univ. Press, Cambridge, 1994.

[HP94b] ———, *Methods of algebraic geometry. Vol. II*, Cambridge Math. Lib., Cambridge Univ. Press, Cambridge, 1994.

[HP03] W. C. Huffman y V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[HS82] J. Heintz y C.-P. Schnorr, *Testing polynomials which are easy to compute*, Logic and algorithmic (Zurich, 1980), Monograph. Enseign. Math., vol. 30, Univ. Genève, Geneva, 1982, 237–254.

[Kat01] N. M. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. **7** (2001), no. 1, 29–44.

[Kle74] S. L. Kleiman, *The transversality of a general translate*, Compositio Math. **28** (1974), 287–297.

[Kle77] ———, *The enumerative theory of singularities*, Real and complex singularities Proc. Ninth Nordic Summer School/NAVF Sympos. Math., Oslo, 1976, Sijthoff and Noordhoff, 1977, 297–396.

[Kun85] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser Boston, Inc., Boston, MA, 1985.

[LN83] R. Lidl y H. Niederreiter, *Finite fields*, vol. 20, Addison-Wesley, Reading, MA, 1983.

[LP02] A. Lascoux y P. Pragacz, *Jacobians of symmetric polynomials*, Ann. Comb. **6** (2002), no. 2, 169–172.

[LW54] S. Lang y A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

[LW08a] J. Li y D. Wan, *On the subset sum problem over finite fields*, Finite Fields Appl. **14** (2008), no. 4, 911–929.

[LW08b] Y. Li y D. Wan, *On error distance of Reed-Solomon codes*, Sci. China Ser. A **51** (2008), no. 11, 1982–1988.

[Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[Nyb94] K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993), Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, 55–64.

[Pie78] R. Piene, *Polar classes of singular varieties*, Ann. Sci. École Norm. Sup. (4) **11** (1978), no. 2, 247–276.

[Rém01] G. Rémond, *Élimination multihomogène*, Introduction to algebraic independence theory, Lecture Notes in Math., vol. 1752, Springer, Berlin, 2001, 53–81.

[Rod09] F. Rodier, *Borne sur le degré des polynômes presque parfaitement nonlinéaires*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 487, Amer. Math. Soc., Providence, RI, 2009, 169–181.

[Sam67] P. Samuel, *Méthodes d'algèbre abstraite en géométrie algébrique*, Seconde édition, corrigée. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 4, Springer-Verlag, Berlin-New York, 1967.

[Sch74] W. M. Schmidt, *A lower bound for the number of solutions of equations over finite fields*, J. Number Theory **6** (1974), 448–480.

[Sch76] ———, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin-New York, 1976.

[Ser91] J.-P. Serre, *Lettre à M. Tsfasman*, Astérisque **198-200** (1991), 11, 351–353 (1992).

[Sha94] I. R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994.

[Sud97] M. Sudan, *Decoding of Reed Solomon codes beyond the error-correction bound*, J. Complexity **13** (1997), no. 1, 180–193.

[Tei82] B. Teissier, *Variétés polaires. II. Multiplicités polaires, sections planes, et conditions de Whitney*, Algebraic geometry (La Rábida, 1981), Lecture Notes in Math., vol. 961, Springer, Berlin, 1982, 314–491.

[Tei88] ———, *Quelques points de l'histoire des variétés polaires, de Poncelet à nos jours*, Séminaire d'Analyse, 1987–1988 (Clermont-Ferrand), vol 4, Univ. Blaise-Pascal, 1988.

[Uch54] S. Uchiyama, *Sur le nombre des valeurs distinctes d'un polynôme à coefficients dans un corps fini*, Proc. Japan Acad. **30** (1954), 930–933.

[Uch55a] ———, *Note on the mean value of $V(f)$*, Proc. Japan Acad. **31** (1955), 199–201.

[Uch55b] ———, *Note on the mean value of $V(f)$. II*, Proc. Japan Acad. **31** (1955), 321–323.

[Uch56] ———, *Note on the mean value of $V(f)$. III*, Proc. Japan Acad. **32** (1956), 97–98.

[Vog84] W. Vogel, *Lectures on results on Bezout's theorem*, Tata Ins. Fundam Res. Lect. Math., vol. 74, Tata Inst. Fundam. Res., Bombay, 1984.

[vzGVZ13] J. von zur Gathen, A. Viola y K. Ziegler, *Counting reducible, powerful, and relatively irreducible multivariate polynomials over finite fields*, SIAM J. Discrete Math. **27** (2013), no. 2, 855–891.

[Wan08] D. Wan, *Algorithmic theory of zeta functions over finite fields*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, 551–578.

[WH12] R. Wu y S. Hong, *On deep holes of standard Reed-Solomon codes*, Sci. China Math. **55** (2012), no. 12, 2447–2455.

[Woo08] T. D. Wooley, *Artin's conjecture for septic and unidecic forms*, Acta Arith. **133** (2008), no. 1, 25–35.

[Yek07] S. Yekhanin, *A note on plane pointless curves*, Finite Fields Appl. **13** (2007), no. 2, 418–422.

[Zah10] J. Zahid, *Non-singular points on hypersurfaces over $\mathbb{F}_q$*, J. Math. Sci **171** (2010), no. 6, 731–735.

[ZFL12] J. Zhang, F.-W. Fu y Q.-Y. Liao, *New deep holes of generalized Reed-Solomon codes*, 2012, Disponible en arXiv:1205.6593.