UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

Puntos racionales en variedades sobre cuerpos finitos. Estimaciones, Algoritmos y aplicaciones

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

Antonio Artemio Cafure

Director de Tesis: Guillermo Matera

Buenos Aires, Julio de 2006

Título: Puntos racionales en variedades sobre cuerpos finitos. Estimaciones, algoritmos y aplicaciones.

Resumen: Dada una variedad algebraica V definida sobre un cuerpo finito $\mathbb{F}_q$ consideramos el conjunto de puntos q–racionales $V(\mathbb{F}_q)$ de V. Tratamos dos problemas que surgen a partir de tal consideración: estimar el cardinal de $V(\mathbb{F}_q)$ y encontrar un elemento de $V(\mathbb{F}_q)$. El abordaje de estos problemas se sostiene en la utilización de métodos de teoría de eliminación efectiva y versiones efectivas de los Teoremas de Bertini. Estimamos la cantidad $V(\mathbb{F}_q)$ de puntos q–racionales en el caso en que V es una variedad absolutamente irreducible. Las estimaciones se expresan en términos de parámetros intrínsecos asociados a la variedad V, principalmente el grado. Damos un algoritmo para encontrar un punto de $V(\mathbb{F}_q)$ cuando V es absolutamente irreducible y está definida por una sucesión regular reducida. Su complejidad en tiempo es grosso–modo cuadrática en el logaritmo de q y un invariante geométrico del sistema de entrada. Este invariante, denominado el grado del sistema, está acotado por el número de Bézout del sistema. El algoritmo funciona para cuerpos de cualquier característica, pero requiere que q sea mayor que el grado de la variedad a la cuarta.

2000 Mathematics Subject Classification. Primaria 11G25, 14G05, 68W30; Secundaria 11G20, 13P05, 68Q10, 68Q25

Palabras clave: Variedades sobre cuerpos finitos, puntos racionales, solución geométrica, straight–line programs, algoritmos probabilísticos, Teoremas de Bertini, teoría de eliminación efectiva.

Title: Rational points in varieties over finite fields. Estimates, algorithms and applications.

Abstract: For a given variety V defined over a finite field we consider the set of q–rational points $V(\mathbb{F}_q)$ of V. We consider two different problems arising form this consideration: estimating the cardinality of $V(\mathbb{F}_q)$ and finding an element of $V(\mathbb{F}_q)$. Our approach rely on methods of effective elimination theory and effective versions of the Bertini theorems. We estimate the number of q–rational points $V(\mathbb{F}_q)$ when V is absolutely irreducible. Our estimates are expressed in terms of intrinsic parameters of V, mainly the degree of V. We also exhibit a probabilistic algorithm which computes a rational point of an absolutely irreducible variety over a finite field defined by a reduced regular sequence. Its time–space complexity is roughly quadratic in the logarithm of the cardinality of the field and a geometric invariant of the input system. This invariant, called the degree, is bounded by the Bézout number of the system. Our algorithm works for fields of any characteristic, but requires the cardinality of the field to be greater than a quantity which is roughly the fourth power of the degree of the input variety.

2000 Mathematics Subject Classification. Primary 11G25, 14G05, 68W30; Secondary 11G20, 13P05, 68Q10, 68Q25

Keywords and phrases: Varieties over finite fields, rational points, geometric solutions, straight–line programs, probabilistic algorithms, Bertini theorems.

A la memoria de Anatoli Czuchlej

1933-2006

No sé si mi canto es lindo
o si saldrá medio triste
nunca juí zorzal ni esiste
plumaje mas ordinario
yo soy pájaro corsario
que no conoce el alpiste.

Yo soy de los del montón
no soy flor de invernadero
soy como el trébol campero
crezco sin hacer barullo
me aprieto contra los yuyos
y así lo aguanto al Pampero.

De seguro si uno piensa
le halla el nudo a la madeja
porque la copla más vieja
como la raíz de la vida
tiene al alma por guarida
que es ande anidan las quejas.

Por eso el hombre al cantar
con emoción verdadera
echa su pena pa'afuera
pa'que la lleven los vientos
y ansí siquiera un momento
se alivia su embichadera.

No es que no ame a su trova
ni que desprecee su canto
es como cuando un quebranto
en la noche de los llanos
hace aflojar al paisano
y el viento le lleva el canto.

En asuntos del cantar
la vida nos va enseñando
que sólo se va volando
la copla que es livianita
siempre caza palomitas
cualquiera que anda cazando.

Fragmentos de *El payador perseguido*
de Atahualpa Yupanqui

Debería agradecerle a Guillermo Matera, mi director, «por el apoyo recibido, por la paciencia, ... que hizo posible que ... » y todas esas expresiones tan remanidas (enunciarlas, en sí, no encierra nada malo). Solamente voy a decir que, haber llegado a esta instancia y ser su primer alumno es una suerte de justicia poética.

A Mariano, mi hermano de la vida. A Tico y a Ezequiel Dratman, el hombre–alambre, mis hermanos de estos últimos años.

Al gran Joos Heintz. Por el ejemplo.

A Pablo Solernó. Porque aprendí de sus clases; por la paciencia y buena predisposición para responder mis preguntas.

A Luis Miguel Pardo por las conversaciones, por el estímulo, por las observaciones.

A Ariel Waissbein con quien hemos trabajado y aprendido.

A Juan Sabia, Teresa Krick, Gabriela Jerónimo y Daniel Perrucci, por haber contribuido de alguna u otra forma a entender algunas cosas.

Agradezco a Alicia Dickenstein, a Joachim von zur Gathen y a Roberto Miatello, por haber aceptado ser jurados.

Un agradecimiento a Gabriel Larotonda, quien me facilitó el formato de la tesis.

A todos aquellos, que no voy a mencionar para no olvidarme de ninguno, que han hecho más divertida la vida en la facultad.

A Antonio Cafure y María Scheiner, mis viejos, por la dignidad infinita; por lo que significa que el hijo de un obrero (con más de 40 años de fábrica) pueda hacer algo en Exactas. A Ahmed, mi hermano y a mi sobrino Estanislao.

A CRISTINA, por el amor, por la paciencia, por permitirme ser Nino. Y al pequeño FELIPE, que ha llegado hace poco y nos está enseñando una nueva dimensión de la felicidad.

Índice general

1 Introducción

> *Every field has its taboos. In algebraic geometry the taboos are (1) writing a draft that can be followed by anyone but two or three of one's closest friends, (2) claiming that a result has applications, (3) mentioning the word "combinatorial", and (4) claiming that algebraic geometry existed before Grothendieck (only some handwaving references to "the Italians" are allowed provided they are not supported by specific references).* Gian–Carlo Rota, Indiscrete Thoughts, *1997*.

Consideremos una variedad algebraica afín o proyectiva V definida sobre un cuerpo finito $\mathbb{F}_q$: V es el conjunto de ceros comunes (en la clausura algebraica $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$) de una familia de polinomios (homogéneos en el caso proyectivo) con coeficientes en $\mathbb{F}_q$. Decimos entonces que V es una $\mathbb{F}_q$–variedad. El conjunto de puntos de V con coordenadas en $\mathbb{F}_q$ es lo que denominaremos el conjunto de puntos q–racionales de V y denotaremos por $V(\mathbb{F}_q)$.

En este trabajo nos proponemos dar cuenta, esencialmente, de los siguientes problemas

1. Obtener estimaciones y resultados de existencia sobre el número $|V(\mathbb{F}_q)|$ de puntos q–racionales de una $\mathbb{F}_q$–variedad V.

2. Desarrollar algoritmos efectivos para calcular un elemento de $V(\mathbb{F}_q)$.

Como una consecuencia natural de los dos puntos anteriores vamos a incursionar también en un aspecto, digamos, aplicado:

3. Estudiar aplicaciones a problemas concretos vinculados a la criptografía.

Sin pretensiones de exhaustividad pasamos, a continuación, a describir la historia y el estado actual de la matemática involucrada en estos problemas.

1.1. Antecedentes

1.1.1. Estimaciones y resultados de existencia

La cuestión de contar de manera exacta, de estimar, de garantizar la existencia o de encontrar puntos q–racionales de una variedad V, es un tema clásico de la geometría aritmética; sus orígenes se pueden rastrear en los intentos de Gauss y Jacobi por estudiar

ciertos tipos de congruencias, y ha ocupado, entre otros, a Hardy, Littlewood, Chevalley, Davenport, Mordell, Hasse, Weil, Lang, Dwork y Deligne.

En 1948, André Weil [Wei48] demuestra lo que se ha dado en llamar la «Hipótesis de Riemann sobre cuerpos finitos» (había anunciado este resultado en 1940) que podemos enunciar del modo siguiente: si $C \subset \mathbb{P}^2$ es una curva no singular absolutamente irreducible de grado δ y género g definida sobre $\mathbb{F}_q$, el número $|C(\mathbb{F}_q)|$ de puntos q–racionales de la curva C verifica la estimación

$$\left||C(\mathbb{F}_q)| - (q+1)\right| \leq 2gq^{1/2}. \tag{1.1}$$

Esta estimación también se conoce como estimación de Hasse–Weil, pues Helmut Hasse demostró en los años 30 el resultado para curvas de género 1. Al año siguiente, Weil [Wei49] formula una serie de conjeturas acerca de la función zeta de cualquier variedad proyectiva no singular y sugiere el desarrollo de una teoría de cohomología adecuada para emprender la tarea de demostrar dichas conjeturas.

Si tomamos en cuenta la desigualdad $2g \leq (\delta-1)(\delta-2)$, obtenemos el equivalente a (1.1) en el caso afín:

$$\left||C(\mathbb{F}_q)| - q\right| \leq (\delta-1)(\delta-2)q^{1/2} + \delta + 1. \tag{1.2}$$

En 1954, Serge Lang y Weil [LW54] establecen un "prototipo" de estimación sobre el número de puntos q–racionales de $\mathbb{F}_q$–variedades absolutamente irreducibles. Demuestran que si $V \subset \mathbb{P}^n$ es una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ, el número de puntos q–racionales $|V(\mathbb{F}_q)|$ verifica la siguiente estimación:

$$\left||V(\mathbb{F}_q)| - p_r\right| \leq (\delta-1)(\delta-2)\, q^{r-1/2} + C(n,r,\delta)\, q^{r-1}, \tag{1.3}$$

donde $p_r := q^r + q^{r-1} + \cdots + q + 1$ y $C(n,r,\delta)$ es una constante independiente de q y no explícita, en el sentido siguiente: si bien se sabía que la constante $C(n,r,\delta)$ dependía de los parámetros señalados, no se proporcionaba ninguna cota superior sobre el valor de la misma. Interpretando esta estimación en términos afines tenemos 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 $|V(\mathbb{F}_q)|$ de V verifica la estimación:

$$\left||V(\mathbb{F}_q)| - q^r\right| \leq (\delta-1)(\delta-2)q^{r-1/2} + C(n,r,\delta)q^{r-1}. \tag{1.4}$$

Hacia fines de la década del 60 Serguei Stepanov sorprende a la comunidad de Teoría de números al presentar una demostración de las conjeturas de Weil para curvas utilizando métodos elementales: una combinación de argumentos combinatorios con un análisis detallado de ciertas extensiones de cuerpos de funciones en característica positiva. Una sorpresa semejante tuvo lugar en 1960 cuando Bernard Dwork [Dwo60] demuestra la

racionalidad de la función zeta para cualquier variedad V, afín o proyectiva, no singular y singular, sin seguir el camino trazado por Weil sino perfeccionando herramientas y métodos de análisis p–ádico.

Si bien se habían demostrado algunas de las conjeturas de Weil hacia fines de los 60, el estado de las estimaciones hacia 1973 no permitía aún obtener estimaciones explícitas para la constante $C(n,r,\delta)$ involucrada en la estimación (1.3), según nos informa Jean–René Joly en [Jol73, Pag. 89].

En una serie de trabajos de principos de los 70, Wolfgang Schmidt, continuando con el trabajo de Stepanov, comienza a proporcionar estimaciones y resultados de existencia sobre la cantidad de puntos q–racionales de diferentes variedades. En un trabajo de 1974 [Sch74] proporciona una cota inferior no trivial (y por ende un resultado de existencia) sobre el número de puntos q–racionales $|H(\mathbb{F}_q)|$ de una hipersuperficie H absolutamente irreducible de grado δ:

$$|H(\mathbb{F}_q)| > q^{n-1} - (\delta-1)(\delta-2)q^{n-3/2} - (5\delta^2+\delta+1)q^{n-2}, \tag{1.5}$$

asumiendo que $q > 10^4 n^3 \delta^5 P^3([4\log\delta])$ donde $P(u)$ es el u–ésimo primo (esta imposición sobre el cardinal del cuerpo finito es lo que denominaremos «regularidad»). Sin embargo, no provee la correspondiente cota superior. Posteriormente, en [Sch76] (un texto que podríamos considerar un clásico) obtiene la siguiente estimación explícita:

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

con $\theta := (\delta+1)\delta/2$. Lo relevante de la estimación estriba no en el término de error (doblemente exponencial) sino en el método propuesto y en el hecho de que se obtiene, por primera vez, una estimación explícita válida para cualquier $\mathbb{F}_q$–hipersuperficie absolutamente irreducible. De ahí en adelante, estos resultados de Schmidt se erigieron en referencias ineludibles para todos aquellos que trataran este u otros problemas vinculados. Al mismo tiempo, la cota inferior y la condición de regularidad bajo la cual ésta es válida no han sido mejoradas desde entonces. El método que desarrolla Schmidt para obtener la estimación se basa en estimar la cantidad de puntos q–racionales en la intersección de la $\mathbb{F}_q$–hipersuperficie absolutamente irreducible H con una $\mathbb{F}_q$–variedad lineal genérica de dimensión 2. Es decir, estima la cantidad de puntos q–racionales de una curva. Para eso, cuenta con que, genéricamente, la curva que se obtiene es absolutamente irreducible y por lo tanto puede aplicar la estimación de Hasse-Weil. Lo interesante de su trabajo es que obtiene estimaciones sobre la cantidad de intersecciones (curvas) que no resultan ser absolutamente irreducibles. Esto es lo que hoy denominaríamos una versión efectiva del primer Teorema de Bertini.

En 1998, combinando (1.5) con el método de Schmidt [Sch76] y la versión efectiva del primer Teorema de Bertini debida a Erich Kaltofen [Kal95], Ming-Deh Huang y

Yiu-Chung Wong [HW98] obtienen:

$$\left||H(\mathbb{F}_q)|-q^{n-1}\right| \leq (\delta-1)(\delta-2)q^{n-3/2}+(\delta^2+2\delta^5)q^{n-2}+2\delta^7 q^{n-5/2}, \tag{1.6}$$

bajo la misma condición de regularidad de (1.5).

Finalmente, Sudhir Ghorpade y Gilles Lachaud ([GL02b], [GL02a]) encuentran un valor explícito para la constante C de (1.4). Más precisamente, en [GL02a, Remark 11.3] (ver también [GL02b, Theorem 4.1]) se muestra la siguiente estimación:

$$\left||V(\mathbb{F}_q)|-q^r\right| \leq (\delta-1)(\delta-2)q^{r-1/2}+6\cdot 2^s(sd+3)^{n+1}q^{r-1}, \tag{1.7}$$

donde s es el número de ecuaciones que definen V, y d es el máximo de los grados de las mismas. En el caso de una hipersuperficie H, la estimación (1.7) toma la forma

$$\left||H(\mathbb{F}_q)|-q^{n-1}\right| \leq (\delta-1)(\delta-2)q^{n-3/2}+12(\delta+3)^{n+1}q^{n-2}. \tag{1.8}$$

La demostración de este resultado sigue un método basado en una generalización del Teorema débil de Lefschetz a variedades singulares y estimaciones de los números de Betti de unos espacios de cohomología étale ℓ–ádica.

La descripción anterior es, a grandes rasgos, la situación en términos de estimaciones generalistas. Por estimaciones generalistas entendemos estimaciones que no consideran cualidades particulares de las variedades con las que se tratan.

No es descabellado imaginar que ante la presencia de alguna característica particular de la variedad en cuestión (no singular, intersección completa, normal, etc) podamos obtener mejores estimaciones y resultados de existencia. Desde esta perspectiva, existen resultados de conteo bajo hipótesis más restrictivas sobre la geometría de las variedades en consideración. Un resultado clásico en tal sentido es la conocida estimación para variedades absolutamente irreducibles no singulares sobre cuerpos finitos de Pierre Deligne [Del74] –su trabajo representó la culminación del programa iniciado por Weil– que expresa que el número de puntos q–racionales $|V(\mathbb{F}_q)|$ de una intersección completa $V \subset \mathbb{P}^n$ no singular de dimensión r y multigrado $\mathbf{d}$ satisface la estimación:

$$\left||V(\mathbb{F}_q)|-p_r\right| \leq b'_r(n,\mathbf{d})q^{r/2}, \tag{1.9}$$

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

Posteriormente, en un trabajo de 1991, Christopher Hooley [Hoo91] extiende en forma no efectiva la estimación (1.9) a intersecciones completas arbitrarias. Si $V \subset \mathbb{P}^n$ es una $\mathbb{F}_q$–variedad intersección completa de dimensión r y dimensión de singularidades m, entonces la cantidad de puntos q–racionales de V verifica la siguiente estimación:

$$\left||V(\mathbb{F}_q)|-p_r\right| = O(q^{(r+m+1)/2}). \tag{1.10}$$

La constante involucrada en la estimación, si bien independiente de q, no es explícita. La demostración proporcionada por Hooley (1.10) consiste en considerar sucesivas secciones por hiperplanos de V hasta que se obtiene una sección no singular. El número de puntos q–racionales de estas secciones no singulares se estima aplicando (1.9). Notemos la familiaridad con el método de Schmidt.

Al respecto, cabe mencionar que en los trabajos de Ghorpade y Lachaud se han obtenido versiones efectivas de dichas estimaciones, utilizando las herramientas cohomológicas mencionadas anteriormente. En [GL02b], [GL02a] obtienen una versión explícita de (1.10). Si V se define con $s := n-r$ ecuaciones de multigrado $\mathbf{d} := (d_1, \ldots, d_s)$ y $d := \max_{1 \leq i \leq s} d_i$, entonces

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_{r-m-1}(n-m-1, \mathbf{d})\, q^{(r+m+1)/2} + C_m(V)\, q^{(r+m)/2}. \tag{1.11}$$

La constante $C_m(V)$ puede acotarse por $9 \cdot 2^s \cdot (sd+3)^{n+1}$ y $b'_{r-m-1}(n-m-1, \mathbf{d})$ es el $(r-m-1)$–ésimo número de Betti primitivo de una intersección completa no singular en $\mathbb{P}^{n-m-1}$ de dimensión $r-m-1$ y multigrado $\mathbf{d}$. Observemos que si $m = -1$, en otras palabras, si V es no singular, (1.11) no es más que la estimación de Deligne (1.9).

Supongamos que $V \subset \mathbb{P}^n$ es una $\mathbb{F}_q$–variedad normal e intersección completa de dimensión r, grado δ y multigrado $\mathbf{d} := (d_1, \ldots, d_{n-r})$. Entonces la dimensión de singularidades de V puede acotarse por $r-2$ y por lo tanto (1.11) toma la forma

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_1(n-r+1, \mathbf{d}) q^{r-\frac{1}{2}} + 9 \cdot 2^{n-r}\big((n-r)d+3\big)^{n+1} q^{r-1}. \tag{1.12}$$

El número de Betti $b'_1(n-r+1, \mathbf{d})$ es menor o igual que $(\delta-1)(\delta-2)$, y la igualdad es válida si y solo si V es una hipersuperficie; concluimos que esta estimación mejora la estimación de Lang–Weil (1.3) y su versión explícita en [GL02b], [GL02a].

Señalemos finalmente, que una cantidad de aplicaciones hacen uso de estimaciones explícitas sobre el valor de la constante $C := C(n, r, \delta)$ (ver e.g., [HW99], [Kna01], [Rag02], [Bog05], entre otros). Más aún, para algunas familias particulares de variedades se han proporcionado mejores estimaciones (ver e.g., [SS90], [Sko92], [Luo99]).

1.1.2. Búsqueda de puntos q–racionales

La resolución de sistemas de ecuaciones polinomiales sobre cuerpos finitos es un problema NP–completo aun si las ecuaciones son cuadráticas y están definidas sobre $\mathbb{F}_2$ ([GJ79]). Más aún, [vzGKS97] muestra que determinar el número de puntos q–racionales de una curva plana rala (sparse) sobre un cuerpo finito $\mathbb{F}_q$ es # P–completo. La ausencia de algoritmos eficientes para hallar puntos racionales en variedades algebraicas sobre cuerpos finitos es un hecho reconocido en el ámbito del cálculo simbólico. De hecho, esta carencia ha propiciado el surgimiento de diversos esquemas criptográficos de clave

pública basados en la dificultad de la resolución de sistemas de ecuaciones polinomiales sobre cuerpos finitos [IM88], [CKPS00].

Podríamos decir, entonces, en lo que atañe a la búsqueda efectiva de soluciones de estos sistemas, que no existe demasiada literatura sobre el tema, si bien se han tratado casos particulares. Por ejemplo, en el paper [vzGSS03] se exhibe un algoritmo determinístico que calcula todos los puntos de una curva plana definida sobre $\mathbb{F}_p$, el cuerpo primo de característica p. La complejidad del mismo es de $O(\delta^5 p)$ operaciones sobre $\mathbb{F}_p$, donde δ es el grado del polinomio libre de cuadrados que define la curva. Por otro lado, los trabajos de [KS99], [CKPS00] y [BFS03] exhiben algoritmos que resuelven un sistema sobredeterminado de ecuaciones cuadráticas sobre un cuerpo finito sobre la base de técnicas de «linealización».

Los algoritmos de búsqueda de puntos racionales en una variedad general sobre un cuerpo finito se basan generalmente en técnicas de reescritura (ver por ejemplo [CLO92, CLO98]). Desafortunadamente, tales algoritmos tienen complejidad superexponencial, hecho que los hace absolutamente inadecuados para tratar con los problemas que suelen aparecer en la práctica. De hecho, sus variantes más eficientes (véase por ejemplo [Fau02]) tienen una complejidad del peor caso superior a la de la búsqueda exhaustiva para sistemas de ecuaciones polinomiales sobre $\mathbb{F}_2$ [CKPS00].

Un enfoque diferente se propone en [HW99]. Allí, el sistema polinomial en consideración se trata mediante deformaciones, basadas en una perturbación del sistema original seguido de un método de «seguimiento de las curvas» (path-following). Sin embargo, la perturbación, generalmente, introduce soluciones espurias que resultan computacionalmente difíciles de identificar y eliminar a efectos de obtener las verdaderas soluciones. De hecho, el algoritmo de Huang-Wong es algebraicamente robusto o universal en el sentido de [HMPW98] y [CGH$^+$03], lo cual implica en particular que su complejidad en tiempo es al menos exponencial.

1.2. Supuestos básicos

Independientemente del problema concreto con el cual tratemos a lo largo de la tesis (estimaciones o algoritmos), y de las herramientas particulares con las que estos problemas sean resueltos, nuestros métodos consisten, esencialmente, en desarrollar versiones efectivas de los teoremas de Bertini y utilizar herramientas de teoría de eliminación tales como las formas de Chow.

Usualmente, las estimaciones, los resultados de existencia de puntos racionales en variedades de dimensión arbitraria y la complejidad de los algoritmos de búsqueda de puntos racionales, se expresan en términos del número de Bézout (el producto de los grados de las ecuaciones) del sistema en consideración (véase e.g., [GL02a], [GL02b] y [HW99]). Así, las estimaciones y los resultados de existencia pueden resultar en sobres-

timaciones de tipo exponenciales, como puede apreciarse comparando los resultados de Ghorpade–Lachaud y de Schmidt. Nuestra propuesta para las estimaciones y los resultados de existencia es que dependan del grado de la variedad en consideración. Así, las cotas permiten diferenciar las variedades de acuerdo a parámetros geométricos que, en los casos «geométricamente bien condicionados» (léase casos de grado bajo), resultan exponencialmente mejores que las cotas existentes.

Para acometer la faceta algorítmica de nuestro trabajo, vamos a considerar, como punto de partida, algoritmos de eliminación para la resolución de sistemas sobre los números reales o complejos, cuya principal característica es que distinguen entradas de acuerdo a consideraciones geométricas. Estos algoritmos desarrollados a lo largo de los trabajos [GHMP95], [Par95], [GHM$^+$98], [GHH$^+$97], [GHMP97], [BGHM97], [BGHM01], [BGHP04], [BGHP05] (ver también [HMW01], [GLS01], [Lec03], [Sch03], [PS04]), podrían considerarse como parte de una nueva generación de algoritmos para la resolución de sistemas de ecuaciones polinomiales.

El punto clave es que la variedad algebraica original se reemplaza por una hipersuperficie birracionalmente equivalente contenida en un espacio ambiente adecuado. Esta hipersuperficie y su polinomio minimal pueden producirse mediante proyecciones lineales genéricas. La ecuación minimal posee la información necesaria sobre la dimensión y el grado de la variedad original y sobre un conjunto de variables independientes, que permite despejar (desacoplar) las restantes variables en función de las independientes. Con esta idea, todos los resultados intermedios que aparecen en dichos algoritmos son formas eliminantes y describen proyecciones de variedades algebraicas relacionadas con el sistema de entrada. Por lo tanto, el tamaño de los resultados intermedios se controla a partir de consideraciones geométricas. La complejidad en tiempo resultante de estos procedimientos de eliminación es finalmente polinomial en todos los parámetros que miden su comportamiento: los parámetros extrínsecos (número de variables, el grado de la ecuaciones de entrada y la cantidad de operaciones aritméticas necesarias para evaluarlas) y un parámetro intrínseco: el grado del sistema de entrada (ver [GHH$^+$97] y [BGHM97]), que se define como el máximo de los grados de las variedades intermedias. En tanto las operaciones aritméticas básicas estén contadas sólo a costo unitario, esta descripción del carácter de la complejidad de estos algoritmos es casi óptimo.

Nuestra idea es, dentro de este marco, desarrollar algoritmos para resolver sistemas de ecuaciones polinomiales sobre cuerpos finitos, teniendo presente las particularidades del trabajo sobre los mismos. Nuestros resultados sobre estimaciones proporcionan condiciones para que esto pueda realizarse.

Por otro lado, todos los algoritmos de búsqueda de puntos racionales en variedades sobre cuerpos finitos conocidos poseen una característica particular, denominada robustez algebraica. Informalmente, un algoritmo se dice algebraicamente robusto si, teniendo como entrada una familia playa de problemas de eliminación, produce soluciones «es-

tables», es decir, soluciones que dependen del problema paramétrico en consideración, y no de la instancia paramétrica que la define. En [CGH$^+$03] se ha demostrado que todo algoritmo algebraicamente robusto requiere necesariamente tiempo exponencial de ejecución en el peor caso. De esta manera, concluimos que el objetivo de producir un algoritmo eficiente (polinomial) general para los procesos de eliminación geométrica no puede alcanzarse en forma evolutiva, es decir, construyendo mejoras sucesivas de los métodos conocidos. Esta conclusión no depende del tipo de algoritmos de eliminación considerado, ni de las representaciones (estructuras de datos) empleadas, sino más bien de la pretensión de universalidad con la que habitualmente se diseñan los algoritmos de eliminación. Teniendo en cuenta estos resultados, hemos reorientado la algorítmica correspondiente hacia una distinción de acuerdo a parámetros geométricos, como el «grado del sistema de entrada» que hemos mencionado más arriba y el grado de la variedad en consideración. Esta «adaptatividad» es el punto clave de los resultados que obtenemos en nuestro trabajo algorítmico: si bien es cierto que en el peor caso tiene complejidad de tipo exponencial (aunque siempre polinomial en el número de Bézout del sistema de entrada), nuestro algoritmo define una noción de «buen condicionamiento» (problemas bien condicionados son aquellos para los cuales el grado del sistema es polinomial) y resulta polinomial para esta clase de problemas.

1.3. Resultados obtenidos y organización del trabajo

Pasamos a describir como está organizado el trabajo y cuales son los resultados más importantes que hemos obtenido, los cuales se enuncian como **Teorema 1**, **Teorema 2**, etc.

El Capítulo 2 está destinado a presentar el vocabulario básico que utilizaremos. Se presentan allí las nociones, en cierto modo, transversales; principalmente, la noción de grado de una variedad. Destinamos una sección a introducir la forma de Chow de una variedad y enunciar algunas de sus propiedades. Esta noción revestirá de una importancia fundamental, ya sea desde las estimaciones como desde el aspecto algorítmico de nuestro trabajo.

En el Capítulo 3 comenzamos presentando algunas cotas superiores sobre la cantidad de puntos q–racionales de diferentes variedades afines o proyectivas. Aplicando la desigualdad de Bézout (2.1) de [Hei83] en lugar de los clásicos argumentos combinatorios, obtenemos cotas superiores que mejoran y generalizan algunos resultados clásicos, mediante el uso de argumentos simples de la teoría de intersección. Posteriormente, presentamos resultados clásicos sobre el número promedio de ceros de una hipersuperficie y discutimos cómo esto justifica el modo de obtener estimaciones para variedades cualesquiera. La última sección del capítulo discurre acerca de la noción de regularidad: condiciones sobre la cantidad de elementos que debe tener un cuerpo finito para que

ciertos hechos geométricos–algebraicos tengan lugar sobre dicho cuerpo finito.

Los métodos para obtener estimaciones sobre la cantidad de puntos q–racionales de una hipersuperficie H absolutamente irreducible de grado δ consisten en intersecar la hipersuperficie con variedades lineales de dimensión 2. En el caso genérico, la curva resultante es absolutamente irreducible y por lo tanto, puede aplicarse la estimación de Hasse–Weil. La cuestión radica, entonces, en llevar a cabo este proceso de manera efectiva y es aquí donde surge la necesidad de disponer de versiones efectivas del primer teorema de Bertini. Inspirados por el trabajo de Kaltofen [Kal95], abordamos este problema en forma algorítmica. A partir de un algoritmo que calcula los factores irreducibles de grado a lo sumo D de un polinomio bivariado de grado δ (ver la Sección 4.1), estimamos la cantidad de variedades lineales L de dimensión 2 tales que la curva intersección $H \cap L$ no tiene componentes absolutamente irreducibles de grado a lo sumo D. En suma, en nuestro método, tributario del método de Schmidt, reducimos eficientemente la estimación sobre la hipersuperficie a estimar sobre curvas. Este análisis cristaliza en el Teorema 4.3.2 que, a continuación, enunciamos.

Teorema 1 *Sea* $H \subset \mathbb{A}^n$ *una* $\mathbb{F}_q$*–hipersuperficie absolutamente irreducible de grado* δ*. Entonces es válida la siguiente estimación:*

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

Observemos que la estimación anterior mejora todas las estimaciones conocidas para $\mathbb{F}_q$–hipersuperficies absolutamente irreducibles y es válida sobre cualquier cuerpo finito $\mathbb{F}_q$.

En seguida, utilizando la cota inferior provista por la estimación anterior, obtenemos una estimación aún mejor pero con una condición de regularidad. Este resultado se presenta en el Teorema 4.3.3.

Teorema 2 *Sea* $H \subset \mathbb{A}^n$ *sea una* $\mathbb{F}_q$*–hipersuperficie absolutamente irreducible de grado* δ*. Si* $q > 15\delta^{\frac{13}{3}}$ *entonces*

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

La importancia de esta última estimación no radica solamente en que estamos en presencia de una estimación sensiblemente mejor que la anterior –ya que pasamos de $O(\delta^{13/3})$ a $O(\delta^2)$ en el segundo término de error, siempre y cuando $q > 15\delta^{\frac{13}{3}}$– sino que también, como consecuencia de ella, deducimos la misma cota inferior (no trivial) que la de Schmidt (1.5) pero con una condición de regularidad ostensiblemente menor, como puede apreciarse en el Corolario 4.3.4

Teorema 3 *Sea* $H \subset \mathbb{A}^n$ *una* $\mathbb{F}_q$*–hipersuperficie absolutamente irreducible de grado*

δ. *Si* $q > 15\delta^{13/3}$ *entonces*

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

Al mismo tiempo, en términos de resultados de existencia, mediante una aplicación directa de la versión efectiva del Primer Teorema de Bertini de Kaltofen (Corolario 4.1.2), probamos en forma muy simple (Teorema 4.3.5) que una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible de grado δ tiene un punto q–racional si $q > 2\delta^4$.

En el Capítulo 5 hacemos uso de la teoría de formas de Chow con el objeto de extender las estimaciones de hipersuperficies a variedades equidimensionales afines. En primer lugar, obtenemos una cota sobre el grado de la condición genérica que posibilita que una variedad afín equidimensional definida sobre un cuerpo arbitrario sea birracionalmente equivalente a una hipersuperficie. Conociendo dicho grado, traducimos convenientemente dicho resultado a un resultado que proporciona condiciones de regularidad bajo las cuales una $\mathbb{F}_q$–variedad equidimensional es birracionalmente equivalente a una $\mathbb{F}_q$–hipersuperficie mediante una proyección lineal definida sobre $\mathbb{F}_q$. Este es el contenido del Teorema 5.1.3, que enunciamos a continuación:

Teorema 4 *Sea* $V \subset \mathbb{A}^n$ *una* $\mathbb{F}_q$*–variedad equidimensional de dimensión* r *y grado* δ. *Si* $q > 2(r+1)\delta^2$ *existen formas lineales* $Y_1, \ldots, Y_{r+1} \in \mathbb{F}_q[X_1, \ldots, X_n]$ *tales que*

(i) *La extensión de anillos* $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$ *es una extensión entera.*

(ii) *La función coordenada inducida por* Y_{r+1} *en* $\overline{\mathbb{F}}_q[V]$ *es un elemento primitivo de la extensión de anillos* $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$.

(iii) $W := \overline{\pi(V)}$ *es una* $\mathbb{F}_q$*–hipersuperficie de grado* δ *birracionalmente equivalente a* V.

Este teorema –al cual retornaremos en ocasión del trabajo algorítmico– nos permite reducir el caso de una $\mathbb{F}_q$–variedad absolutamente irreducible al de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible. Utilizando las estimaciones del Capítulo 4, la construcción explícita del morfismo birracional dado por el **Teorema 4** y que, en el caso en que V es absolutamente irreducible, tenemos una condición de regularidad lineal en δ (cf. Teorema 5.1.4), llegamos a la siguiente estimación (Teorema 5.2.1):

Teorema 5 *Sea* $V \subset \mathbb{A}^n$ *una* $\mathbb{F}_q$*–variedad absolutamente irreducible de dimensión* r *y grado* δ. *Si* $q > r\delta$ *entonces:*

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

Es de observar que esta estimación mejora la estimación (1.7) en los casos de codimensión baja, por ejemplo $2r \geq n+1$ y grado de las ecuaciones bajo, por ejemplo $d \leq (n-r)$.

El contenido de los Capítulos 4 y 5 recién esbozado se presenta en el trabajo [CM06b].

Finalmente, como una consecuencia natural del trabajo anterior, en el Capítulo 6 establecemos mejores resultados de conteo y existencia bajo hipótesis más restrictivas sobre la geometría de las variedades en consideración; más precisamente, en el caso de una variedad proyectiva intersección completa normal. Como antes, vamos a requerir, en este caso, de una versión efectiva del Segundo Teorema de Bertini. El Teorema 6.2.3 representa una versión propia de tal resultado:

Teorema 6 *Sea $V \subset \mathbb{P}^n$ una variedad intersección completa normal de dimensión r y grado δ, y sea $\pi : V \to \mathbb{P}^{r-1}$ una proyección lineal genérica. Entonces existe una variedad $W \subset \mathbb{P}^{r-1}$ de grado a lo sumo $2(n-r)^2(d-1)^2\delta$ tal que la fibra $\pi^{-1}(y)$ es una curva no singular de grado acotado por δ para cada $y \notin W$.*

Así como el número de puntos q–racionales de una curva absolutamente irreducible se estima utilizando la estimación de Hasse–Weil, ahora, el número de puntos q–racionales de estas curvas no singulares e intersección completa se estima aplicando la estimación (1.9). Aplicando los resultados del Capítulo 5 obtenemos la siguiente estimación (Teorema 6.3.1):

Teorema 7 *Sea $V \subset \mathbb{P}^n$ una $\mathbb{F}_q$–variedad intersección completa normal de dimensión r, grado δ y multigrado $\mathbf{d}$. Si $q > 2(r+1)(n-r)(d-1)\delta$ es válida la siguiente estimación:*

$$\left| |V(\mathbb{F}_q)| - p_r \right| \leq b_1'(n-r+1, \mathbf{d}) q^{r-1/2} + 2(n-r)^2 d^2 \delta^2 q^{r-1},$$

donde $b_1'(n-r+1, \mathbf{d})$ denota el primer número de Betti de una curva intersección completa no singular en $\mathbb{P}^{n-r+1}$ de multigrado $\mathbf{d}$.

Como hemos señalado, esta nueva estimación, válida bajo la condición de regularidad $q > 2(r+1)(n-r)(d-1)\delta$, mejora claramente (1.12) en el caso de una hipersuperficie. De hecho, para una hipersuperficie (1.12) es

$$\left| |V(\mathbb{F}_q)| - p_{n-1} \right| \leq (\delta-1)(\delta-2) q^{n-3/2} + 18(\delta+3)^{n+1} q^{n-2}.$$

Esta estimación también mejora (1.12) en los casos de codimensión baja, por ejemplo $2r \geq n+1$ y grado de las ecuaciones bajo, por ejemplo $d \leq (n-r)$. Al mismo tiempo, mejoramos nuestra propia estimación generalista $C \leq 5\delta^{13/3}$ del **Teorema 5**.

La segunda parte de este trabajo concierne al aspecto algorítmico, es decir, a la búsqueda efectiva de soluciones q–racionales. En el trabajo [CM06a] se presenta por primera vez el algoritmo que vamos a desarrollar. Es un algoritmo probabilístico que calcula un punto q–racional de una $\mathbb{F}_q$–variedad afín absolutamente irreducible definida por una sucesión regular reducida. La complejidad de nuestro algoritmo es cuadrática en el logaritmo de la cantidad de elementos del cuerpo y un invariante geométrico del sistema

de entrada análogo al mencionado en característica cero, el "grado del sistema", siempre acotado por el número de Bézout del sistema.

Sea entonces V una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ definida por polinomios $F_1,\dots,F_{n-r} \in \mathbb{F}_q[X_1,\dots,X_n]$ de grado a lo sumo d, que forman una sucesión regular reducida, es decir, para cada $s = 1,\dots,n-r$ el ideal $(F_1,\dots,F_s)$ es radical. Consideremos las variedades intermedias $V_s := V(F_1,\dots,F_s)$, sea $\delta_s := \deg V_s$ y $\Delta := \max_{1\le s\le n-r} \delta_s$. Por un instante, fijemos s y supongamos que hemos realizado un cambio de variables, transformando las variables $X_1,\dots,X_n$ en nuevas variables $Y_1,\dots,Y_n$, y que hemos elegido un punto $P^{(s)} \in \mathbb{A}^{n-s}$ con las siguientes propiedades:

1. Las variables están en posición de Noether con respecto a V_s con $Y_1,\dots,Y_{n-s}$ variables libres. Por lo tanto, la proyección $\pi_s : V_s \to \mathbb{A}^{n-s}$ en las formas lineales $Y_1,\dots,Y_{n-s}$ es un morfismo finito.

2. La forma Y_{n-s+1} induce un elemento primitivo de la extensión entera de anillos $\overline{\mathbb{F}}_q[Y_1,\dots,Y_{n-s}] \hookrightarrow \overline{\mathbb{F}}_q[V_s]$.

3. El punto $P^{(s)} = (p_1,\dots,p_{n-s})$ es un punto no ramificado del morfismo π_s y la fibra de dimensión cero $V_{P^{(s)}} := \pi_s^{-1}(P^{(s)})$ tiene δ_s puntos. Además, si $P^{(s+1)} = (p_1,\dots,p_{n-s-1})$ denota el vector de $\mathbb{A}^{n-s-1}$ conformado por las primeras $n-s-1$ coordenadas de $P^{(s)}$, resulta que $P^{(s+1)}$ es punto no ramificado de π_{s+1} y la fibra $V_{P^{(s+1)}}$ tiene la siguiente propiedad: para cada $Q \in V_{P^{(s+1)}}$, el morfismo π_s es no ramificado en $\pi_s(Q)$.

La puesta en marcha del algoritmo descansa sobre la posibilidad de que las condiciones anteriores se verifiquen simultáneamente en cada una de las $n-r$ etapas del mismo. De las dos primeras condiciones ya hemos dado cuenta en el **Teorema 4**. La tercera condición es la que requiere ser elaborada. Nuevamente, obtenemos una cota superior sobre el grado de la condición genérica que subyace a la posibilidad mencionada. En efecto, el Teorema 7.2.7 proporciona tal cota de grado que presentamos en el siguiente resultado.

Teorema 8 *Existe un polinomio* B *con coeficientes en* $\overline{\mathbb{F}}_q$ *y* $n(n+1)+n-1$ *indeterminadas de grado acotado por* $4n^4d\Delta^4$ *tal que para cada* $(\lambda,\gamma,P) \in \mathbb{A}^{n(n+1)} \times \mathbb{A}^{n-1}$ *con* $B(\lambda,\gamma,P) \neq 0$*, definiendo las formas lineales* $(Y_1,\dots,Y_n) = \lambda X + \gamma$ *y* $P^{(s)} = (p_1,\dots,p_{n-s})$*, para cada* $s = 1,\dots,n-r$ *se verifican simultáneamente las siguientes condiciones:*

(i) *el morfismo* $\pi_s : V_s \to \mathbb{A}^{n-s}$ *es finito,* $P^{(s)} \in \mathbb{A}^{n-s}$ *es un punto de levantamiento (no ramificado) de* π_s *y la forma lineal* Y_{n-s+1} *es un elemento primitivo de la fibra* $\pi_s^{-1}(P^{(s)})$.

(ii) *El morfismo* $\pi_{s+1} : V_{s+1} \to \mathbb{A}^{n-s-1}$ *es finito,* $P^{(s+1)} \in \mathbb{A}^{n-s-1}$ *es un punto de levantamiento de* π_{s+1} *y la forma lineal* Y_{n-s} *es un elemento primitivo de la fibra* $\pi_{s+1}^{-1}(P^{(s+1)})$.

(iii) *Cada punto* $Q \in \pi_s\big(\pi_{s+1}^{-1}(P^{(s+1)})\big)$ *es un punto de levantamiento de* π_s *y la forma lineal* Y_{n-s+1} *es un elemento primitivo de* $\pi_s^{-1}(Q)$.

Con un resultado de esta índole es sencillo establecer una condición de regularidad para que los hechos anteriores acontezcan sobre un cuerpo finito. Así es, entonces, cómo se inicia el algoritmo: determinando de antemano una extensión finita K de $\mathbb{F}_q$ de cardinal mayor que $60n^4d\Delta^4$. Aplicando el lema de Zippel–Schwartz, la probabilidad de elegir un elemento $(\lambda,\gamma,P) \in K^{n(n+1)} \times K^{n-1}$ que no anula al polinomio B es mayor o igual que $14/15$.

Observemos que en el último paso de nuestro algoritmo recuperamos la variedad de entrada V. Como es una $\mathbb{F}_q$–variedad estamos interesados en describirla mediante formas lineales $Z_1,\dots,Z_{r+1} \in \mathbb{F}_q[X_1,\dots,X_n]$ y un punto de levantamiento $P = (p_1,\dots,p_r) \in \mathbb{F}_q^r$ de la proyección $\pi \to \mathbb{A}^r$ en las formas $Z_1,\dots,Z_r$. El Corolario 7.2.8 da una condición de regularidad para obtener tal descripción. Concluimos el Capítulo 7 con una versión efectiva del primer teorema de Bertini (Teorema 7.3.1). Este resultado nos permitirá reducir la búsqueda del punto q–racional de V a la búsqueda de un punto q–racional en una curva absolutamente irreducible definida sobre $\mathbb{F}_q$.

Teorema 9 *Existe un polinomio no nulo* $C \in \overline{\mathbb{F}}_q[\Omega_1,\dots,\Omega_r]$ *de grado a lo sumo* $2\delta^4$ *tal que si* $\omega := (\omega_1,\dots,\omega_r) \in \mathbb{A}^r$ *no anula a* C *y* $L_\omega \subset \mathbb{A}^n$ *es la variedad lineal de dimensión* $n-r+1$ *parametrizada por las ecuaciones* $Z_1 = \omega_1 T + p_1,\dots,Z_r = \omega_1 T + p_r$ *entonces* $V \cap L_\omega$ *es una variedad afín absolutamente irreducible de dimensión 1 (*$\Omega_1,\dots,\Omega_r$ *y* T *son nuevas indeterminadas y* $(p_1,\dots,p_r)$ *son las coordenadas del punto* P*).*

El algoritmo puede dividirse en tres etapas principales, etapas que se corresponden, cada una, con un capítulo del trabajo.

Fijamos un cuerpo finito K que extiende a $\mathbb{F}_q$ con $|K| > 60n^4d\Delta^4$ y elegimos aleatoriamente $(\lambda,\gamma,P) \in K^{n(n+1)} \times K^{n-1}$. Con probabilidad mayor a $14/15$ el punto (λ,γ,P) no anula al polinomio B del **Teorema 8**. Quedan definidas formas lineales $Y = (Y_1,\dots,Y_n) = \lambda X + \gamma$ y un punto $P = (p_1,\dots,p_{n-1})$ tales que para cada $1 \le s \le n-r-1$ son válidas las condiciones de dicho teorema.

La primera parte (Capítulo 8) es un proceso que, tomando como dato de entrada la sucesión regular reducida $F_1,\dots,F_{n-r} \in \mathbb{F}_q[X_1,\dots,X_n]$ que define la variedad V, proporciona una descripción completa de una sección lineal genérica de dimensión cero de nuestra variedad de entrada V. Tal descripción está representada por la proyección $\tilde{\pi} : V \to \mathbb{A}^r$ en las formas lineales $Y_1,\dots,Y_r \in K[X_1,\dots,X_n]$ y una parametrización de la fibra no ramificada $\tilde{\pi}^{-1}(p_1,\dots,p_r)$.

Este procedimiento se lleva a cabo en $r-1$ pasos; en el paso s–ésimo se calcula una descripción completa de una sección lineal de dimensión cero de la variedad intermedia V_{s+1}, representada por la fibra no ramificada $\pi_{s+1}^{-1}(P^{(s+1)})$ de la proyección lineal $\pi_{s+1}: V_{s+1} \to \mathbb{A}^{n-s-1}$ en las formas $Y_1,\ldots,Y_{n-s-1}$ (que resulta ser además un morfismo finito). Para esto, en la Sección 8.3 la fibra no ramificada $\pi_s^{-1}(P^{(s)})$ del paso previo se «levanta», aplicando la versión del operador de Newton–Hensel global de [GLS01], a la curva

$$W_{P^{(s+1)}} = V_s \cap \{Y_1 = p_1,\ldots,Y_{n-s-1} = p_{n-s-1}\}.$$

Posteriormente, intersecando esta curva con la hipersuperficie definida por F_{s+1} obtenemos una descripción completa de la fibra $\pi_{s+1}^{-1}(P^{(s+1)})$. Esta intersección se considera en las Secciones 8.4.1 y 8.4.2. Una de las ventajas de este levantamiento es que, al trabajar con este tipo de curvas, podemos describirlas por medio de polinomios bivariados, los cuales pueden representarse y manipularse por su escritura densa con un costo algorítmico razonable. Este enfoque constituyó un cambio importante en la algorítmica y fue obtenido por primera vez, simultánea e independientemente, en los trabajos [GLS01], [HMW01].

El Capítulo 9 trata con la segunda parte del algoritmo, y en ella nos dedicamos a obtener una descripción de una sección lineal de dimensión cero $\mathbb{F}_q$–definible de V. Nuestra intención es pasar de la descripción anterior con formas lineales $Y_1,\ldots,Y_{r+1} \in K[X_1,\ldots,X_n]$ y un punto de levantamiento $P \in K^r$, a una descripción con formas lineales $Z_1,\ldots,Z_{r+1} \in \mathbb{F}_q[X_1,\ldots,X_n]$ y un punto de levantamiento $Q \in \mathbb{F}_q^r$. Este pasaje se logra definiendo una homotopía, basada en un levantamiento de Newton–Hensel global. Esta homotopía deforma el morfismo finito $\tilde{\pi}: V \to \mathbb{A}^r$ y la fibra genérica K–definible no ramificada $\tilde{\pi}^{-1}(P)$ en un morfismo finito $\pi: V \to \mathbb{A}^r$ definido sobre $\mathbb{F}_q$ y una fibra genérica no ramificada $\pi^{-1}(Q)$ definida sobre $\mathbb{F}_q$, donde Q es un punto con coordenadas en $\mathbb{F}_q$.

Nos abocamos a describir la tercera y última etapa del algoritmo, es decir, el contenido del Capítulo 10. Aplicando el **Teorema 9** obtenemos una curva plana C definida sobre $\mathbb{F}_q$ absolutamente irreducible con la propiedad de que cualquier punto q–racional suave de C inmediatamente proporciona un punto q–racional de la variedad V. ¿Cómo llevamos a cabo entonces el cálculo de un punto q–racional suave de esta curva plana? Las condiciones de regularidad garantizan que la curva tiene suficientes puntos q–racionales del tipo requerido. Mediante un algoritmo probabilístico que involucra el cálculo de un número de máximo común divisores y factorización de polinomios univariados con coeficientes en $\mathbb{F}_q$, encontramos un punto q–racional de la curva plana, y, por ende, de la variedad V.

El siguiente resultado (Teorema 10.3.1) resume el costo del algoritmo delineado en los párrafos precedentes.

Teorema 10 *Sea* $q > 8n^2d\delta^4$. *Si los polinomios* $F_1,\ldots,F_{n-r}$ *que definen la va-*

riedad V *se evalúan con* $\mathcal{T}$ *operaciones en* $\mathbb{F}_q$*, entonces un punto* q*–racional de* V *puede calcularse con* $O\big((n\mathcal{T}+n^5)M(\Delta)M(d\Delta)\log q\big)$ *operaciones en* $\mathbb{F}_q$*,* donde $M(m) := m\log^2 m\log\log m$.

Debemos señalar que, por primera vez en el ámbito de la resolución de sistemas de ecuaciones polinomiales sobre cuerpos finitos, se presenta un algoritmo cuya complejidad es polinomial en el número de Bézout del sistema, teniendo incluso una complejidad exponencialmente mejor nuestra estimación de complejidad del peor caso en los casos "geométricamente bien condicionados". Como se observa, nuestro algoritmo funciona para cuerpos de característica arbitraria, pero requiere que la cantidad de elementos del mismo sea al menos del orden de una potencia cuarta del grado de la variedad de entrada. Esto también constituye una mejora sustancial respecto de todos los algoritmos anteriormente presentados (ver por ejemplo [HW99]), dado que éstos requieren que el cuerpo finito tenga cardinal al menos del orden de una potencia quinta del grado del sistema o del número de Bézout del sistema, pudiendo éstos ser exponenciales con respecto al grado de la variedad de entrada.

Finalmente, en el Capítulo 11 analizamos de qué manera este algoritmo y las técnicas subyacentes al mismo, contribuyen al criptoanálisis de los esquemas criptográficos multivariados sobre cuerpos finitos. Los resultados de este capítulo aparecen en forma resumida en [CMW06].

Es una idea difundida en ciertos ambientes de la criptografía que la dificultad intrínseca de la resolución de sistemas de ecuaciones polinomiales implicaría la seguridad de un esquema criptográfico que codifique mensajes como soluciones de ciertos sistemas de ecuaciones polinomiales sobre cuerpos finitos (ver por ejemplo [IM88], [CKPS00]).

Se ha pensado durante cierto tiempo que cualquier problema de tipo NP–completo podría ser utilizado a fines de obtener esquemas criptográficos seguros. Esta creencia fue derribada y los intentos por construir criptosistemas utilizando el problema de la mochila –intentos que fracasaron rotundamente– constituyen un ejemplo de las limitaciones de este enfoque. En el caso que nos concierne, el de los sistemas de ecuaciones polinomiales sobre cuerpos finitos, creemos que ciertos parámetros geométricos, asociados a los sistemas de ecuaciones polinomiales en consideración, son claves para garantizar la seguridad del esquema criptográfico multivariado en cuestión. En particular, estudiamos tales parámetros y presentamos un algoritmo, polinomial con respecto a los mismos, que decodifica el esquema criptográfico correspondiente. De esta forma, creemos aportar evidencia acerca de que la seguridad de los esquemas criptográficos multivariados es una cuestión delicada que puede analizarse empleando herramientas de la teoría de eliminación efectiva.

Dados $F_1,\dots,F_n \in \mathbb{F}_q[X_1,\dots,X_n]$ polinomios de grado a lo sumo d, consideramos la aplicación $F\colon \mathbb{A}^n \to \mathbb{A}^n$ definida por $F(x) := \big(F_1(x),\dots,F_n(x)\big)$. Asumiendo que la restricción de F a $\mathbb{F}_q^n$ es biyectiva, desarrollamos un algoritmo que, dado $y^{(0)} \in \mathbb{F}_q^n$, calcula

el único punto $x^{(0)} \in \mathbb{F}_q^n$ tal que $F(x^{(0)}) = y^{(0)}$. Para eso, pensamos el gráfico de F como una subvariedad $V \subset \mathbb{A}^{2n}$ (absolutamente irreducible) y consideramos la proyección $\pi : V \to \mathbb{A}^n$ en las variables $Y_1, \ldots, Y_n$. Denotemos por δ el grado de V y por D el grado del morfismo π. La idea es deformar el sistema $F(X) = y^{(0)}$ en un sistema $F(X) = F(x^{(1)})$, donde $x^{(1)}$ es un punto con coordenadas en una extensión finita K de $\mathbb{F}_q$. La deformación que planteamos está fuertemente inspirada por el trabajo [PS04]. Nuestro resultado es el siguiente (ver Teorema 11.3.7):

Teorema 12 *Si los polinomios* $F_1, \ldots, F_n$ *se evalúan con* $\mathcal{T}$ *operaciones sobre* $\mathbb{F}_q$*, la única solución* q*–racional del sistema* $F(X) = y^{(0)}$ *puede calcularse con* $O((\mathcal{T} + n^4 + D^2)n\delta^2)$ *operaciones sobre* $\mathbb{F}_q$*.*

En nuestra idea de identificar parámetros relevantes en términos criptográficos vemos que el grado de la variedad en cuestión, el gráfico de la función F, y el grado del morfismo proyección surgen naturalmente como parámetros a tener en cuenta. En este sentido, no nos resulta útil aplicar el algoritmo proporcionado en el **Teorema 10** ya que la complejidad de éste depende del grado del sistema de ecuaciones. Notemos, no obstante, que en el caso en que el grado del sistema es igual al grado de la variedad, la complejidad del algoritmo del **Teorema 11** es claramente superior a la del algoritmo del **Teorema 10**, y en esa situación convendría aplicar este último.

2 Preliminares

En este capítulo presentamos definiciones, resultados y vocabulario de geometría algebraica y álgebra conmutativa que serán utilizados a lo largo de todo el trabajo. Seguimos principalmente los textos [Kun85], [Sha94], [Eis95].

2.1. Definiciones y terminología básica

Dado un cuerpo K denotaremos por $\mathbb{A}^n(K)$ el espacio afín de dimensión n definido sobre K y por $\mathbb{P}^n(K)$ el espacio proyectivo de dimensión n definido sobre K.

Definición 2.1.1. *Sea K un cuerpo y sea $\overline{K}$ la clausura algebraica de K.*

(i) *Un subconjunto $V \subset \mathbb{A}^n(\overline{K})$ es una K–variedad afín si existen polinomios en $K[X_1,\ldots,X_n]$ tal que V es el conjunto de ceros comunes de estos polinomios en $\mathbb{A}^n(\overline{K})$.*

(ii) *Un subconjunto $V \subset \mathbb{P}^n(\overline{K})$ es una K–variedad proyectiva si existen polinomios homogéneos en $K[X_0,X_1,\ldots,X_n]$ tal que V es el conjunto de ceros comunes de estos polinomios en $\mathbb{P}^n(\overline{K})$.*

Cuando tratemos con el espacio afín o proyectivo de dimensión n sobre un cuerpo algebraicamente cerrado escribiremos $\mathbb{A}^n$ y $\mathbb{P}^n$.

A continuación, una serie de definiciones y resultados válidos tanto para K–variedades afines como para K–variedades proyectivas; por eso, simplemente, los enunciamos como resultados válidos para K–variedades. Cuando algún resultado dependa de la naturaleza afín o proyectiva de la variedad lo mencionaremos explícitamente.

Dada una K–variedad V en el espacio n–dimensional denotamos por $I(V)$ el ideal de la variedad y por $K[V]$ su anillo de coordenadas. Observemos que $I(V)$ es un ideal radical y por lo tanto $K[V]$ resulta ser una K–álgebra reducida.

A cada K–variedad afín $V \subset \mathbb{A}^n$ podemos asociarle una K–variedad proyectiva: la clausura proyectiva $\overline{V} \subset \mathbb{P}^n$ (respecto de la K–topología de Zariski de $\mathbb{P}^n$, considerando una inmersión de $\mathbb{A}^n$ en $\mathbb{P}^n$). La clausura proyectiva $\overline{V}$ es la menor variedad proyectiva que contiene a V. Los puntos de $\overline{V} \setminus V$ se denominan puntos del infinito. La dimensión de $\overline{V}$ es igual a la de V y V es irreducible si y solo si $\overline{V}$ lo es.

Definición 2.1.2. *Sea V una K–variedad y sea $\overline{K}$ la clausura algebraica de K.*

1. V *se dice* K–irreducible *si no puede descomponerse como unión de* K*–variedades propias.*

2. V *se dice* absolutamente irreducible *si es irreducible como* $\overline{K}$*–variedad.*

3. V *se dice* relativamente irreducible *(con respecto a* K*) si es* K*–irreducible y existe una extensión algebraica* K' *de* K *y* K'*–variedades absolutamente irreducibles* $V_1, \ldots, V_N$ *tal que* $V = V_1 \cup \cdots \cup V_N$.

Señalemos que, en el caso relativamente irreducible, la variedad V resulta ser equidimensional.

Lema 2.1.3. *(Lema de Normalización de Noether) Sea* V *una* K*–variedad afín de dimensión* r *con* K *un cuerpo infinito. Existen* r *formas lineales* $Y_1, \ldots, Y_r \in K[X_1, \ldots, X_n]$ *tales que*

1. *las clases de* $Y_1, \ldots, Y_r$ *en* $K[V]$*, denotadas por* $y_1, \ldots, y_r$*, son* K*–algebraicamente independientes sobre* $K[V]$*,*

2. *la extensión* $K[y_1, \ldots, y_r] \hookrightarrow K[V]$ *es una extensión entera de anillos.*

Más adelante, vamos a mostrar que, aún en el caso en que K sea un cuerpo finito, perdura la validez del resultado anterior si imponemos ciertas condiciones sobre el cardinal de K.

Supongamos que hemos realizado un cambio lineal de coordenadas, transformando las variables $X_1, \ldots, X_n$ en nuevas variables $Y_1, \ldots, Y_n$. Decimos que las variables $Y_1, \ldots, Y_n$ están en *posición de Noether* respecto de V si las variables $Y_1, \ldots, Y_r$ verifican las condiciones del Lema 2.1.3. Las variables $Y_1, \ldots, Y_r$ se denominan variables *libres* mientras que $Y_{r+1}, \ldots, Y_n$ se denominan variables *dependientes*.

Definición 2.1.4. *Sean* V *y* W *dos* K*–variedades irreducibles de igual dimensión y sea* $f : V \to W$ *un morfismo dominante. Denotemos por* f^* *el morfismo inducido entre los cuerpos de funciones. El grado de la extensión finita de cuerpos* $f^*(K(W)) \subset K(V)$ *se denomina el* grado *del morfismo* f.

De esta definición se deduce el siguiente Teorema:

Teorema 2.1.5. *[Sha94, Ch. II, §6, Theorem 3] Sea* $f : V \to W$ *un morfismo finito de variedades irreducibles con* W *una variedad normal (el anillo de coordenadas es integralmente cerrado). Entonces la cantidad de preimágenes de cada* $y \in W$ *es menor o igual que el grado de* f.

A continuación, presentamos la noción de punto no ramificado.

Definición 2.1.6. *Decimos que* f *es* no ramificado *en* $y \in W$ *o que* y *es un* punto no ramificado *de* f *si la cantidad de preimágenes de* y *es igual al grado de* f.

Teorema 2.1.7. *[Sha94, Ch. II, §6, Theorem 4] En las condiciones de la definición anterior, si la extensión de cuerpos es separable, existe un abierto* $U \subset W$ *tal que para cada* $y \in U$ *el morfismo* f *es no ramificado en* y.

Si bien las definiciones y resultados anteriores justifican gran parte de nuestra tarea, necesitamos extenderlos ya que no siempre trataremos con variedades irreducibles; al mismo tiempo, los morfismos con los cuales trataremos en nuestro trabajo son proyecciones lineales en algún espacio afín o proyectivo. De ahí que brindemos una definición particular de no ramificación, que, en el caso de variedades irreducibles, resultará equivalente a la anterior.

Consideremos entonces una K–variedad equidimensional V de dimensión r (K un cuerpo perfecto) definida por una sucesión regular $F_1, \ldots, F_{n-r} \in K[X_1, \ldots, X_n]$ y supongamos que hemos realizado un cambio lineal de coordenadas, transformando las variables $X_1, \ldots, X_n$ en nuevas variables $Y_1, \ldots, Y_n$, de modo que éstas están en *posición de Noether* respecto de V. Consideremos el morfismo finito $\pi : V \to \mathbb{A}^r$ definido por la proyección en $Y_1, \ldots, Y_r$. Si $P \in \mathbb{A}^r$, deducimos que el cardinal de la fibra $V_P := \pi^{-1}(P)$ es menor o igual que el rango del $K[Y_1, \ldots, Y_r]$–módulo libre $K[V]$.

Definición 2.1.8. *Un punto* $P = (p_1, \ldots, p_r) \in \mathbb{A}^r$ *es un punto no ramificado de* π *si el ideal generado por* $F_1, \ldots, F_{n-r}, Y_1 - P_1, \ldots, Y_r - P_r$ *es radical.*

Lo interesante de la definición anterior es que es una definición que pone en juego el teorema de la función implícita. En efecto, obtenemos el siguiente resultado.

Lema 2.1.9. *Un punto* $P \in \mathbb{A}^r$ *es un punto no ramificado de* π *si, y solo si, la matriz Jacobiana respecto de las variables dependientes* $(\partial F_j / \partial Y_{r+k})_{1 \le j,k \le n-r}(x)$ *es inversible para cada* $x \in V_P := \pi^{-1}(P)$.

Demostración. Sea $P \in \mathbb{A}^r$ un punto no ramificado y consideremos el ideal radical $I := (F_1, \ldots, F_{n-r}, Y_1 - P_1, \ldots, Y_r - P_r)$. En particular, el ideal I es el ideal de la fibra V_P. De [CLO98, Chapter 4, Corollary 2.6] se sigue que V_P es no singular. Por lo tanto, el criterio del jacobiano implica que la matriz $(\partial F_j / \partial Y_{r+k})_{1 \le j,k \le n-r}(x)$ es inversible para cada $x \in V_P := \pi^{-1}(P)$.

Por otro lado, supongamos que la matriz jacobiana es inversible para cada $x \in V_P$. Entonces, no es un divisor de cero en $\overline{K}[Y_1, \ldots, Y_n]/I$. Deducimos de [Eis95, Theorem 18.15] que $\overline{K}[Y_1, \ldots, Y_n]/I$ es reducido, y por ende, que el ideal I es radical. □

Como consecuencia, llegamos a que si $P \in \mathbb{A}^r$ es un punto no ramificado de π entonces el cardinal de la fibra V_P es igual a la dimensión del K–espacio vectorial $K[Y_1, \ldots, Y_n]/I$, donde $I = (F_1, \ldots, F_{n-r}, Y_1 - P_1, \ldots, Y_r - P_r)$. Esta dimensión es igual al rango de $K[V]$

como $K[Y_1,\dots,Y_r]$–módulo libre, que coincide con el grado del morfismo π, es decir, el rango del anillo total de fracciones $K(V)$ como $K(Y_1,\dots,Y_r)$–álgebra. Así vemos que, en este caso, la Definición 2.1.8 extiende la Definición 2.1.6.

2.2. El grado de una variedad

Sea V una K–variedad equidimensional de dimensión r. Adoptamos la definición usual de grado de una variedad; es decir, el *grado* $\deg V$ de V es el número máximo de puntos en la intersección de V con una variedad lineal genérica L de codimensión r para la cual $|V\cap L|<\infty$. En cambio, si V es una K–variedad arbitraria seguimos [Hei83, Definition 1, Remark 2] y definimos el grado de V como la suma de los grados de sus K–componentes irreducibles; en símbolos, si $V=V_1\cup\cdots\cup V_N$ es la descomposición de V en K–componentes irreducibles entonces $\deg V:=\sum_{i=1}^{N}\deg V_i$.

Si $V\subset\mathbb{A}^n$ es una K–variedad de grado δ, su clausura proyectiva $\overline{V}\subset\mathbb{P}^n$ también tiene grado δ (ver por ejemplo [CGH91, Proposition 1.11]).

Con la definición de grado que hemos dado, el grado de la intersección de dos variedades satisface la *Desigualdad de Bézout* ([Hei83, Ful84, Vog84]).

Teorema 2.2.1. *Si V y W son K–variedades entonces*

$$\deg V\cap W\le\deg V\deg W. \tag{2.1}$$

El próximo resultado garantiza que las proyecciones lineales de una variedad arbitraria tienen grado acotado por el grado de la variedad.

Lema 2.2.2. *[Hei83, Lemma 2] Sea $\phi:V\to W$ un morfismo lineal entre K–variedades. Entonces $\deg\overline{\phi(V)}\le\deg V$.*

Consideremos ahora una K–variedad $V\subset\mathbb{A}^n$ irreducible de dimensión r y grado δ. Supongamos que hemos elegido variables $Y_1,\dots,Y_n$ con $Y_1,\dots,Y_r$ variables libres, de modo tal que la extensión de cuerpos $K(Y_1,\dots,Y_r)\hookrightarrow K(V)$ es separable. La proyección $\pi:V\to\mathbb{A}^r$ en las formas $Y_1,\dots,Y_r$ es un morfismo dominante. De la Proposición 2.1.7 y de la definición de grado de una variedad deducimos que si D es el grado de la extensión de cuerpos $K(Y_1,\dots,Y_r)\hookrightarrow K(V)$, entonces D es menor o igual que δ.

Finalmente, enunciamos un resultado que se revelará de suma importancia al momento de obtener estimaciones sobre la cantidad de puntos q–racionales de una $\mathbb{F}_q$–variedad.

Proposición 2.2.3. *[HS82, Proposition 2.3] Sean $V_1,\dots,V_s\subset\mathbb{A}^n$ variedades. Supongamos que $\dim V_1=r$ y sea D el máximo de los grados de $V_2,\dots,V_s$. Entonces se verifica que $\deg(V_1\cap\cdots\cap V_s)\le\deg V_1 D^r$.*

2.3. La forma de Chow de una variedad y la noción de solución geométrica

En esta sección presentamos la noción de forma de Chow de una variedad V. Es un concepto decisivo ya que su consideración trae aparejada una serie de consecuencias positivas para nuestro trabajo. La forma de Chow constituye el puntapié inicial para probar un número de propiedades de las variedades con las cuales se tratan: propiedades de la dimensión de una variedad, la definición de grado de las mismas, etc. En esta sección seguimos el texto de Hodge–Pedoe [HP68] aunque [Sam67] y, en menor medida, [Sha84], pueden citarse también como referencias; de todos modos, Shafarevich señala que las dos primeras son las referencias que deben consultarse si se desea indagar en mayor detalle las propiedades de la forma de Chow. El texto de Hodge–Pedoe es muy interesante desde una perspectiva histórica: constituye una muestra de cómo se hacía geometría algebraica antes de la introducción de los métodos del álgebra conmutativa. Por supuesto, que todo el lenguaje se puede reformular en términos actuales. Esto es lo que hacemos en esta sección.

Sea $V \subset \mathbb{A}^n$ una K–variedad irreducible de dimensión r y grado δ(con K un cuerpo perfecto infinito) y sea $\overline{K}$ la clausura algebraica de K.

Sea $\Lambda := (\Lambda_{i,j})_{1\leq i\leq r+1,\, 1\leq j\leq n}$ una matriz de indeterminadas y $\Gamma := (\Gamma_1,\ldots,\Gamma_{r+1})$ un vector de indeterminadas sobre K. Para cada $1 \leq i \leq r+1$, denotamos por $\Lambda^{(i)} := (\Lambda_{i,1},\ldots,\Lambda_{i,n})$ la i–ésima fila de Λ. Definimos a continuación $r+1$ formas lineales genéricas de $K(\Lambda,\Gamma)[X_1,\ldots,X_n]$ mediante las ecuaciones

$$\widetilde{Y}_i := \sum_{j=1}^{n} \Lambda_{ij} X_j + \Gamma_i \quad (i = 1,\ldots,r+1). \tag{2.2}$$

Si consideramos la extensión de cuerpos $K \hookrightarrow K(\Lambda,\Gamma)$, la variedad V, pensada como una $K(\Lambda,\Gamma)$–variedad, también es irreducible y de dimensión r. Por lo tanto, el anillo de coordenadas de V como $K(\Lambda,\Gamma)$–variedad resulta isomorfo a $K(\Lambda,\Gamma) \otimes_K K[V]$. Si $\xi_1,\ldots,\xi_n \in K[V]$ denotan las funciones coordenadas inducidas por $X_1,\ldots,X_n$, reemplazando en (2.2) definimos $r+1$ elementos de $K(\Lambda,\Gamma) \otimes_K K[V]$ como

$$\widehat{Y}_i := \sum_{j=1}^{n} \Lambda_{i,j} \xi_j + \Gamma_i.$$

Estos elementos son algebraicamente dependientes sobre $K(\Lambda,\Gamma)$, lo cual implica que existe un polinomio $P_V \in K[\Lambda,\Gamma,\widetilde{Y}_1,\ldots,\widetilde{Y}_{r+1}]$ irreducible, de modo tal que en $K(\Lambda,\Gamma) \otimes_K K[V]$ se verifica la siguiente identidad:

$$P(\Lambda,\Gamma,\widehat{Y}_1,\ldots,\widehat{Y}_{r+1}) = 0. \tag{2.3}$$

Este polinomio se denomina la forma de Chow de la variedad V. Es un polinomio multihomogéneo y satisface las siguientes cotas de grado:

- $\deg_{\widetilde{Y}_1,\dots,\widetilde{Y}_{r+1}} P_V = \deg_{\widetilde{Y}_{r+1}} P_V = \delta$,
- $\deg_{\Lambda^{(i)},\Gamma_i} P_V \leq \delta$.

Si $\phi \in K[\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_{r+1}]$ es otro polinomio tal que $\phi(\Lambda,\Gamma,\widehat{Y}_1,\dots,\widehat{Y}_{r+1}) = 0$ entonces P_V divide a ϕ. Además, es el único polinomio, salvo escalares, separable respecto de cada indeterminada $\widetilde{Y}_i$ con la propiedad de ser nulo si y solo si las formas lineales tienen un cero en común en la variedad.

Observación 2.3.1. Si $V \subset \mathbb{P}^n$ es una K–variedad proyectiva irreducible de dimensión r y grado δ, argumentando en forma similar, se obtiene la forma de Chow P_V de la variedad V. Consideramos formas lineales genéricas como en (2.2), aunque homogéneas. Notemos que para una elección adecuada del hiperplano del infinito $\{X_0 = 0\}$, éste no contiene a V. Entonces, $\dim V \cap \{X_0 = 0\} = r-1$ y, si escribimos $V_{\text{aff}} := V \cap \{X_0 = 1\}$, tenemos que $V_{\text{aff}} \subset \mathbb{A}^n$ es una variedad afín irreducible (cuya clausura proyectiva es V), de dimensión r y grado δ. En este sentido, podemos visualizar la forma de Chow de V_{aff} como una especialización de la forma de Chow de V.

Cuando V es una variedad equidimensional de dimensión r y grado δ definimos la forma de Chow P_V de V como el producto de las formas de Chow de cada componente irreducible. Claramente, P_V es un polinomio multihomogéneo de grado δ en cada grupo de indeterminadas $\Lambda^{(i)},\Gamma_i$ y en $\widetilde{Y}_1,\dots,\widetilde{Y}_r$. Además, como $K[\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_r][\widetilde{Y}_{r+1}]/(P_V)$ es una K–álgebra reducida y K es un cuerpo perfecto, como consecuencia de [Mat80, Proposition 27.G] deducimos que $K(\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_r)[\widetilde{Y}_{r+1}]/(P_V)$ es una $K(\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_r)$–álgebra reducida. Esto implica que, en particular, P_V es un elemento separable respecto de $\widetilde{Y}_{r+1}$.

Continuamos con otras propiedades, a la postre decisivas, de la forma de Chow. De (2.3) deducimos para cada $j = 1,\dots,n$ que la identidad

$$\frac{\partial P_V}{\partial \Lambda_{r+1,j}}(\Lambda,\Gamma,\widehat{Y}_1,\dots,\widehat{Y}_{r+1}) + \frac{\partial P_V}{\partial \widetilde{Y}_{r+1}}(\Lambda,\Gamma,\widehat{Y}_1,\dots,\widehat{Y}_{r+1})\frac{\partial \widetilde{Y}_{r+1}}{\partial \Lambda_{r+1,j}} = 0$$

es válida en $K[\Lambda,\Gamma] \otimes_K K[V]$. Observemos que, como consecuencia de la separabilidad de P_V respecto de $\widetilde{Y}_{r+1}$, el polinomio $\partial P_V/\partial \widetilde{Y}_{r+1}$ es no nulo. Como $\partial \widetilde{Y}_{r+1}/\partial \Lambda_{i,j} = \xi_j$ podemos escribir

$$\frac{\partial P_V}{\partial \Lambda_{r+1,j}}(\Lambda,\widehat{Y}_1,\dots,\widehat{Y}_{r+1}) + \xi_j \frac{\partial P_V}{\partial \widetilde{Y}_{r+1}}(\Lambda,\widehat{Y}_1,\dots,\widehat{Y}_{r+1}) = 0. \tag{2.4}$$

Como $\overline{K}$ es algebraicamente cerrado, existe $(\lambda,\gamma) \in \overline{K}^{(r+1)(n+1)}$, a partir del cual defin-

imos $r+1$ formas lineales

$$Y_i := \sum_{j=1}^{n} \lambda_{ij} X_j + \gamma_i,$$

tales que, si denotamos por $\zeta_i := \sum_{j=1}^{n} \lambda_{i,j}\xi_j + \gamma_i$ los elementos de $K[V]$ inducidos por estas formas lineales, resulta que $\zeta_1, \ldots, \zeta_r$ son algebraicamente independientes sobre el cuerpo K, la extensión de cuerpos $K(Y_1, \ldots, Y_r) \hookrightarrow K(V)$ es separable de grado $D \leq \delta$ y la ecuación irreducible que relaciona $\zeta_1, \ldots, \zeta_{r+1}$ es igual a

$$m(\zeta_1, \ldots, \zeta_{r+1}) := P_V(\lambda, \gamma, \zeta_1, \ldots, \zeta_{r+1}) = 0.$$

Es más, las formas lineales $Y_1, \ldots, Y_{r+1}$ se pueden elegir de modo que la extensión de anillos $K[Y_1, \ldots, Y_r] \hookrightarrow K[V]$ sea una extensión entera. Cada una de las condiciones anteriores es una condición genérica. Por lo tanto, existe $(\lambda, \gamma) \in \overline{K}^{(r+1)(n+1)}$ que permite que todas, se verifiquen simultáneamente. Más adelante, nos interesará encontrar cotas superiores para el grado de esas condiciones genéricas, lo que redundará en versiones efectivas de dichos resultados.

Especializando entonces (2.4) en $(\Lambda, \Gamma) = (\lambda, \gamma)$ para un elemento (λ, γ) conveniente, y reemplazando $P_V(\lambda, \gamma, Y_1, \ldots, Y_{r+1})$ por $m(Y_1, \ldots, Y_{r+1})$, obtenemos que la identidad

$$\frac{\partial m}{\partial \widetilde{Y}_{r+1}}(\zeta_1, \ldots, \zeta_{r+1})\xi_j - \nu_j(\zeta_1, \ldots, \zeta_{r+1}) = 0 \tag{2.5}$$

es válida en $K[V]$, donde los n polinomios

$$\nu_j(Y_1, \ldots, Y_{r+1}) := -\frac{\partial P_V}{\partial \Lambda_{r+1,j}}(Y_1, \ldots, Y_{r+1})$$

tienen coeficientes en $\overline{K}$ y grado acotado por $\delta - 1$. En consecuencia, los polinomios

$$m(Y_1, \ldots, Y_{r+1}) \text{ y } \frac{\partial m}{\partial Y_{r+1}}(Y_1, \ldots, Y_{r+1})X_j - \nu_j(Y_1, \ldots, Y_{r+1}) \ (1 \leq j \leq n) \tag{2.6}$$

pertenecen al ideal de la variedad $I(V)$ como $\overline{K}$–variedad. En suma, definen una variedad que contiene a la variedad V.

Por otro lado, si x' es un punto cualquiera que satisface las ecuaciones (2.6) y tal que $(\partial m/\partial Y_{r+1})(x') \neq 0$ podemos probar que $x' \in V$. Esta última afirmación, que será demostrada en el Capítulo 5, muestra que el sistema de ecuaciones hallado caracteriza la variedad V. Este sistema de ecuaciones para la variedad V es lo que daremos en llamar una *solución geométrica* de la variedad V. La sucesión de argumentos esgrimidos en torno a la forma de Chow, nos permiten proporcionar la siguiente definición:

Definición 2.3.2. *Sea $V \subset \mathbb{A}^n$ una K–variedad equidimensional de dimensión r y grado δ. Una* solución geométrica *de V es una reescritura de V mediante un cambio*

lineal de coordenadas $Y = AX + \gamma$, *dado por una matriz inversible* A *de tamaño* $n \times n$ *con entradas en* $\overline{K}$ *y un vector* $\gamma \in \overline{K}^n$ *tal que:*

- *Las variables* $Y_1, \ldots, Y_n$ *están en posición de Noether respecto de* V, *siendo* $Y_1, \ldots, Y_r$ *variables libres.*
- *La forma lineal* Y_{r+1} *induce un elemento primitivo de la extensión entera de anillos* $K[Y_1, \ldots, Y_r] \hookrightarrow K[V]$; *es decir, un elemento* $y_{r+1} \in K[V]$ *cuyo polinomio minimal* $m \in K[Y_1, \ldots, Y_r][T]$ *sobre* $K[Y_1, \ldots, Y_r]$ *satisface la condición* $\deg_T m = D$, *donde* D *es el rango del* $K[Y_1, \ldots, Y_r]$*–módulo libre* $K[V]$. *Observemos que* $\deg m \leq \delta$.
- *El polinomio minimal* m *de* y_{r+1} *sobre* $K[Y_1, \ldots, Y_r]$.
- *Una* parametrización *genérica de* V *mediante los ceros de* m *dada por polinomios*

$$v_{r+2}(Y_1, \ldots, Y_r, T), \ldots, v_n(Y_1, \ldots, Y_r, T) \in K[Y_1, \ldots, Y_r][T]$$

de grados $\deg_T v_{r+j} < D$ *y tal que*

$$\frac{\partial m}{\partial Y_{r+1}}(Y_1, \ldots, Y_r, Y_{r+1}) Y_{r+j} - v_{r+j}(Y_1, \ldots, Y_r, Y_{r+1}) \in I(V)$$

para $2 \leq j \leq n - r$. *Observemos que la parametrización es única salvo elementos no nulos de* K.

Otras denominaciones para la representación de la variedad dada por la definición anterior, suelen ser *representación paramétrica* o *monoidal* [HP68] o también *representación racional univariada* [Rou99]. Nosotros, también diremos que las ecuaciones parametrizan las variables por los ceros del minimal m. Es importante resaltar que la noción de solución geométrica tiene una larga historia que se remonta por lo menos hasta Leopold Kronecker [Kro82] (ver también [Mac16], [Zar95]). Los trabajos [CG83] y [GM89] podrían considerarse como los primeros en los cuales esta noción fue implícitamente usada por primera vez en computación simbólica moderna.

La importancia y la utilidad de esta noción se pondrá de manifiesto a lo largo de toda la tesis. Observemos que en el caso en que V es una K–variedad de dimensión cero, este resultado podría considerarse una variante eficiente del clásico Shape Lemma [CLO98]. En los capítulos venideros daremos versiones efectivas de los resultados aquí enunciados. Si bien nuestros resultados estarán enunciados para $\mathbb{F}_q$–variedades, los mismos tienen un rango de validez más amplio que se extiende a cuerpos perfectos cualesquiera.

3 Cotas superiores, estimaciones y resultados de existencia

En este capítulo presentamos cotas superiores, algunas clásicas, otras propias, sobre la cantidad de puntos q–racionales de algunas variedades particulares. Motivamos además la discusión sobre el modo de obtener estimaciones y sobre el papel desempeñado por la noción de regularidad.

3.1. Algunas cotas superiores

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos y $\overline{\mathbb{F}}_q$ su clausura algebraica. Sea V una variedad en el espacio (afín o proyectivo sobre $\overline{\mathbb{F}}_q$) de dimensión n. Un punto $x \in V$ con coordenadas en $\mathbb{F}_q$ es un punto q–racional de V. Denotaremos por $V(\mathbb{F}_q)$ al conjunto de puntos q–racionales de una variedad V. En el caso en que V es afín tenemos que

$$V(\mathbb{F}_q) := V \cap \mathbb{A}^n(\mathbb{F}_q) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_q) : (x_1, \ldots, x_n) \in V\},$$

mientras que si V es una variedad proyectiva escribimos

$$V(\mathbb{F}_q) := V \cap \mathbb{P}^n(\mathbb{F}_q) = \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{F}_q) : (x_0 : x_1 : \cdots : x_n) \in V\},$$

donde $(x_0 : x_1 : \cdots : x_n)$ es un sistema de coordenadas homogéneas de $x \in V$. Por ejemplo, el espacio afín de dimensión n sobre $\mathbb{F}_q$ tiene cardinal $|\mathbb{A}^n(\mathbb{F}_q)| = q^n$, mientras que 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 variedad V surge entonces el problema de calcular o de estimar, el número $|V(\mathbb{F}_q)|$ de puntos q–racionales de V. Hay abundante material sobre el conteo exacto de puntos q–racionales de curvas proyectivas; también, sobre ecuaciones diagonales, formas cuadráticas, etc. En general, no es posible determinar $|V(\mathbb{F}_q)|$ explícitamente y, por ende, los esfuerzos se dirigen hacia una reformulación del problema en términos de lograr cotas superiores, cotas inferiores o estimaciones sobre la cantidad de puntos q–racionales. Es más, en vistas de algunas aplicaciones, es suficiente garantizar la existencia de puntos q–racionales.

Comencemos con el caso de una hipersuperficie y presentemos un resultado clásico.

Proposición 3.1.1 ([LN83], [Sch76]). *Sea* $F \in \overline{\mathbb{F}}_q[X_1,\ldots,X_n]$ *un polinomio de grado* d. *Entonces la cantidad de ceros* q*–racionales de* F *(puntos* q*–racionales de la hipersuperficie definida por* F*) es a lo sumo* dq^{n-1}. *Si* F *es homogéneo entonces la cantidad de ceros* q*–racionales no nulos es a lo sumo* $d(q^{n-1}-1)$.

Las notas del texto [LN83] informan que el caso afín de la proposición anterior fue demostrado por primera vez por Oystein Ore en 1922.

En el caso de ciertas $\mathbb{F}_q$–hipersuperficies, Jean-Pierre Serre proporciona una cota superior más precisa.

Proposición 3.1.2 ([Ser91]). *Sea* $H \subset \mathbb{P}^n$ *una* $\mathbb{F}_q$*–hipersuperficie de grado* $d \leq q+1$. *La cantidad de puntos* q*–racionales verifica* $|H(\mathbb{F}_q)| \leq \delta q^{n-1} + p_{n-2}$.

A continuación presentamos algunas cotas superiores para el número de puntos q–racionales de ciertas variedades. Estos resultados son consecuencia de argumentos elementales de teoría de eliminación efectiva y de la Desigualdad de Bézout (2.1). El propósito es mostrar como estos argumentos simplifican las pruebas previas (cf. [LN83], [Sch74], [Sch76]), de índole combinatoria, y proporcionan, en algunos casos, mejores resultados. El primer resultado que presentamos es una cota superior para la cantidad de puntos q–racionales de una variedad V arbitraria. Este resultado generaliza el de la Proposición 3.1.1.

Proposición 3.1.3. *Sea* V *una variedad de dimensión* r *y grado* δ *en el espacio de dimensión* n *sobre* $\overline{\mathbb{F}}_q$. *El número de puntos* q*–racionales* $|V(\mathbb{F}_q)|$ *verifica la siguiente desigualdad:*

$$|V(\mathbb{F}_q)| \leq \begin{cases} \delta q^r & \text{si } V \text{ es afín,} \\ \delta p_r & \text{si } V \text{ es proyectiva.} \end{cases}$$

Demostración. Comenzamos con el caso afín. Para cada $1 \leq i \leq n$, consideramos la $\mathbb{F}_q$–hipersuperficie $W_i \subset \mathbb{A}^n$ definida por el polinomio $X_i^q - X_i$. Por lo tanto, el conjunto de puntos q–racionales de V se escribe en la forma $V(\mathbb{F}_q) = V \cap W_1 \cap \cdots \cap W_n$. Si $V(\mathbb{F}_q)$ es vacío el grado es igual a 0 y la cota es válida. Supongamos entonces que V tiene puntos q–racionales, con lo cual $V(\mathbb{F}_q)$ es una variedad de dimensión cero. Aplicamos la Proposición 2.2.3 y obtenemos

$$|V(\mathbb{F}_q)| = |V \cap W_1 \cap \cdots \cap W_n| = \deg(V \cap W_1 \cap \cdots \cap W_n) \leq \delta q^r,$$

lo que demuestra el resultado en el caso afín.

Pasamos al caso proyectivo. En este caso la demostración es por inducción en la dimensión de V. Si $r = 0$ entonces es claro que $|V(\mathbb{F}_q)| \leq \delta$, con lo cual podemos suponer que $r \geq 1$. Supongamos, en primer lugar, que V es absolutamente irreducible. Después

de un cambio lineal de coordenadas asumimos que el hiperplano del infinito $\{X_0 = 0\}$ no contiene a V.

Entonces $V_{\text{aff}} := V \cap \{X_0 = 1\}$ es una variedad afín de dimensión r cuya clausura proyectiva es V. Por lo tanto, $\deg V_{\text{aff}} = \deg V = \delta$ y así del caso afín deducimos que $|V_{\text{aff}}(\mathbb{F}_q)| \leq \delta q^r$.

Por otro lado, como el hiperplano del infinito no contiene a V resulta que $V_\infty := V \cap \{X_0 = 0\} = V \setminus V_{\text{aff}}$ es una variedad proyectiva de dimensión a lo sumo $r-1$ y de grado acotado por δ. Por hipótesis inductiva tenemos que $|V_\infty(\mathbb{F}_q)| \leq \delta p_{r-1}$.

En suma,

$$|V(\mathbb{F}_q)| = |V_{\text{aff}}(\mathbb{F}_q)| + |V_\infty(\mathbb{F}_q)| \leq \delta q^r + \delta p_{r-1} = \delta p_r.$$

Esto completa el paso inductivo cuando V es absolutamente irreducible. Ahora, si V es una variedad proyectiva arbitraria, consideramos $V = V_1 \cup \cdots \cup V_N$ la descomposición de V en componentes absolutamente irreducibles. Cada componente V_i tiene dimensión a lo sumo r y si denotamos por δ_i el grado de cada componente V_i, el grado de V es $\delta = \sum_{i=1}^N \delta_i$. De este modo

$$|V(\mathbb{F}_q)| \leq \sum_{i=1}^N |V_i(\mathbb{F}_q)| \leq \sum_{i=1}^N \delta_i p_r \leq \delta p_r.$$

Esto termina la demostración de la proposición.

□

Señalemos que el resultado anterior, en el caso proyectivo, es demostrado en [GL02b, Proposition 12.1] aunque con una demostración diferente. Sin embargo, nuestra demostración es más sencilla e ilustra el tipo de argumentos que utilizaremos.

Proposición 3.1.4. *Sean* $F_1, \ldots, F_m \in \overline{\mathbb{F}}_q[X_1, \ldots, X_n]$ $(m \geq 2)$ *polinomios de grado acotado por* d *sin factores en común en* $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$ *y consideremos* $V \subset \mathbb{A}^n$ *la variedad definida por* $F_1, \ldots, F_m$. *Entonces* $|V(\mathbb{F}_q)| \leq d^2 q^{n-2}$.

Demostración. Como F_1 y F_2 no tienen factores en común en $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$, tenemos que la variedad V' definida por F_1 y F_2 es una variedad de dimensión $n-2$. De la Proposición 3.1.3 y de la desigualdad de Bézout (2.1) concluimos que $|V'(\mathbb{F}_q)| \leq d^2 q^{n-2}$ y por lo tanto $|V(\mathbb{F}_q)| \leq d^2 q^{n-2}$. □

La cota superior que acabamos de obtener mejora las cotas $2n\delta^3 q^{n-2}$ de [Sch74, Lemma 4] y $\delta^3 q^{n-2}$ de [Sch76, Lemma IV.3D].

Proposición 3.1.5. *Sea* $V \subset \mathbb{A}^n$ *una* $\mathbb{F}_q$*–variedad relativamente irreducible de dimensión* r *y grado* δ. *Entonces* $|V(\mathbb{F}_q)| \leq \delta^2 q^{r-1}/4$.

Demostración. Sea $V = V_1 \cup \cdots \cup V_N$ la descomposición de V en componentes absolutamente irreducibles y denotemos por δ_i el grado de cada componente V_i. El conjunto de puntos q–racionales $V(\mathbb{F}_q)$ está contenido en cada una de las componentes V_i [HP68, Ch. X, 12, Theorem II,]; en particular, tenemos que $V(\mathbb{F}_q) \subset (V_1 \cap V_2)(\mathbb{F}_q)$. Aplicamos la Proposición 3.1.3 y obtenemos $|(V_1 \cap V_2)(\mathbb{F}_q)| \leq \delta_1\delta_2 q^{r-1} \leq \delta^2 q^{r-1}/4$. □

En el caso de una $\mathbb{F}_q$–hipersuperficie relativamente irreducible V, nuestra cota superior toma la forma $|V(\mathbb{F}_q)| \leq \delta^2 q^{n-2}/4$. De esta manera, con este resultado mejoramos la cota superior $\delta q^{n-1} - (\delta-1)q^{n-2}$, de [CR96, Theorem 3.1], válida bajo la condición $1 < \delta < q-1$. Nuestra cota es válida para todo q, y además para $\delta \leq q$, se verifica que $\delta^2 q^{n-2}/4 < \delta q^{n-1} - (\delta-1)q^{n-2}$.

3.2. Número promedio de ceros

En la sección anterior exhibimos distintas cotas superiores para la cantidad de puntos q–racionales de diferentes variedades. No obstante, no disponemos de ninguna información sobre cómo estimar la cantidad de puntos q–racionales. Si bien en la Introducción hemos discurrido sobre diferentes estimaciones, aún está pendiente la discusión sobre cómo llegar a ellas. En esta sección, justamente, intentamos motivar esta discusión, remitiéndonos a resultados sobre número promedio de ceros y el consecuente error que se comete al estimar con ese número promedio. Para eso presentamos algunos resultados clásicos que justificarán la manera de lograr estimaciones.

Para cada natural d, consideremos el conjunto Ω_d de los polinomios $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ de grado acotado por d. Dado un polinomio $F \in \Omega_d$, sea $N(F)$ el número de ceros q–racionales de F, es decir, el número de ceros en $\mathbb{F}_q^n$. Con estas notaciones, estos resultados clásicos ([Sch76],[LN83]):

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

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

Estos resultados expresan que un polinomio $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ en n indeterminadas tiene en promedio q^{n-1} ceros en $\mathbb{F}_q^n$ y que el valor promedio de $(N(F) - q^{n-1})^2$ es $q^{n-1} - q^{n-2} = O(q^{n-1})$. Entonces, si H es una $\mathbb{F}_q$–hipersuperficie vamos a estimar por q^{n-1} el número de sus puntos q–racionales y esperamos que $\left||H(\mathbb{F}_q)| - q^{n-1}\right|$ sea del orden de $O(q^{(n-1)/2})$. Por supuesto, esto puede conducir a estimaciones groseras si no tomamos en consideración algunas características geométricas de las hipersuperficies en cuestión, como por ejemplo, la cantidad de componentes irreducibles.

Felizmente, hay una cantidad de situaciones en las que la ocurrencia del caso esperado

tiene lugar. Por ejemplo, la estimación de Hasse–Weil (1.1):

$$\left||C(\mathbb{F}_q)|-p_1\right| \leq 2gq^{1/2}.$$

Es más, esta estimación es óptima en general, ya que existen curvas cuya cantidad de puntos q–racionales es exactamente la que se deduce de la estimación. Estas curvas se denominan curvas maximales. Por otro lado, la estimación de Lang–Weil está lejos de lo que se espera obtener.

Ahora, ¿cómo justificamos el hecho de estimar el número de puntos q–racionales de una $\mathbb{F}_q$–variedad arbitraria de dimensión r absolutamente irreducible por q^r? Una variedad irreducible de dimensión r en el espacio ambiente de dimensión n es birracionalmente equivalente a una hipersuperficie en el espacio ambiente de dimensión $r+1$. Si además, el morfismo birracional está definido sobre $\mathbb{F}_q$, los puntos q–racionales de la hipersuperficie se corresponden con los de V (suponiendo que sea una $\mathbb{F}_q$–hipersuperficie); solo resta estimar el número de puntos q–racionales en los cerrados no isomorfos, y, como éstos tienen dimensión menor que r, asintóticamente, podemos soslayar el aporte a la estimación de los puntos q–racionales de estos conjuntos. Esto justifica la manera de estimar y genera la siguiente pregunta, ¿bajo qué condiciones existe un morfismo birracional definido sobre $\mathbb{F}_q$?

Por otro lado, hasta el momento, no hemos hecho mención alguna respecto de los resultados de existencia de puntos q–racionales: dada una $\mathbb{F}_q$–variedad V decidir si tiene un punto q–racional o también, determinar una cota inferior positiva para la cantidad de puntos q–racionales de V (esta formulación del problema engloba a la primera). Por ejemplo, podemos deducir cotas inferiores sobre el número de puntos q–racionales a partir de las estimaciones, lo que en el caso de la estimación de Hasse-Weil resulta en que la cantidad de puntos q–racionales de una curva proyectiva C absolutamente irreducible no singular de género g está acotada inferiormente por $q+1-2gq^{1/2}$. Observemos que para que la cota inferior sea positiva es preciso establecer cierta relación entre q y g. También es posible obtener cotas inferiores que no provienen de estimaciones como la cota inferior de Schmidt (1.5): el número $|H(\mathbb{F}_q)|$ de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie H absolutamente irreducible de grado δ está acotado inferiormente por $q^{n-1}-(\delta-1)(\delta-2)q^{n-3/2}-(5\delta^2+\delta+1)q^{n-2}$ asumiendo que $q > 10^4 n^3 \delta^5 P^3([4\log\delta])$, donde $P(u)$ es el u–ésimo primo. Observemos que la cota inferior es válida solamente después de imponer condiciones sobre el tamaño del cuerpo finito. Además, bajo esas condiciones, la cota inferior es positiva.

3.3. La noción de regularidad

Supongamos que F es un elemento de $\mathbb{F}_q[X_1,\ldots,X_n]$ de grado d. Por lo tanto, la Proposición 3.1.1 establece que $\mathbb{F}$ tiene a lo sumo dq^{n-1} ceros q–racionales. Para garan-

tizar entonces que exista $x \in \mathbb{F}_q^n$ que no anule a F requerimos que $q > d$. Este resultado, en apariencia inocente, reviste de una importancia fundamental ya que representa el punto de partida desde el cual es posible que las condiciones genéricas se transforman en resultados efectivos. Una gran cantidad de definiciones y resultados de álgebra y geometría algebraica se enuncian en términos genéricos sobre cuerpos algebraicamente cerrados o sobre cuerpos infinitos. Sin embargo, esta manera de enunciarlos no es obstáculo para que esos resultados también cobren legítima existencia sobre cuerpos finitos. Simplemente, en caso de conocer una cota superior, digamos D, sobre el grado de cierta condición genérica que deseamos obtener, imponemos que nuestro cuerpo finito $\mathbb{F}_q$ tenga cardinal mayor que D; de esa forma, Proposición 3.1.1 mediante, logramos que exista un punto con coordenadas en $\mathbb{F}_q$ que no anula a la condición genérica y, en consecuencia, el resultado que esta condición entraña, es válido sobre $\mathbb{F}_q$. Esto exige un esfuerzo ya que no siempre es posible determinar cotas superiores sobre el grado de las condiciones genéricas que se están estudiando. Con todo, este requerimiento sobre la cantidad de elementos de un cuerpo finito que posibilita la realización de ciertas condiciones genéricas geométricas y/o algebraicas sobre dicho cuerpo finito es lo que denominaremos *regularidad*.

Estos son algunos ejemplos de la noción de regularidad:

- Si $q > d$ un polinomio $\mathbb{F} \in \mathbb{F}_q[X_1, \ldots, X_n]$ de grado d no es la función nula sobre $\mathbb{F}_q^n$.
- Si $q > 4g^2$ la cota inferior de la estimación de Hasse–Weil es no trivial y, por lo tanto, la curva tiene puntos q–racionales.
- Si $q > 10^4 n^3 \delta^{5+\epsilon}$ el número de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible es mayor o igual que $q^{n-1} - (\delta-1)(\delta-2)q^{n-3/2} - (5\delta^2+\delta+1)q^{n-2}$.

A lo largo de este trabajo iremos presentando diferentes resultados de esta índole. La cuestión radica entonces en determinar cotas superiores sobre el grado de la condición genérica en danza, y una vez conocido este grado, determinar el cardinal del cuerpo finito.

A fines ilustrativos del tipo y el modo en que obtendremos nuestros resultados presentamos una versión efectiva del Lema de normalización de Noether.

Proposición 3.3.1. *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$–variedad equidimensional de dimensión r y grado δ. Existe un polinomio no nulo A, con coeficientes en $\overline{\mathbb{F}}_q$, en $r(n+1)$ indeterminadas y de grado a lo sumo $r\delta$ tal que para cada $(\lambda, \gamma) \in \mathbb{A}^{r(n+1)}$ con $A(\lambda, \gamma) \neq 0$, definiendo las formas lineales $Y := \lambda X + \gamma := (Y_1, \ldots, Y_r)$, la extensión de anillos $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$ es una extensión entera.*

Demostración. Retomemos las notaciones de la Sección 2.3. Introducimos una matriz de indeterminadas $\Lambda := (\Lambda_{ij})_{1 \leq i \leq r+1, 1 \leq j \leq n}$ sobre $\overline{\mathbb{F}}_q$, un vector de indeterminadas $\Gamma :=$

$(\Gamma_1,\dots,\Gamma_{r+1})$ y, para cada $1\le i\le r+1$, denotamos por $\Lambda^{(i)}:=(\Lambda_{i,1},\dots,\Lambda_{i,n})$ la i–ésima fila de Λ. Consideremos, además, las $r+1$ formas lineales genéricas $\widetilde{Y}:=\Lambda X+\Gamma$. En consecuencia, disponemos de la forma de Chow $P_V\in\overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_{r+1}]$ de la variedad V. Recordemos que verifica las siguientes cotas de grado:

- $\deg_{\widetilde{Y}_1,\dots,\widetilde{Y}_{r+1}} P_V=\deg_{\widetilde{Y}_{r+1}} P_V=\delta$,
- $\deg_{\Lambda^{(i)},\Gamma_i} P_V\le\delta$ for $1\le i\le r+1$.

Denotamos por $\widetilde{A}_1\in\overline{\mathbb{F}}_q[\Lambda,\Gamma]$ el coeficiente no nulo del monomio $\widetilde{Y}_{r+1}^{\delta}$ de P_V, pensando P_V como un elemento de $\overline{\mathbb{F}}_q[\Lambda,\Gamma][\widetilde{Y}_1,\dots,\widetilde{Y}_{r+1}]$ y consideramos, a su vez, un coeficiente $A_1\in\overline{\mathbb{F}}_q[\Lambda^{(1)},\dots,\Lambda^{(r)},\Gamma_1,\dots,\Gamma_r]$ de un monomio no nulo de $\widetilde{A}_1$, pensando $\widetilde{A}_1$ como un elemento de $\overline{\mathbb{F}}_q[\Lambda^{(1)},\dots,\Lambda^{(r)},\Gamma_1,\dots,\Gamma_r][\Lambda^{(r+1)},\Gamma_{r+1}]$. Observemos que $\deg A_1\le r\delta$. Si $(\lambda,\gamma)\in\mathbb{A}^{r(n+1)}$ es un elemento para el cual $A_1(\lambda,\gamma)\neq 0$, definimos las r formas lineales $Y:=(Y_1,\dots,Y_r):=\lambda X+\gamma$. Dado que $A_1^*:=\widetilde{A}_1(\lambda,\gamma,\Lambda^{(r+1)},\Gamma_{r+1})\in\overline{\mathbb{F}}_q[\Lambda^{(r+1)},\Gamma_{r+1}]$ es un polinomio no nulo, existen n vectores linealmente independientes $w_1,\dots,w_n\in\overline{\mathbb{F}}_q^n$ y elementos $a_1,\dots,a_n\in\overline{\mathbb{F}}_q$ tales que $A_1^*(w_k,a_k)\neq 0$ para cada $1\le k\le n$. Considerando las n formas lineales $\ell_k:=w_kX+a_k$ resulta que el polinomio $P_V(\lambda,\gamma,w_k,a_k,Y_1,\dots,Y_r,\ell_k)$ representa una ecuación de dependencia entera sobre $\overline{\mathbb{F}}_q[Y_1,\dots,Y_r]$ para la función coordenada de $\overline{\mathbb{F}}_q[V]$ definida por ℓ_k. Como $\overline{\mathbb{F}}_q[\ell_1,\dots,\ell_n]=\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ comprobamos que la extensión de anillos es una extensión entera. Definimos como $A:=A_1$, el polinomio cuya existencia garantiza la proposición. □

Entonces, para que $Y_1,\dots,Y_r$ sean formas lineales de $\mathbb{F}_q[X_1,\dots,X_n]$, deberíamos tomar $(\lambda,\gamma)\in\mathbb{F}_q^{r(n+1)}$ que no anule al polinomio A de la Proposición 3.3.1. Por la Proposición 3.1.1, el polinomio A tiene a lo sumo $r\delta q^{r(n+1)-1}$ ceros en $\mathbb{F}_q^{r(n+1)}$. Concluimos que imponiendo la condición de regularidad $q>r\delta$ logramos tal cometido.

Corolario 3.3.2. *Sea $V\subset\mathbb{A}^n$ una $\mathbb{F}_q$–variedad equidimensional de dimensión r y grado δ. Entonces si $q>r\delta$, existen formas lineales $Y_1,\dots,Y_r\in\mathbb{F}_q[X_1,\dots,X_n]$ tales que la extensión de anillos $\overline{\mathbb{F}}_q[Y_1,\dots,Y_r]\hookrightarrow\mathbb{F}_q[V]$ es una extensión entera.*

Para concluir la sección, mostramos cómo los resultados de regularidad pueden abordarse en términos probabilísticos. El próximo resultado, una reescritura de la Proposición 3.1.1, es el conocido –en el ámbito del cálculo simbólico– Lema de Zippel–Schwartz ([Zip79], [Sch80]).

Teorema 3.3.3. *Sea $F\in\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ un polinomio de grado a lo sumo d y sea $\mu>0$. Si K es una extensión finita de $\mathbb{F}_q$ con $|K|>\mu d$ entonces la probabilidad de elegir al azar $a\in K^n$ tal que $F(a)\neq 0$ es mayor o igual que $1-1/\mu$.*

Por supuesto, este resultado supone una distribución uniforme de probabilidad en los elementos de K^n. Reiteramos que nos permite reinterpretar la regularidad desde un punto de vista probabilístico.

4 Estimaciones para hipersuperficies afines

Las estimaciones sobre el número de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie $H \subset \mathbb{A}^n$ absolutamente irreducible de [Sch76], [HW98], dependen de manera decisiva de una versión efectiva del primer Teorema de Bertini (véase e.g., [Sha94, §II.6.1, Theorem 1]): la intersección de H con una variedad lineal genérica $L \subset \mathbb{A}^n$ de dimensión 2 es una curva absolutamente irreducible. En nuestro contexto, por versión efectiva del teorema de Bertini entendemos estimar el número de $\mathbb{F}_q$–variedades lineales L para las cuales $H \cap L$ no es una curva absolutamente irreducible. Las estimaciones sobre la cantidad de puntos q–racionales de hipersuperficies que presentaremos en este capítulo derivan de una variante efectiva del primer teorema de Bertini.

4.1. Un Teorema de Bertini efectivo

Consideremos un polinomio $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ absolutamente irreducible de grado δ y sea $H \subset \mathbb{A}^n$ la $\mathbb{F}_q$–hipersuperficie definida por F. Nuestras estimaciones sobre el número de puntos q–racionales de H derivan del análisis de las variedades que se obtienen al intersecar H con una $\mathbb{F}_q$–variedad lineal de dimensión 2.

Necesitamos entonces una estimación sobre el número de $\mathbb{F}_q$–planos $L \subset \mathbb{A}^n$ ($\mathbb{F}_q$–variedades lineales de dimensión 2) definidos sobre $\mathbb{F}_q$ para los cuales $H \cap L$ tiene una componente absolutamente irreducible, definida sobre $\mathbb{F}_q$, de grado a lo sumo D, para $1 \leq D \leq \delta - 1$.

Siguiendo [Kal95], vamos a estudiar la condición genérica que garantiza la no existencia de componentes irreducibles de $H \cap L$ de grado a lo sumo D. Para eso, en la Sección 4.1.1 presentamos un algoritmo que, dado un polinomio $F \in K[X, Y]$ calcula los factores irreducibles de F sobre K de grado a lo sumo D. Luego, en la Sección 4.1.2 obtenemos una cota superior sobre la condición genérica en consideración.

4.1.1. Cálculo de los factores irreducibles de grado a lo sumo D

El algoritmo que presentamos es una variante del correspondiente algoritmo de [Kal95] (ver también [GKL04]).

Algoritmo *Factorización sobre el cuerpo de coeficientes de grado a lo sumo* D.

Input: Un polinomio $F \in K[X, Y]$ mónico en X de grado a lo sumo δ, donde K es un cuerpo arbitrario, tal que la resultante $\mathrm{Res}_X(F(X,0), \partial F(X,0)/\partial X) \neq 0$, y un entero D con

$1 \leq D \leq \delta - 1$.

Output: O bien el algoritmo devuelve los factores irreducibles de F definidos sobre K de grado a lo sumo D, o bien F no tiene factores irreducibles en $K[X,Y]$ de grado a lo sumo D.

Fijamos el máximo orden de aproximación requerido: $\ell_{max} \leftarrow 2D\delta$.

Para todas las raíces $\zeta_i \in \overline{K}$ *de* $F(X,0) \in K[X]$ *Realizar los pasos* **N** *y* **L**.

Paso N: Sea $K_i := K(\zeta_i)$. *Fijamos los puntos iniciales de la iteración de Newton*

$$\alpha_{i,0} \leftarrow \zeta_i \in K_i,\ \beta_{i,0} \leftarrow (\partial F/\partial X)(\alpha_{i,0},0)^{-1} \in K_i.$$

(Describimos la iteración de Newton)

Para $j \leftarrow 0,\ldots,\lfloor \log_2(\ell_{máx}) \rfloor$ *Hacer*

$$\begin{aligned} \alpha_{i,j+1} &\leftarrow (\alpha_{i,j} - \beta_{i,j}F(\alpha_{i,j},Y)) && \mod (Y^{2^{j+1}}),\\ \beta_{i,j+1} &\leftarrow \left(2\beta_{i,j} - (\partial F/\partial X)(\alpha_{i,j+1},Y)\beta_{i,j}^2\right) && \mod (Y^{2^{j+1}}). \end{aligned}$$

(Observemos que $\alpha_{i,j+1}$ y $\beta_{i,j+1}$ son polinomios de $K_i[Y]$ que satisfacen

$$F(\alpha_{i,j+1},Y) \equiv 0 \mod (Y^{2^{j+1}}),$$

$$\beta_{i,j+1} \cdot (\partial F/\partial X)(\alpha_{i,j+1},Y) \equiv 1 \mod (Y^{2^{j+1}}).$$

Fijamos la raíz aproximada

$$\alpha_i \leftarrow \alpha_{i,\lfloor \log_2(\ell_{máx}) \rfloor + 1} \mod (Y^{\ell_{máx}+1}) \in K_i[Y].$$

(Calculamos las potencias de α_i.)

Para $\mu \leftarrow 0,\ldots,\delta-1$ *Hacer*

$$\sum_{k=0}^{\ell_{máx}} a_{i,k}^{(\mu)} Y^k \leftarrow \alpha_i^\mu \mod (Y^{\ell_{máx}+1}) \text{ with } a_{i,k}^{(\mu)} \in K_i.$$

Paso L: Buscamos el polinomio de grado menor en $K[X,Y]$ cuya raíz es α_i.

Para $m \leftarrow 1,\ldots,D$ *Hacer*

Fijamos el orden de aproximación: $\ell \leftarrow 2m\delta$.

(Chequeamos si la ecuación $\alpha_i^m + \sum_{\mu=0}^{m-1} h_{i,\mu}(Y)\alpha_i^\mu \equiv 0 \mod (Y^{\ell+1})$ tiene solución para $h_{i,\mu}(Y) \in K[Y]$ con $\deg(h_{i,\mu}) \leq m - \mu$. Escribiendo $h_{i,\mu}(Y) = \sum_{\eta=0}^{m-\mu} u_{i,\mu,\eta} Y^\eta$, con $u_{i,\mu,\eta} \in K$, y agrupando los coeficientes de Y^k llegamos al siguiente problema.)

Para $0 \leq k \leq \ell$, *resolver el siguiente sistema lineal sobre* K *en las variables*

$u_{i,\mu,\eta}$ $(0 \le \mu \le m-1,\ 0 \le \eta \le m-\mu)$:

$$a_{i,k}^{(m)} + \sum_{\mu=0}^{m-1} \sum_{\eta=0}^{m-\mu} a_{i,k-\eta}^{(\mu)} u_{i,\mu,\eta} = 0 \quad (\text{donde} \quad a_{i,\nu}^{(\mu)} = 0 \text{ for } \nu < 0), \tag{4.1}$$

(Como $\deg h_{i,\mu} \le m-\mu$, para cada μ tenemos $m-\mu+1$ indeterminadas, y por lo tanto el sistema tiene $(m+1)(m+2)/2-1$ indeterminadas.)

Si (4.1) tiene una solución entonces

$$F_i(X,Y) \leftarrow X^m + \sum_{\mu=0}^{m-1} \sum_{\eta=0}^{m-\mu} u_{i,\mu,\eta} Y^\eta X^\mu.$$

(El polinomio $F_i(X,Y)$ es un factor irreducible de $F(X,Y)$ de grado D o tiene algún factor irreducible de grado menor que D.)

Verificar si F_i ha sido producido por una raíz ζ_l con $l < i$. Si no, agregar F_i a la lista de factores irreducibles de grado menor que D.

Si (4.1) no tiene solución para todo $i = 1,\dots,\delta$ y $m = 1,\dots,D$, entonces F no tiene factores irreducibles en $K[X,Y]$ de grado a lo sumo D.

El lema siguiente justifica la validez del algoritmo:

Lema 4.1.1. *El polinomio $F(X,Y)$ tiene un factor irreducible sobre K de grado a lo sumo D si y solo si al menos uno de los $D\delta$ sistemas lineales (4.1) tiene una solución en K.*

Demostración. Supongamos que (4.1) tiene una solución en K, esto es, existe $1 \le i \le \delta$ y un polinomio no nulo $G(X,Y) \in K[X,Y]$ de grado a lo sumo $1 \le m \le D$ tal que $G(\alpha_i, Y) \equiv 0 \pmod{Y^{2m\delta+1}}$. Denotemos por $\rho \in K[Y]$ la resultante $\rho(Y) := \mathrm{Res}_X(F,G)$. Evaluando la identidad correspondiente en $X = \alpha_i$ concluimos que $\rho(Y) \equiv 0 \pmod{Y^{2m\delta+1}}$. Como ρ es un polinomio de grado a lo sumo $2m\delta$, entonces $\rho = 0$. Por lo tanto, F y G tienen un factor común no trivial en $K[X,Y]$, y, en consecuencia, F tiene un factor de grado a lo sumo D.

Supongamos ahora que $F(X,Y)$ tiene un factor irreducible $G(X,Y) \in K[X,Y]$ de grado a lo sumo $D \ge 1$. Existe entonces una factorización no trivial de $F(X,Y) = G(X,Y)H(X,Y)$ sobre $K[X,Y]$. Sea $1 \le i \le \delta$ un entero para el cual $G(\alpha_{i,0}, 0) = 0$. Entonces $G(\alpha_{i,0}, 0) \ne 0$, lo cual implica que $H(\alpha_{i,0}, Y) \not\equiv 0 \bmod (Y)$ y de esta manera

$$H(\alpha_{i,j}, Y) \not\equiv 0 \bmod (Y) \text{ para } 1 \le j \le \lfloor \log_2(\ell_{\max}) \rfloor + 1.$$

Por lo tanto $H(\alpha_i, Y) \not\equiv 0 \bmod (Y)$, y como $F(\alpha_i, Y) \equiv 0 \bmod (Y^{2D\delta+1})$ podemos afirmar que $G(\alpha_i, Y) \equiv 0 \bmod (Y^{2D\delta+1})$. Concluimos que los coeficientes de G, considerado como

un polinomio de $K[Y][X]$, constituyen una solución de al menos uno de los $D\delta$ sistemas lineales (4.1). Esto completa la demostración. □

4.1.2. Sobre la existencia de componentes irreducibles de grado dado

Sea $F \in K[X_1,\dots,X_n]$ un polinomio absolutamente irreducible de grado δ y sea D un entero tal que $1 \le D \le \delta-1$. Dados $\nu_1,\dots,\nu_n,\omega_2,\dots,\omega_n \in \overline{K}$, consideramos el polinomio

$$\chi(X,Y,Z_2,\dots,Z_n) := F(X+\nu_1,\omega_2X+Z_2Y+\nu_2,\dots,\omega_nX+Z_nY+\nu_n)$$

como un elemento de $\overline{K}[X,Y,Z_2,\dots,Z_n]$. Siguiendo [Kal95, Lemma 4 y Lemma 5], existe un polinomio no nulo $\Upsilon \in K[T_1,\dots,T_n,U_2,\dots,U_n]$ de grado a lo sumo $2\delta^2$ tal que si $\nu_1,\dots,\nu_n,\omega_2,\dots,\omega_n \in \overline{K}$ verifican que

$$\Upsilon(\nu_1,\dots,\nu_n,\omega_2,\dots,\omega_n) \neq 0, \tag{4.2}$$

entonces son válidas las siguientes condiciones:

- el coeficiente principal de χ con respecto a X es un elemento no nulo de $\overline{K}$,
- el discriminante de $\chi(X,0,Z_2,\dots,Z_n)$ con respecto a X es no nulo,
- χ es un elemento irreducible de $\overline{K}[X,Y,Z_2,\dots,Z_n]$.

Asumiendo la condición (4.2), Kaltofen prueba un hecho crucial para su versión efectiva del primer teorema de Bertini [Kal95, Theorem 5]: muestra la existencia de un polinomio $\Psi \in \overline{K}[Z_2,\dots,Z_n]$ de grado a lo sumo $3\delta^4/2-2\delta^3+\delta^2/2$ tal que para cualquier $\eta := (\eta_2,\dots,\eta_n) \in \overline{K}^{n-1}$ con $\Psi(\eta) \neq 0$, el polinomio bivariado $\chi(X,Y,\eta_2,\dots,\eta_n) \in \overline{K}[X,Y]$ es absolutamente irreducible.

Consideremos el polinomio

$$\Xi := \Upsilon(T_1,\dots,T_n,U_2,\dots,U_n)\Psi(Z_2,\dots,Z_n).$$

Es un polinomio en $3n-2$ indeterminadas, con coeficientes en $\overline{K}$, y de grado acotado por $3\delta^4/2-2\delta^3+5\delta^2/2$. Si tomamos una $(3n-2)$–upla

$$(\nu,\omega,\eta) := (\nu_1,\dots,\nu_n,\omega_2,\dots,\omega_n,\eta_2,\dots,\eta_n) \in \overline{K}^{3n-2}$$

que no anula a Ξ, entonces el polinomio

$$\chi(X,Y,\eta_2,\dots,\eta_n) := F(X+\nu_1,\omega_2X+\eta_2Y+\nu_2,\dots,\omega_nX+\eta_nY+\nu_n)$$

es absolutamente irreducible. En particular, si $K=\mathbb{F}_q$ deducimos el siguiente corolario:

Corolario 4.1.2. *Sea* $F \in \mathbb{F}_q[X_1,\ldots,X_n]$ *absolutamente irreducible de grado* δ. *Existen a lo sumo* $(3\delta^4/2-2\delta^3+5\delta^2/2)q^{3n-3}$ *elementos* $(\nu,\omega,\eta) \in \mathbb{F}_q^{3n-2}$ *para los cuales* $\chi(X,Y,\eta)$ *no es absolutamente irreducible.*

Queremos obtener una estimación sobre el grado, similar a la de $\deg\Xi$, de la condición genérica que subyace al hecho que el polinomio $\chi(X,Y,\eta_2,\ldots,\eta_n)$ no tiene factores absolutamente irreducibles de grado a lo sumo D, para $1 \le D \le \delta-1$. El próximo teorema, una variante de [Kal95, Theorem 5], será de suma importancia al momento de obtener las estimaciones.

Teorema 4.1.3. *Sea* $1 \le D \le \delta-1$ *y supongamos que* $\nu_1,\ldots,\nu_n,\omega_2,\ldots,\omega_n$ *satisfacen la condición (4.2). Existe un polinomio no nulo* $\Psi_D \in \overline{K}[Z_2,\ldots,Z_n]$ *de grado*

$$\deg\Psi_D \le D\delta^2(D+1)(D+2) - \frac{1}{8}(D^2+3D)(D^2+3D+2)\delta$$

tal que para cada $\eta := (\eta_2,\ldots,\eta_n) \in \overline{K}^{n-1}$ *con* $\Psi_D(\eta) \ne 0$, *el polinomio*

$$\chi(X,Y,\eta) := f(X+\nu_1, \omega_2 X+\eta_2 Y+\nu_2, \ldots, \omega_n X+\eta_n Y+\nu_n)$$

no tiene factores irreducibles de grado acotado por D *en* $\overline{K}[X,Y]$.

Demostración. Como χ es irreducible over $\overline{K}[Z_2,\ldots,Z_n][X,Y]$, el Lema de Gauss implica que χ es irreducible sobre $\overline{K}(Z_2,\ldots,Z_n)[X,Y]$. Aplicamos el algoritmo *Factorización sobre el cuerpo de coeficientes...* al polinomio

$$\psi := \frac{1}{l}\chi \in \overline{K}(Z_2,\ldots,Z_n)[X,Y],$$

donde $l \in \overline{K}$ es el coeficiente principal de χ con respecto a X. Como $\psi(X,0) \in \overline{K}[X]$, la raíz ζ_i usada para construir el cuerpo $K_i := K(\zeta_i)$ del algoritmo es, en realidad, un elemento de $\overline{K}$ para $1 \le i \le \delta$. Entonces la irreducibilidad de ψ sobre $\overline{K}(Z_2,\ldots,Z_n)[X,Y]$ implica que el sistema lineal (4.1) derivado en el paso L no tiene solución en K_i para $1 \le m \le D$ y $1 \le i \le \delta$. Esto significa que para $m = D$ y $1 \le i \le \delta$, la matriz ampliada del sistema, $\widetilde{M}_D^{(i)}(Z_2,\ldots,Z_n)$, tiene rango mayor que el de la matriz de los coeficientes $M_D^{(i)}(Z_2,\ldots,Z_n)$. Es más, como $\partial\psi(X,0)/\partial X \in \overline{K}$, todos los denominadores utilizados en la construcción de este sistema son elementos de $\overline{K}$. Sea $\Psi_D^{(i)} \in \overline{K}[Z_2,\ldots,Z_n]$ un menor maximal no nulo de la matriz ampliada $\widetilde{M}_D^{(i)}(Z_2,\ldots,Z_n)$ y sea $\eta := (\eta_2,\ldots,\eta_n) \in \overline{K}^{n-1}$ tal que $\prod_{i=1}^{\delta}\Psi_D^{(i)}(\eta) \ne 0$. Entonces el sistema (4.1) no tiene soluciones para $i = 1,\ldots,\delta$, lo que a su vez implica que $\chi(X,Y,\eta_2,\ldots,\eta_n)$ no tiene ningún factor irreducible sobre $\overline{K}[X,Y]$ de grado a lo sumo D, ya que el algoritmo *Factorización sobre el cuerpo de coeficientes...* debería haber calculado tal factor de $\chi(X,Y,\eta)$ sobre $\overline{K}$. El polinomio $\Psi_D := \prod_{i=1}^{\delta}\Psi_D^{(i)}$ es el polinomio que estamos buscando.

Resta aún demostrar la cota de grado para Ψ_D. La demostración sigue esencialmente la demostración de [Kal95, Theorem 5], teniendo en cuenta simplemente que la cantidad de indeterminadas es diferente y que el orden de aproximación también lo es. Cada raíz ζ_i de $\psi(x,0)$ da lugar a un sistema lineal, para $m = D$, que tiene $(D+1)(D+2)/2-1$ indeterminadas. Cualquier menor maximal no nulo $\Psi_D^{(i)}$ satisface la siguiente cota de grado:

$$\begin{aligned}\deg_{Z_2,\ldots,Z_n}\Psi_D^{(i)} &\leq \textstyle\sum_{j=0}^{(D+1)(D+2)/2-1}(\ell_{\text{máx}}-j)\\ &\leq 2D\delta(D+1)(D+2)/2-(D^2+3D)(D^2+3D+2)/8.\end{aligned}$$

Deducimos en forma inmediata la cota de grado para Ψ_D. □

Dado que el Teorema 4.1.3 es válido bajo la condición (4.2), si definimos

$$\Xi_D := \Upsilon(T_1,\ldots,T_n,U_2,\ldots,U_n)\Psi_D(Z_2,\ldots,Z_n),$$

tenemos que Ξ_D es un polinomio en $3n-2$ indeterminadas con coeficientes en $\overline{K}$ de grado acotado por

$$\deg\Xi_D \leq D^3\delta^2-\frac{1}{8}D^4\delta-\frac{3}{4}D^3\delta+3D^2\delta^2-\frac{11}{8}D^2\delta+2D\delta^2-\frac{3}{4}D\delta+2\delta^2,$$

que satisface la siguiente propiedad: para cada $(\nu,\omega,\eta) \in \overline{K}^{3n-2}$ con $\Xi_D(\nu,\omega,\eta) \neq 0$, el polinomio $\chi(X,Y,\eta_2,\ldots,\eta_n)$ no tiene factores irreducibles sobre $\overline{K}$ de grado acotado por D. Nuevamente, considerando $K = \mathbb{F}_q$ tenemos el siguiente corolario:

Corolario 4.1.4. *Sea $F \in \mathbb{F}_q[X_1,\ldots,X_n]$ un polinomio absolutamente irreducible de grado $\delta \geq 2$ y sea D un entero tal que $1 \leq D \leq \delta-1$. Existen a lo sumo $(D^3\delta^2-D^4\delta/8-3D^3\delta/4+3D^2\delta^2-11D^2\delta/8+2D\delta^2-3D\delta/4+2\delta^2)q^{3n-3}$ elementos $(\nu,\omega,\eta) \in \mathbb{F}_q^{3n-2}$ para los cuales $\chi(X,Y,\eta_2,\ldots,\eta_n)$ tiene un factor irreducible sobre $\overline{\mathbb{F}}_q[X,Y]$ de grado acotado por D.*

4.2. Sobre las secciones lineales de dimensión 1 de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible

En esta sección vamos a interpretar los resultados de la sección previa desde un punto de vista geométrico. Consideramos el cuerpo $K := \mathbb{F}_q$ y vamos a pensar a cada $(\nu,\omega,\eta) \in \mathbb{F}_q^{3n-2}$ no nulo como una parametrización de una $\mathbb{F}_q$–variedad lineal de $\mathbb{A}^n$ de dimensión 2.

Sea $F \in \mathbb{F}_q[X_1,\ldots,X_n]$ de grado δ. Si $L \subset \mathbb{A}^n$ es un $\mathbb{F}_q$–plano, vamos a representar la restricción de F a L como un polinomio bivariado $F_L \in \mathbb{F}_q[X,Y]$, donde X,Y son los

parámetros de una parametrización de L, definida sobre $\mathbb{F}_q$. Por supuesto, habría que considerar que ocurre si consideramos otra parametrización de L definida sobre $\mathbb{F}_q$. El polinomio F_L está bien definido salvo un cambio de coordenadas lineales definido sobre $\mathbb{F}_q$. Por lo tanto, tiene sentido referirse al grado de F_L y a la irreducibilidad o irreducibilidad absoluta de F_L; además, el número de componentes absolutamente irreducibles no depende de la parametrización elegida (cf. [Sch76, V.§4]).

En particular, vamos a considerar los $\mathbb{F}_q$–planos de $\mathbb{A}^n$ que se parametrizan del siguiente modo:

$$X_1 = \nu_1 + X, \qquad X_i = \nu_i + \omega_i X + \eta_i Y \quad (2 \leq i \leq n). \tag{4.3}$$

Introducimos algunas notaciones. Por M_T denotamos el conjunto de todos los $\mathbb{F}_q$–planos de $\mathbb{A}^n$ definidas sobre $\mathbb{F}_q$, y por M, el subconjunto formado por los elementos de M_T con una parametrización como en (4.3).

Sea entonces $L \in M$ y consideremos la restricción de F a L, es decir, el polinomio $F_L \in \mathbb{F}_q[X,Y]$. Vamos a denotar por $\nu(L)$ el número de factores absolutamente irreducibles en $\mathbb{F}_q[X,Y]$ de F_L. Observemos que este número verifica $0 \leq \nu(L) \leq \delta - 1$; en el caso en que F es idénticamente 0 sobre L definimos $\nu(L) := q$. Posteriormente, para $0 \leq j \leq \delta$ y $j = q-1$ consideramos los siguientes subconjuntos de M:

$$\Pi_j := \big\{ L \in M : |\nu(L) - 1| = j \big\}.$$

Por lo tanto, si $j \in \{0, 2, \ldots, \delta - 1\}$ y $L \in \Pi_j$, el polinomio F_L tiene $j+1$ factores absolutamente irreducibles en $\mathbb{F}_q[X,Y]$; si $L \in \Pi_1$, el polinomio F_L es relativamente irreducible o tiene 2 factores absolutamente irreducibles en $\mathbb{F}_q[X,Y]$; y, finalmente, Π_{q-1} es el conjunto de planos L para los cuales F_L es idénticamente nulo.

Lo importante es que, cada vez que L pertenezca a Π_j para $j \in \{0, 2, \ldots, \delta - 1\}$, el polinomio F_L tendrá un factor absolutamente irreducible de grado a lo sumo $D_j := \lfloor \delta/(j+1) \rfloor$.

Del Teorema 4.1.3 y del Corolario 4.1.4 deducimos que para cada $L \in M$ con una parametrización dada por (ν, ω, η), con $\Xi_{D_j}(\nu, \omega, \eta) \neq 0$, el polinomio F_L no tiene factores absolutamente irreducibles en $\mathbb{F}_q[X,Y]$ de grado acotado por D_j. En otras palabras, para cada $(\nu, \omega, \eta) \in \mathbb{F}_q^{3n-2}$ con esta propiedad, el polinomio F_L tiene a lo sumo j factores irreducibles sobre $\overline{\mathbb{F}}_q$, lo que en particular implica que $L \notin \Pi_j \cup \cdots \cup \Pi_{\delta-1}$. Tenemos entonces, ligero abuso de notación mediante, que

$$\Pi_j \cup \cdots \cup \Pi_{\delta-1} \subset \{(\nu, \omega, \eta) \in \mathbb{F}_q^{3n-2} : \Xi_{D_j}(\nu, \omega, \eta) = 0\}.$$

Teniendo en cuenta que cada elemento de M tiene $q^3(q-1)$ parametrizaciones (defi-

nidas sobre $\mathbb{F}_q$) del tipo (4.3), de la Proposición 3.1.3 deducimos:

$$|\Pi_j| + \cdots + |\Pi_{\delta-1}| \leq \deg \Xi_{D_j} \frac{q^{3n-3}}{q^3(q-1)}.$$

Por lo tanto, como una consecuencia del Corolario 4.1.4 obtenemos

$$\sum_{k=j}^{\delta-1} |\Pi_k| \leq \left(\delta^5\left(\tfrac{1}{j^3} - \tfrac{1}{8j^4}\right) + 3\delta^4\left(\tfrac{1}{j^2} - \tfrac{1}{4j^3}\right) + \delta^3\left(\tfrac{2}{j} - \tfrac{11}{8j^2}\right) - \tfrac{3}{4}\tfrac{\delta^2}{j} + 2\delta^2\right)\tfrac{q^{3n-6}}{(q-1)}. \tag{4.4}$$

La siguiente proposición es fundamental para nuestras estimaciones sobre la cantidad de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible, ya que nos va a permitir obtener una mejor estimación que la que se obtendría por una aplicación directa del Corolario 4.1.2.

Proposición 4.2.1. *Sea $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ un polinomio absolutamente irreducible de grado δ mayor que 1. Entonces*

$$\sum_{j=1}^{\delta-1} j|(\Pi_j)| \leq (2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}})\frac{q^{3n-3}}{q^3(q-1)}.$$

Demostración. En primer lugar, si $\delta = 2$ la expresión $\sum_{j=1}^{\delta-1} j|(\Pi_j)|$ consiste solo del término $|\Pi_1|$ y, por lo tanto, el Corolario 4.1.2 proporciona la siguiente acotación:

$$|\Pi_1| \leq \left(\frac{3}{2}\delta^4 - 2\delta^3 + \frac{5}{2}\delta^2\right)\frac{q^{3n-6}}{(q-1)} \leq \frac{3}{2}\delta^4\frac{q^{3n-6}}{(q-1)}. \tag{4.5}$$

Supongamos entonces que $\delta \geq 3$. Sea r un número real, que fijaremos luego, en el intervalo abierto $(1, \delta-1)$ y escribamos:

$$\sum_{j=1}^{\delta-1} j|\Pi_j| = \sum_{j=1}^{\lfloor r\rfloor} j|\Pi_j| + \sum_{j=\lfloor r\rfloor+1}^{\delta-1} j|\Pi_j| \leq \lfloor r\rfloor \sum_{j=1}^{\delta-1} |\Pi_j| + \sum_{j=\lfloor r\rfloor+1}^{\delta-1} (j - \lfloor r\rfloor)|\Pi_j|.$$

Del Corolario 4.1.2 tenemos que:

$$\lfloor r\rfloor \sum_{j=1}^{\delta-1} |\Pi_j| \leq r\left(\frac{3}{2}\delta^4 - 2\delta^3 + \frac{5}{2}\delta^2\right)\frac{q^{3n-6}}{(q-1)}. \tag{4.6}$$

Por otro lado, de la desigualdad (4.4) tenemos que:

$$\begin{aligned} \sum_{j=\lfloor r\rfloor+1}^{\delta-1} (j - \lfloor r\rfloor)|\Pi_j| &= \sum_{j=\lfloor r\rfloor+1}^{\delta-1} (|\Pi_j| + \cdots + |\Pi_{\delta-1}|) \\ &\leq (\delta^5 c_1 + 3\delta^4 c_2 + \delta^3 c_3 - \tfrac{3}{4}\delta^2 c_4 + 2\delta^2)\frac{q^{3n-6}}{(q-1)}, \end{aligned} \tag{4.7}$$

donde c_1, c_2, c_3, c_4 son los números siguientes:

$$c_1 := \sum_{j=\lfloor r\rfloor+1}^{\delta-1} \frac{1}{j^3} - \frac{1}{8j^4}, \quad c_2 := \sum_{j=\lfloor r\rfloor+1}^{\delta-1} \frac{1}{j^2} - \frac{1}{4j^3},$$

$$c_3 := \sum_{j=\lfloor r\rfloor+1}^{\delta-1} \frac{2}{j} - \frac{11}{8j^2}, \quad c_4 := \sum_{j=\lfloor r\rfloor+1}^{\delta-1} \frac{1}{j}.$$

Tenemos que acotar estas expresiones convenientemente. Para eso observemos que si g es una función real, positiva y decreciente entonces

$$\sum_{j=\lfloor r\rfloor+1}^{\delta-1} g(j) \leq \int_r^{\delta-1} g(x)dx.$$

También, si $\delta \geq 3$, entonces $1 < \delta/(\delta-1) \leq 3/2$. Ahora, fijando $r := \delta^{\frac{1}{3}}$, aplicamos las acotaciones anteriores y obtenemos las siguientes desigualdades:

$$\begin{aligned}
\delta^5 c_1 &\leq \delta^5 \left(\tfrac{1}{2}(\delta^{\frac{1}{3}})^{-2} - \tfrac{1}{24}(\delta^{\frac{1}{3}})^{-3} - \tfrac{1}{2}(\delta-1)^{-2} + \tfrac{1}{24}(\delta-1)^{-3} \right) \\
&\leq \tfrac{1}{2}\delta^{\frac{13}{3}} - \tfrac{1}{24}\delta^4 - \tfrac{1}{2}\delta^3 + \tfrac{9}{64}\delta^2 \\
3\delta^4 c_2 &\leq 3\delta^4 \left(\delta^{-\frac{1}{3}} - \tfrac{1}{8}(\delta^{\frac{1}{3}})^{-2} - (\delta-1)^{-1} + \tfrac{1}{8}(\delta-1)^{-2} \right) \\
&\leq 3\delta^{\frac{11}{3}} - \tfrac{3}{8}\delta^{\frac{10}{3}} - 3\delta^3 + \tfrac{27}{32}\delta^2 \\
\delta^3 c_3 &\leq \delta^3 (2\ln(\delta-1) + \tfrac{11}{8}(\delta-1)^{-1} - 2\ln\delta^{\frac{1}{3}} - \tfrac{11}{8}\delta^{-\frac{1}{3}}) \\
&\leq \tfrac{4}{3}\delta^3 \ln\delta + \tfrac{33}{16}\delta^2 - \tfrac{11}{8}\delta^{\frac{8}{3}}.
\end{aligned}$$

Deducimos, por lo tanto, la siguiente acotación:

$$\begin{aligned}
&\delta^5 c_1 + 3\delta^4 c_2 + \delta^3 c_3 - \tfrac{3}{4}\delta^2 c_4 + 2\delta^2 \leq \\
&\leq \tfrac{1}{2}\delta^{\frac{13}{3}} - \tfrac{1}{24}\delta^4 + 3\delta^{\frac{11}{3}} - \tfrac{3}{8}\delta^{\frac{10}{3}} + \tfrac{4}{3}\delta^3 \ln\delta - \tfrac{7}{2}\delta^3 - \tfrac{11}{8}\delta^{\frac{8}{3}} + \tfrac{323}{64}\delta^2
\end{aligned} \tag{4.8}$$

Finalmente, de (4.6), (4.7) y (4.8) y de $\frac{4}{3}\delta^3 \ln\delta \leq 3\delta^{3+1/3}$ deducimos que

$$\begin{aligned}
\textstyle\sum_{j=1}^{\delta-1} j|\Pi_j| &\leq 2\delta^{\frac{13}{3}} - \tfrac{1}{24}\delta^4 + 3\delta^{\frac{11}{3}} + \tfrac{5}{8}\delta^{\frac{10}{3}} - \tfrac{7}{2}\delta^3 - \tfrac{11}{8}\delta^{\frac{8}{3}} + \tfrac{5}{2}\delta^{\frac{7}{3}} + \tfrac{323}{64}\delta^2 \\
&\leq 2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}}
\end{aligned}$$

para $\delta \geq 3$. De esta manera demostramos la proposición. □

4.3. Estimaciones para una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible

En esta sección obtenemos diferentes tipos de estimaciones sobre el número de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible. En primer lugar, mostramos una estimación sin regularidad que mejora las estimaciones (1.8) y (1.6). Luego, una estimación que mejora tanto el lado derecho como la condición de regularidad de la cota inferior (1.5), proporcionando al mismo tiempo una cota superior.

Nuestro enfoque combina ideas de [Sch74] y [Sch76] junto con la estimación de la sección previa.

4.3.1. Una estimación sin regularidad

En lo que sigue, utilizaremos el siguiente lema de [Sch74].

Lema 4.3.1. [Sch74, Lemma 5] *Sea* $F \in \mathbb{F}_q[X,Y]$ *un polinomio de grado* $\delta > 0$ *y sea* ν *el número de factores absolutamente irreducibles de* F *definidos sobre* $\mathbb{F}_q$. *Entonces el número* N *de ceros* q*–racionales de* F *satisface la siguiente estimación:*

$$|N - \nu q| \leq \omega(q,\delta) + \delta^2,$$

donde $\omega(q,\delta) := (\delta-1)(\delta-2)q^{1/2} + \delta + 1$.

Sea $F \in \mathbb{F}_q[X_1,\ldots,X_n]$ absolutamente irreducible de grado $\delta > 0$. Recordemos que M_T representa el conjunto de $\mathbb{F}_q$–planos de $\mathbb{A}^n$ y M el conjunto de $\mathbb{F}_q$–planos con una parametrización como en (4.3). Además, para $j \in \{0,2,\ldots,\delta-1\}$, si $L \in \Pi_j$, el polinomio F_L tiene $j+1$ factores absolutamente irreducibles definidos sobre $\mathbb{F}_q$; si $L \in \Pi_1$, el polinomio F_L, o bien es relativamente irreducible, o bien tiene 2 factores absolutamente irreducibles definidos sobre $\mathbb{F}_q$. Finalmente, Π_{q-1} es el conjunto de $\mathbb{F}_q$–planos $L \in M$ para los cuales F_L es idénticamente cero. Introducimos las siguientes cantidades:

$$A := |M|, \qquad B := \sum_{j=1}^{\delta-1} j|\Pi_j|, \qquad C := |\Pi_{q-1}|, \qquad D := |M_T| - |M|.$$

Cada elemento de M se representa por $D' := q^3(q-1)$ parametrizaciones diferentes de tipo (4.3). Teniendo en cuenta que hay $q^{2n-1}(q^{n-1}-1)$ parametrizaciones diferentes de tipo (4.3), concluimos que el cardinal de M es

$$A = \frac{q^{2n-1}(q^{n-1}-1)}{q^3(q-1)}. \tag{4.9}$$

Aplicando la Proposición 4.2.1, tenemos que $B \leq (2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}})\frac{q^{3n-3}}{q^3(q-1)}$, y por lo tanto

$$\frac{B}{A} \leq \left(2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}}\right)\frac{q^{n-2}}{q^{n-1}-1}. \tag{4.10}$$

Argumentando de manera recursiva podemos pensar, sin pérdida de generalidad, que F no puede expresarse como polinomio en $n-2$ variables (ver e.g., [Sch76]). Fijemos $c \in \mathbb{F}_q^{n-2}$ para el cual $F(c, X_{n-1}, X_n)$ es idénticamente cero. Escribimos

$$F = \sum_{\alpha \in \mathcal{J}} f_\alpha X_{n-1}^{\alpha_1} X_n^{\alpha_2},$$

donde $\mathcal{J} \subset \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ es un conjunto finito y $f_\alpha \in \mathbb{F}_q[X_1, \ldots, X_{n-2}]$ para cada $\alpha = (\alpha_1, \alpha_2) \in \mathcal{J}$. Como F no es un elemento de $\mathbb{F}_q[X_1, \ldots, X_{n-2}]$, se sigue que $f_\alpha(c) = 0$ para cada $\alpha \in \mathcal{J}$. La absoluta irreducibilidad de F implica que los polinomios $\{f_\alpha : \alpha \in \mathcal{J}\} \subset \mathbb{F}_q[X_1, \ldots, X_{n-2}]$ no tienen factores en común no triviales en $\overline{\mathbb{F}}_q[X_1, \ldots, X_{n-2}]$ y, en consecuencia, el Lema 3.1.4 implica que existen a lo sumo $\delta^2 q^{n-4}$ elementos $c \in \mathbb{F}_q^{n-2}$ para los cuales $F(c, X_{n-1}, X_n) = 0$; en otrs términos, existen a lo sumo $\delta^2 q^{n-4}$ variedades lineales L de M paralelas a $X_1 = 0, \ldots, X_{n-2} = 0$ para las cuales $F_L = 0$. Si A_0 denota el número de subespacios diferentes de M, repitiendo este argumento para todos los subespacios de M obtenemos

$$\frac{C}{A} \leq \frac{\delta^2 q^{n-4} A_0}{q^{n-2} A_0} = \frac{\delta^2}{q^2}. \tag{4.11}$$

De (4.9) y de

$$|M_T| = \frac{q^n(q^n-1)(q^n-q)}{q^2(q^2-1)(q^2-q)}$$

derivamos una acotación de la proporción D/A:

$$\frac{D}{A} = \frac{1}{A}(|M_T| - A) = \frac{1}{A}\frac{q^n(q^{n-1}-1)(q^{n-1}-q)}{q^2(q^2-1)(q^2-q)} \leq \frac{4}{3q^2}. \tag{4.12}$$

Finalmente, como cada punto $x \in \mathbb{F}_q^n$ está contenido en

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

variedades $L \in M_T$, obtenemos la acotación

$$\frac{A}{E} \leq q^{n-2}. \tag{4.13}$$

Estamos en condiciones de enunciar y probar nuestra estimación sobre la cantidad de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible. Nuestra

estimación es válida para cualquier cuerpo finito $\mathbb{F}_q$, es decir, es válida *sin ninguna condición de regularidad.*

Teorema 4.3.2. *Sea $H \subset \mathbb{A}^n$ una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible de grado δ. Entonces el número de puntos q–racionales $|H(\mathbb{F}_q)|$ de H satisface la siguiente estimación:*

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

Demostración. Sea $F \in \mathbb{F}_q[X_1,\ldots,X_n]$ el polinomio absolutamente irreducible que define H. Como el teorema es cierto si $\delta = 1$ vamos a suponer que $\delta \geq 2$. Escribiendo $N := |H(\mathbb{F}_q)|$ tenemos que

$$\big|N - q^{n-1}\big| \leq \frac{1}{E}\Big(\sum_{L\in\mathcal{M}} |N(F_L) - q| \quad + \sum_{L\in\mathcal{M}_T\setminus\mathcal{M}} |N(F_L) - q|\Big), \tag{4.14}$$

donde el símbolo $N(F_L)$ representa la cantidad de ceros q–racionales del polinomio F_L.

Dado $L \in \Pi_j$ con $j \in \{0,\ldots,\delta-1\}$, el Lema 4.3.1 implica que

$$\big|N(F_L) - q\big| \leq \big|N(F_L) - \nu(L)q\big| + \big|\nu(L) - 1\big|q \leq \omega(q,\delta) + \delta^2 + jq,$$

donde $\nu(L)$ es la cantidad de factores absolutamente irreducibles definidos sobre $\mathbb{F}_q$ del polinomio F_L. Tenemos entonces que

$$\begin{aligned}
\sum_{L\in\mathcal{M}} |N(F_L) - q| &\leq \sum_{j=0}^{\delta-1}\Big(\sum_{L\in\Pi_j} \big(\omega(q,\delta) + \delta^2 + jq\big)\Big) + \sum_{L\in\Pi_{q-1}} (q^2 - q) \\
&\leq \Big(\sum_{j=0}^{\delta-1} |\Pi_j|\Big)\big(\omega(q,\delta) + \delta^2\big) + q\sum_{j=1}^{q-1} j|\Pi_j| \\
&\leq A(\omega(q,\delta) + \delta^2) + Bq + Cq(q-1).
\end{aligned}$$

Reemplazando en (4.14), de (4.10), (4.11), (4.12), (4.13) obtenemos para $\delta \geq 3$:

$$\begin{aligned}
|N - q^{n-1}| &\leq \tfrac{1}{E}\big(A(\omega(q,\delta) + \delta^2) + Bq + Cq(q-1) + Dq^2\big) \\
&\leq \tfrac{A}{E}\big(\omega(q,\delta) + \delta^2 + \tfrac{B}{A}q + \tfrac{C}{A}q(q-1) + \tfrac{D}{A}q^2\big) \\
&\leq q^{n-2}\Big(\omega(q,\delta) + \delta^2 + (2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}})\tfrac{4}{3} + \delta^2 + \tfrac{4}{3}\Big) \\
&\leq (\delta-1)(\delta-2)q^{n-3/2} + 5\delta^{\frac{13}{3}} q^{n-2}.
\end{aligned} \tag{4.15}$$

Si $\delta = 2$, combinando (4.14) con la acotación (4.5) de la demostración de la Proposición

4.2.1, obtenemos

$$\begin{aligned} |N - q^{n-1}| &\leq q^{n-2}\left(\omega(q,\delta) + \delta^2 + (\tfrac{3}{2}\delta^4 - 2\delta^3 + \tfrac{5}{2}\delta^2)\tfrac{4}{3} + \delta^2 + \tfrac{4}{3}\right) \\ &\leq (\delta-1)(\delta-2)q^{n-3/2} + (2\delta^4 + 3\delta)q^{n-2} \qquad (4.16) \\ &\leq (\delta-1)(\delta-2)q^{n-3/2} + 5\delta^{\frac{13}{3}}q^{n-2}. \end{aligned}$$

□

Con nuestra estimación mejoramos la estimación de [HW98]

$$\left||H(\mathbb{F}_q)| - q^{n-1}\right| \leq (\delta-1)(\delta-2)q^{n-3/2} + (2\delta^5 + \delta^2)q^{n-2} + 2\delta^7 q^{n-5/2},$$

válida solo para $q > cn^3\delta^5 \log^3 \delta$, y también mejoramos la estimación de [GL02a], [GL02b] que, en el caso de una hipersuperficie, toma la forma

$$\left||H(\mathbb{F}_q)| - q^{n-1}\right| \leq (\delta-1)(\delta-2)q^{n-3/2} + 12(\delta+3)^{n+1}q^{n-2}.$$

Por otro lado, cabe mencionar que en [CR96, Theorem 3.2 and 3.4]), los autores muestran que para un polinomio $F \in \mathbb{F}_q[X_1,\ldots,X_n]$ de grado $\delta > 1$, que define una $\mathbb{F}_q$–hipersuperficie H, son válidas las siguientes afirmaciones sobre el conjunto de puntos q–racionales $H(\mathbb{F}_q)$ para q suficientemente grande:

(i) si F es absolutamente irreducible entonces $|H(\mathbb{F}_q)| < \delta q^{n-1} - (\delta-1)q^{n-2}$,

(ii) si F tiene un factor no lineal absolutamente irreducible definido sobre $\mathbb{F}_q$, entonces $|H(\mathbb{F}_q)| < \delta q^{n-1} - (\delta-1)q^{n-2}$.

Se interrogan por la posibilidad de extender la validez de las afirmaciones anteriores a todo q. Si bien no damos una respuesta a la inquietud planteada, nuestras estimaciones proveen valores explícitos $q_0 = q_0(\delta)$ y $q_1 = q_1(\delta)$ tales que (i) vale para $q \geq q_0$ y (ii) para $q \geq q_1$. De hecho, el Teorema 4.3.2 implica que podemos elegir $q_0 := 13\delta^{\frac{10}{3}}$ y $q_1 := 9\delta^{\frac{13}{3}}$.

4.3.2. Una estimación con regularidad

En esta sección vamos a exhibir una estimación sobre el número de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible que mejora la del Teorema 4.3.2, aunque es válida bajo una cierta condición de regularidad. Por supuesto, invocamos las notaciones utilizadas a lo largo de este capítulo.

Teorema 4.3.3. *Sea $H \subset \mathbb{A}^n$ una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible de grado δ. Si $q > 15\delta^{\frac{13}{3}}$ el número de puntos q–racionales $|H(\mathbb{F}_q)|$ satisface la siguiente*

estimación:

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

Demostración. Como antes, como el teorema es cierto para $\delta=1$, podemos asumir sin pérdida de generalidad que $\delta \ge 2$.

Para un plano $L \in \Pi_j$ $(j>0)$, del Lema 4.3.1 tenemos que $\big|N(F_L)-q\big| < jq+\omega(q,\delta)+\delta^2$. Por lo tanto,

$$\begin{aligned}\big|N(F_L)-Nq^{2-n}\big| &\ge \big|N(F_L)-q\big|-q^{2-n}\big|N-q^{n-1}\big| \\ &\ge jq-\omega(q,\delta)-\delta^2-\omega(q,\delta)-5\delta^{\frac{13}{3}} \\ &\ge \tfrac{1}{2}jq,\end{aligned}$$

donde la última desigualdad es válida si y solo si $\frac{1}{2}jq \ge 2q^{1/2}(\delta-1)(\delta-2)+2(\delta+1)+\delta^2+5\delta^{\frac{13}{3}}$. Y la validez de esta última se desprende de la condición sobre q.

Aplicando [Sch74, Lemma 6] tenemos que $\frac{1}{4}q^2\sum_{j=1}^{q-1} j^2|\Pi_j| \le \delta E q^{n-1}$, y luego que $\sum_{j=1}^{q-1} j|\Pi_j| \le 4\delta E q^{n-3}$. Entonces

$$\begin{aligned}\big|N-q^{n-1}\big| &= \tfrac{1}{E}\big|\textstyle\sum_{L\in M_T^{(2)}}\big(N(F_L)-q\big)\big| \le \tfrac{1}{E}\sum_{L\in M_T^{(2)}}\big|(N(F_L)-q)\big| \\ &\le \tfrac{1}{E}\Big((A+D)\big(\omega(q,\delta)+\delta^2\big)+\textstyle\sum_{j=1}^{q-1}2jq|\Pi_j|\Big) \\ &\le q^{n-2}\big(\omega(q,\delta)+\delta^2+8\delta\big) \\ &\le q^{n-2}\big(\omega(q,\delta)+5\delta^2\big).\end{aligned}$$

□

De esta estimación deducimos inmediatamente una cota inferior no trivial sobre la cantidad de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible.

Corolario 4.3.4. *Sea H una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible de grado δ. Si $q > 15\delta^{13/3}$ el número de puntos q–racionales $|H(\mathbb{F}_q)|$ satisface la siguiente cota inferior no trivial:*

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

Nuestra estimación mejora significativamente la condición de regularidad de [Sch74] (la que presentamos en (1.5)) $q > 10^4 n^3\delta^5\vartheta^3([4\log\delta])$ y, al mismo tiempo, provee una cota superior, no proporcionada en [Sch74].

En el contexto de la resolución de ecuaciones polinomiales sobre cuerpos finitos, es preciso disponer de cotas inferiores sobre el número de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible H, como las de los Teoremas 4.3.2 y 4.3.3 o la de [Sch74], ya que permiten establecer condiciones sobre la existencia de un pun-

to q–racional de una hipersuperficie H. De hecho, de [Sch74] se deduce que una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible de grado δ tiene un punto q–racional si $q > 10^4 n^3 \delta^5 \vartheta^3([4\log\delta])$. Del Teorema 4.3.2 vemos que esta condición puede mejorarse a $q > 9\delta^{\frac{13}{3}}$. Sin embargo, un argumento sencillo permite mejorar significativamente esta condición de regularidad:

Teorema 4.3.5. *Sea* H *una* $\mathbb{F}_q$*–hipersuperficie absolutamente irreducible de grado* δ*. Si* $q > 2\delta^4$ *entonces* H *tiene un punto* q*–racional.*

Demostración. Sea $F \in \mathbb{F}_q[X_1,\dots,X_n]$ el polinomio absolutamente irreducible que define H. Dado que $q > 2\delta^4$, del Corolario 4.1.2 concluimos que existe $(\nu,\omega,\eta) \in \mathbb{F}_q^{3n-2}$ para el cual $\chi(X,Y) := F(X+\nu_1, \omega_2 X+\eta_2 Y+\nu_2,\dots,\omega_n X+\eta_n Y+\nu_n)$ es absolutamente irreducible de grado δ. La estimación (1.2) muestra que χ tiene al menos $q-(\delta-1)(\delta-2)q^{\frac{1}{2}}-\delta-1$ ceros q–racionales. Para $q > 2\delta^4$ la cantidad anterior es un número estrictamente positivo, y por lo tanto χ tiene al menos un cero q–racional, que da lugar a un puntoq–racional de H. □

Finalmente, observemos que, en el caso en que la característica de $\mathbb{F}_q$ es suficientemente grande, las estimaciones de los Teoremas 4.3.2 y 4.3.3 pueden mejorarse, utilizando una versión efectiva del primer teorema de Bertini debida a S. Gao [Gao03]. De [Gao03, Theorem 5.1] deducimos el siguiente resultado:

Corolario 4.3.6. *Sea* $\mathbb{F}_q$ *un cuerpo finito de característica mayor que* $2\delta^2$*. Sea* $F \in \mathbb{F}_q[X_1,\dots,X_n]$ *un polinomio absolutamente irreducible de grado* $\delta > 1$*. Existen a lo sumo* $\frac{3}{2}\delta^3 \frac{q^{3n-3}}{q^3(q-1)}$ $\mathbb{F}_q$*–planos* $L \subset \mathbb{A}^n$ *(con parametrizaciones como en (4.3)) tales que la restricción* f_L *es un polinomio absolutamente irreducible.*

Con las notaciones de la Sección 4.3.1, del Corolario 4.3.6 obtenemos

$$\frac{B}{A} := \frac{1}{A}\sum_{j=1}^{\delta-1} j|\Pi_j| \le \frac{\delta}{A}\sum_{j=1}^{\delta-1}|\Pi_j| \le \frac{3}{2}\frac{\delta^4}{A}\frac{q^{3n-3}}{q^3(q-1)} \le \frac{3}{2}\delta^4\frac{q^{n-2}}{q^{n-1}-1}.$$

Combinando esta acotación para la proporción B/A con (4.15) de la demostración del Teorema 4.3.2, obtenemos la siguiente estimación sobre el número $|H(\mathbb{F}_q)|$ de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible $H \subset \mathbb{A}^n$ de grado δ:

$$\left||H(\mathbb{F}_q)| - q^{n-1}\right| \le (\delta-1)(\delta-2)q^{n-3/2} + 3\delta^4 q^{n-2}.$$

A su vez, repitiendo el procedimiento de la demostración del Teorema 4.3.3, es decir, reemplazando en esa demostración, la cota inferior que se obtiene del Teorema 4.3.2 por la estimación anterior, obtenemos para $q > 27\delta^4$:

$$\left||H(\mathbb{F}_q)| - q^{n-1}\right| \le (\delta-1)(\delta-2)q^{n-3/2} + (5\delta^2+\delta+1)q^{n-2}.$$

En suma, podemos enunciar el siguiente corolario:

Corolario 4.3.7. *Sea $\mathbb{F}_q$ un cuerpo finito de característica mayor que $2\delta^2$, y sea $H \subset \mathbb{A}^n$ una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible de grado $\delta > 1$. Entonces*

$$\big||H(\mathbb{F}_q)| - q^{n-1}\big| \leq (\delta-1)(\delta-2)q^{n-3/2} + 3\delta^4 q^{n-2}.$$

Además, si $q > 27\delta^4$, entonces

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

Estas estimaciones mejoran las de los Teoremas 4.3.2 y 4.3.3 para característica mayor que $2\delta^2$, pero no mejoran el resultado de existencia del Teorema 4.3.5. De hecho, el Corolario 4.3.7 no provee una cota inferior no trivial sobre la cantidad de puntos q–racionales de H para $q \leq 4\delta^4$. Teniendo en cuenta que estimaciones como las de los Teoremas 4.3.2 y 4.3.3 y Corolario 4.3.7 no proporcionan cotas inferiores no triviales para $q \leq (\delta-1)^2(\delta-2)^2$, podemos afirmar que nuestro resultado de existencia del Teorema 4.3.5 se aproxima a este valor óptimo.

4.4. Una estimación para una $\mathbb{F}_q$–hipersuperficie arbitraria

Concluimos el capítulo con una estimación sobre la cantidad de puntos q–racionales de una $\mathbb{F}_q$–hipersuperficie arbitraria. La estimación se expresará en términos de la cantidad de componentes absolutamente irreducibles definidas sobre $\mathbb{F}_q$.

Dada una $\mathbb{F}_q$–hipersuperficie H arbitraria de grado δ consideramos la descomposición de H en componentes $\mathbb{F}_q$–irreducibles:

$$H = H_1 \cup \cdots H_\sigma \cup H_{\sigma+1} \cup \cdots \cup H_m.$$

El ordenamiento propuesto responde al criterio siguiente:

1. las componentes $H_1, \ldots, H_\sigma$ son absolutamente irreducibles;
2. las componentes $H_{\sigma+1}, \ldots, H_m$ son relativamente irreducibles.

La idea en que se basa la estimación es que solo las componentes $H_1, \ldots, H_\sigma$ son relevantes a los fines de estimar $|H(\mathbb{F}_q)|$.

Denotemos por δ_i el grado de cada una de las componentes $H_1, \ldots, H_m$, sea $\Delta := \sum_{i=1}^{\sigma} \delta_i$ y recordemos que $\delta = \sum_{i=1}^{m} \delta_i$.

Teorema 4.4.1. *El número de puntos q–racionales $|H(\mathbb{F}_q)|$ de la $\mathbb{F}_q$–hipersuperficie H verifica la siguiente estimación:*

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

donde $\operatorname{sign}(\sigma) := 0$ *para* $\sigma = 0$ *y* $\operatorname{sign}(\sigma) := 1$ *en caso contrario.*

Demostración. Escribimos $N := |H(\mathbb{F}_q)|$ y $N_i := |H_i(\mathbb{F}_q)|$ para $1 \leq i \leq m$. Podemos expresar la diferencia $\left|N - \sigma q^{n-1}\right|$ del siguiente modo:

$$\left|N - \sigma q^{n-1}\right| \leq \left|N - \sum_{i=1}^{\sigma} N_i\right| + \sum_{i=1}^{\sigma} \left|N_i - q^{n-1}\right|.$$

Para cada $\sigma + 1 \leq i \leq m$, la $\mathbb{F}_q$–hipersuperficie H_i es relativamente irreducible. Por lo tanto, la Proposición 3.1.5 implica que

$$N - \sum_{i=1}^{\sigma} N_i \leq \sum_{i=\sigma+1}^{m} N_i < q^{n-2} \sum_{i=\sigma+1}^{m} \delta_i^2/4 \leq q^{n-2}\delta^2/4. \tag{4.17}$$

Por otro lado,

$$\sum_{i=1}^{\sigma} N_i - N \leq \sum_{1 \leq i < j \leq \sigma} |H_i \cap H_j(\mathbb{F}_q)| \leq q^{n-2} \sum_{1 \leq i < j \leq \sigma} \delta_i \delta_j \leq q^{n-2}\delta^2/2. \tag{4.18}$$

De (4.17) y (4.18) obtenemos:

$$\left|N - \sum_{i=1}^{\sigma} N_i\right| \leq q^{n-2}\delta^2/2. \tag{4.19}$$

Para cada $1 \leq i \leq \sigma$, la $\mathbb{F}_q$–hipersuperficie $H_i \subset \mathbb{A}^n$ es absolutamente irreducible. Podemos aplicar el Teorema 4.3.2 y concluir que:

$$\begin{aligned} \sum_{i=1}^{\sigma} \left|N_i - q^{n-1}\right| &\leq q^{n-2} \sum_{i=1}^{\sigma} \left((\delta_i - 1)(\delta_i - 2)q^{1/2} + 5\delta_i^{\frac{13}{3}}\right) \\ &\leq \operatorname{sign}(\sigma)(\Delta - 1)(\Delta - 2)q^{n-\frac{3}{2}} + 5\Delta^{\frac{13}{3}} q^{n-2}. \end{aligned}$$

Terminamos la demostración combinando las dos estimaciones obtenidas. □

Tenemos que señalar que si las componentes $\mathbb{F}_q$–irreducibles de la hipersuperficie H son relativamente irreducibles, la estimación que acabamos de dar se reduce esencialmente a la cota superior proporcionada por la Proposición 3.1.5. Señalemos también que el método empleado en esta sección será retomado cuando estimemos la cantidad de puntos q–racionales de una $\mathbb{F}_q$–variedad arbitraria (cf. Teorema 5.3.1).

5 Estimaciones para variedades afines

Una variedad V absolutamente irreducible de dimensión r en el espacio de dimensión n es birracionalmente equivalente a una hipersuperficie H, absolutamente irreducible, en el espacio de dimensión $r+1$. Este hecho es el que nos permite estimar la cantidad de puntos q–racionales de una $\mathbb{F}_q$–variedad absolutamente irreducible V, a partir de estimar los de una $\mathbb{F}_q$–hipersuperficie H absolutamente irreducible. Para eso, obtenemos condiciones de regularidad bajo las cuales existe una $\mathbb{F}_q$–hipersuperficie birracionalmente equivalente a la $\mathbb{F}_q$–variedad dada.

5.1. Reducción a una hipersuperficie

Consideremos una $\mathbb{F}_q$–variedad $V \subset \mathbb{A}^n$ equidimensional de dimensión r y grado δ. Nuestros próximos resultados establecen condiciones para que una proyección lineal genérica $\pi : V \to \mathbb{A}^{r+1}$, definida por formas lineales definidas sobre $\mathbb{F}_q$, induzca un morfismo birracional con inversa $\mathbb{F}_q$–definible. Este hecho nos permitirá extender las estimaciones sobre la cantidad de puntos q–racionales de una hipersuperficie absolutamente irreducible al caso de una variedad absolutamente irreducible.

Sea $\Lambda := (\Lambda_{ij})_{1\le i\le r+1, 1\le j\le n}$ una matriz de indeterminadas de $(r+1)\times n$ y para cada $1 \le i \le r+1$ denotemos por $\Lambda^{(i)} := (\Lambda_{i,1}, \ldots, \Lambda_{i,n})$ la i–ésima fila de Λ. Sea $\Gamma := (\Gamma_1, \ldots, \Gamma_{r+1})$ un vector de indeterminadas y definamos $\widetilde{Y} := \Lambda X + \Gamma$.

Proposición 5.1.1. *Existe un polinomio no nulo $A \in \overline{\mathbb{F}}_q[\Lambda, \Gamma]$ de grado a lo sumo $2(r+1)\delta^2$ tal que para cada $(\lambda, \gamma) \in \mathbb{A}^{(r+1)(n+1)}$ con $A(\lambda, \gamma) \neq 0$, definiendo las formas lineales $Y := \lambda X + \gamma := (Y_1, \ldots, Y_{r+1})$, se verifican las siguientes condiciones:*

(i) *La extensión de anillos $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$ es una extensión entera.*

(ii) *La forma lineal Y_{r+1} induce un elemento primitivo de la extensión entera de anillos $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$; esto es, el grado de la ecuación de dependencia entera minimal de Y_{r+1} sobre $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$ es igual al rango de $\overline{\mathbb{F}}_q[V]$ como $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$–módulo libre.*

Demostración. Consideremos la forma de Chow $P_V \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{r+1}]$ de la variedad V. Recordemos que verifica las siguientes cotas de grado:

- $\deg_{\widetilde{Y}_1, \ldots, \widetilde{Y}_{r+1}} P_V = \deg_{\widetilde{Y}_{r+1}} P_V = \delta$,

- $\deg_{\Lambda^{(i)},\Gamma_i} P_V \leq \delta$ for $1 \leq i \leq r+1$.

De la Proposición 3.3.1, deducimos que existe $A_1 \in \overline{\mathbb{F}}_q[\Lambda,\Gamma]$ de grado acotado por $r\delta$ tal que si $(\lambda,\gamma) \in \mathbb{A}^{(r+1)(n+1)}$ no anula a $A_1(\lambda,\gamma) \neq 0$, la extensión de anillos $\overline{\mathbb{F}}_q[Y_1,\ldots,Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$ es entera.

La forma de Chow P_V es un elemento separable de $\overline{\mathbb{F}}_q(\Lambda,\Gamma,\widetilde{Y}_1,\ldots,\widetilde{Y}_r)[\widetilde{Y}_{r+1}]$, con lo cual P_V y $\partial P_V/\partial\widetilde{Y}_{r+1}$ son coprimos en $\overline{\mathbb{F}}_q(\Lambda,\Gamma,\widetilde{Y}_1,\ldots,\widetilde{Y}_r)[\widetilde{Y}_{r+1}]$ y, por ende, el discriminante

$$\rho := \operatorname{Res}_{\widetilde{Y}_{r+1}}(P_V, \partial P_V/\partial\widetilde{Y}_{r+1})$$

de P_V con respecto a $\widetilde{Y}_{r+1}$ es un elemento no nulo de $\overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}_1,\ldots,\widetilde{Y}_r]$ que verifica las siguientes cotas de grado:

- $\deg_{\widetilde{Y}_1,\ldots,\widetilde{Y}_r} \rho \leq (2\delta-1)\delta$,
- $\deg_{\Lambda^{(i)},\Gamma_i} \rho \leq (2\delta-1)\delta$ para $1 \leq i \leq r+1$.

Sea $\rho_1 \in \overline{\mathbb{F}}_q[\Lambda,\Gamma]$ un coeficiente no nulo de un monomio de ρ, considerando ρ como un elemento de $\overline{\mathbb{F}}_q[\Lambda,\Gamma][\widetilde{Y}_1,\ldots,\widetilde{Y}_r]$. Definimos entonces el polinomio $A \in \overline{\mathbb{F}}_q[\Lambda,\Gamma]$, del enunciado de la Proposición, como $A := A_1\rho_1$. Es claro que el grado de A está acotado por $2(r+1)\delta^2$.

Tomemos entonces un elemento cualquiera $(\lambda,\gamma) \in \mathbb{A}^{(r+1)(n+1)}$ que no anule al polinomio A, y denotemos por $(\lambda^*,\gamma^*) \in \mathbb{A}^{r(n+1)}$ la matriz formada por las primeras r filas de (λ,γ). Para simplificar la escritura vamos a considerar los polinomios P_V^* y ρ^*, obtenidos a partir de P_V y ρ evaluando las indeterminadas $\Lambda^{(1)},\ldots,\Lambda^{(r)},\Gamma_1,\ldots,\Gamma_r$ en (λ^*,γ^*). De esta manera, ρ^* es un polinomio no nulo de $\overline{\mathbb{F}}_q[\Lambda^{(r+1)},\Gamma_{r+1},Y_1,\ldots,Y_r]$ que coincide con el discriminante de $P_V^*(\Lambda^{(r+1)},\Gamma_{r+1},Y_1,\ldots,Y_r,\widetilde{Y}_{r+1})$ con respecto a $\widetilde{Y}_{r+1}$.

Si $\xi_1,\ldots,\xi_n \in \overline{\mathbb{F}}_q[V]$ son las clases inducidos por $X_1,\ldots,X_n$, definimos r elementos de $\overline{\mathbb{F}}_q[V]$ (las clases de las formas lineales $Y_1,\ldots,Y_r$) como $\zeta_i := \sum_{j=1}^n \lambda_{i,j}\xi_j$. Introducimos además la indeterminada $\widehat{Y}_{r+1} := \sum_{j=1}^n \Lambda_{r+1,j}\xi_j$. De las propiedades de la forma de Chow de V presentadas en la Sección 2.3 deducimos que para cada $1 \leq k \leq n$, la identidad

$$\begin{aligned}(\partial P_V^*/\partial\widetilde{Y}_{r+1})(\Lambda^{(r+1)},\Gamma_{r+1},\zeta_1,\ldots,\zeta_r,\widehat{Y}_{r+1})\xi_k + \\ +(\partial P_V^*/\partial\Lambda_{r+1,k})(\Lambda^{(r+1)},\Gamma_{r+1},\zeta_1,\ldots,\zeta_r,\widehat{Y}_{r+1}) = 0\end{aligned} \tag{5.1}$$

es válida en $\overline{\mathbb{F}}_q[\Lambda^{(r+1)},\Gamma_{r+1}] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$.

El discriminante ρ^* puede expresarse como una combinación polinomial entre P_V^* y $\partial P_V^*/\partial\widetilde{Y}_{r+1}$. De (5.1) deducimos la existencia de n polinomios no nulos $P_1,\ldots,P_n \in \overline{\mathbb{F}}_q[\Lambda^{(r+1)},\Gamma_{r+1},Z_1,\ldots,Z_{r+1}]$, para los cuales se satisfacen las n identidades

$$\rho^*(\Lambda^{(r+1)},\Gamma_{r+1},\zeta_1,\ldots,\zeta_r)\xi_k + P_k(\Lambda^{(r+1)},\Gamma_{r+1},\zeta_1,\ldots,\zeta_r,\widehat{Y}_{r+1}) = 0. \tag{5.2}$$

Reemplazando en cada una de las n identidades (5.2) $\Lambda^{(r+1)}$ y Γ_{r+1} por $\lambda^{(r+1)}$ y γ_{r+1}, respectivamente, concluimos que Y_{r+1} induce un elemento primitivo de la extensión de $\overline{\mathbb{F}}_q$–álgebras $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$.

Observemos que $\overline{\mathbb{F}}_q[V]$ es un $\overline{\mathbb{F}}_q[Y_1,\dots,Y_r]$–módulo libre de rango (finito) igual a la dimensión del $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r)$–espacio vectorial de $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$. Por otro lado, dado que $\overline{\mathbb{F}}_q[Y_1,\dots,Y_r]$ es integralmente cerrado tenemos que la ecuación minimal sobre $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r)$ de un elemento $\xi \in \overline{\mathbb{F}}_q[V]$ es igual a la ecuación minimal de dependencia entera de ξ sobre $\overline{\mathbb{F}}_q[Y_1,\dots,Y_r]$ (ver [Kun85, Lemma II.2.15]). Combinando esta observación con el hecho que Y_{r+1} induce un elemento primitivo de la extensión de $\overline{\mathbb{F}}_q$–álgebras $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$ concluimos que Y_{r+1} también induce un elemento primitivo de la extensión de $\overline{\mathbb{F}}_q$–álgebras $\overline{\mathbb{F}}_q[Y_1,\dots,Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$. Esto muestra la condición (iii). □

Elijamos $(\lambda,\gamma) \in \mathbb{A}^{(r+1)(n+1)}$ que no anule al polinomio A obtenido en la Proposición 5.1.1 y sean $Y = (Y_1,\dots,Y_{r+1}) := \lambda Y + \gamma$ las consecuentes $r+1$ formas lineales. Lo relevante de la Proposición 5.1.1 es que, bajo estas condiciones, expresa que la $\mathbb{F}_q$–variedad V es birracionalmente equivalente a una $\overline{\mathbb{F}}_q$–hipersuperficie $W \subset \mathbb{A}^{r+1}$ de grado δ: la imagen de V bajo la proyección definida por las formas lineales $Y_1,\dots,Y_{r+1}$. Es decir, la elección de $Y_1,\dots,Y_{r+1}$ implica que si escribimos

$$\begin{array}{rccl} \pi & : & V & \to & \mathbb{A}^{r+1} \\ & & x & \mapsto & \big(Y_1(x),\dots,Y_{r+1}(x)\big), \end{array}$$

la imagen $W := \overline{\pi(V)}$ es una hipersuperficie de $\mathbb{A}^{r+1}$de grado δ, definida por un polinomio $m \in \overline{\mathbb{F}}_q[Y_1,\dots,Y_{r+1}]$ separable y mónico en Y_{r+1} de grado $\deg m = \deg_{Y_{r+1}} m = \delta$ (observemos que este polinomio se obtiene a partir de la forma de Chow y resulta ser la ecuación minimal de Y_{r+1} en la extensión entera de anillos $\overline{\mathbb{F}}_q[Y_1,\dots,Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$).

Nuestro próximo resultado muestra, no solo que la variedad V es birracionalmente equivalente a la hipersuperficie W sino que, además, caracteriza los abiertos isomorfos. Para eso, definimos las siguientes subvariedades $V_1 \subset \mathbb{A}^n$ y $W_1 \subset \mathbb{A}^{r+1}$:

$$V_1 := \left\{ x \in \mathbb{A}^n : \frac{\partial m}{\partial Y_{r+1}}(Y_1(x),\dots,Y_{r+1}(x)) = 0 \right\},$$

$$W_1 := \left\{ y \in \mathbb{A}^{r+1} : \frac{\partial m}{\partial Y_{r+1}}(y) = 0 \right\}.$$

Proposición 5.1.2. *$\pi|_{V\setminus V_1} : V\setminus V_1 \to W\setminus W_1$ es un isomorfismo de abiertos Zariski.*

Demostración. Como $\pi(V\setminus V_1) \subset W\setminus W_1$, el morfismo $\pi|_{V\setminus V_1} : V\setminus V_1 \to W\setminus W_1$ está bien definido.

Mostramos en primer lugar que π es inyectivo. Notemos que, especializando la identi-

dad (5.1) de la demostración de la Proposición 5.1.1 en $\Lambda^{(r+1)} = \lambda^{(r+1)}$ y $\Gamma_{r+1} = \gamma_{r+1}$, obtenemos los polinomios $\nu_1, \ldots, \nu_n \in \overline{\mathbb{F}}_q[Y_1, \ldots, Y_{r+1}]$ de (2.5) junto con las correspondientes n identidades

$$\nu_i(Y_1, \ldots, Y_{r+1}) - X_i \cdot \frac{\partial m}{\partial Y_{r+1}}(Y_1, \ldots, Y_{r+1}) \equiv 0 \bmod I(V) \ . \tag{5.3}$$

Sean $x := (x_1, \ldots, x_n), x' := (x'_1, \ldots, x'_n) \in V \setminus V_1$ tales que $\pi(x) = \pi(x')$. Tenemos entonces que $Y_i(x) = Y_i(x')$ para $1 \leq i \leq r+1$. Por lo tanto, dado que $(\partial q/\partial Y_{r+1})(y) \neq 0$, de (5.3) observamos que $x_i = x'_i$ para $1 \leq i \leq n$; es decir, π es inyectivo.

Mostramos ahora que $\pi|_{V \setminus V_1} : V \setminus V_1 \to W \setminus W_1$ es suryectivo. Escribamos $m_0 := \partial m/\partial Y_{r+1}$, sea $y := (y_1, \ldots, y_{r+1})$ un punto de $W \setminus W_1$, y consideremos el elemento de $\mathbb{A}^n$

$$x := \left(\frac{\nu_1}{m_0}(y), \ldots, \frac{\nu_n}{m_0}(y) \right).$$

Tenemos que probar que x pertenece a $V \setminus V_1$. Para eso, sea f un elemento cualquiera del ideal $I(V)$ y consideremos el polinomio $\tilde{f} := (m_0(Y_1, \ldots, Y_{r+1}))^N f$, con $N := \deg f$. Pensando a $\tilde{f}$ como un polinomio en $n+1$ indeterminadas, es fácil ver que existe $g \in \mathbb{F}_q[T_1, \ldots, T_{n+1}]$ tal que $\tilde{f} = g(m_0 X_1, \ldots, m_0 X_n, m_0)$; además, $\tilde{f} \in I(V)$, con lo cual $\tilde{f}(z) = 0$ para todo $z \in V$ y, por lo tanto, de (5.3) concluimos que

$$g(\nu_1, \ldots, \nu_n, m_0)\big(Y_1(z), \ldots, Y_{r+1}(z)\big) = 0.$$

En particular, m divide a $\hat{f} := g(\nu_1, \ldots, \nu_n, m_0)$ en $\mathbb{F}_q[Y_1, \ldots, Y_{r+1}]$ y por lo tanto $\hat{f}(y) = m_0(y)^N f(x) = 0$. Teniendo en cuenta que $m_0(y) \neq 0$ concluimos que $f(x) = 0$, es decir, $x \in V \setminus V_1$.

Para completar la demostración de la suryectividad de π resta probar que $\pi(x) = y$. Observemos que la identidad (5.3) muestra que cualquier $z \in V$ verifica

$$Y_i(z) m_0\big(Y_1(z), \ldots, Y_{r+1}(z)\big) - \sum_{j=1}^{n} \lambda_{i,j} \nu_j\big(Y_1(z), \ldots, Y_{r+1}(z)\big) = 0$$

para $1 \leq i \leq r+1$. Como antes, esto implica que m divide al polinomio $Y_i m_0 - \sum_{j=1}^{n} \lambda_{i,j} \nu_j$ en $\mathbb{F}_q[Y_1, \ldots Y_{r+1}]$, lo que a su vez muestra que

$$y_i = \sum_{j=1}^{n} \lambda_{i,j} (\nu_j/m_0)(y) = \sum_{j=1}^{n} \lambda_{i,j} x_j$$

para $1 \leq i \leq r+1$. De esta forma, mostramos que $\pi(x) = y$.

Para terminar, probamos que $\pi|_{V\setminus V_1} : V\setminus V_1 \to W\setminus W_1$ es un isomorfismo. Sea

$$\begin{array}{rccl} \phi & : & W\setminus W_1 & \to & V\setminus V_1 \\ & & y & \mapsto & \left(\dfrac{\nu_1}{m_0}(y),\ldots,\dfrac{\nu_n}{m_0}(y)\right). \end{array}$$

Nuestras argumentaciones muestran que ϕ está bien definido y que $\pi\circ\phi$ es la identidad de $W\setminus W_1$.

□

Nuestra meta es estimar la cantidad de puntos q–racionales de V a partir de la estimación para los puntos q–racionales de la hipersuperficie W; pero para obtener estas estimaciones, es preciso que W sea una $\mathbb{F}_q$– hipersuperficie. En tanto las formas lineales $Y_1,\ldots,Y_{r+1}$ pertenezcan a $\mathbb{F}_q[X_1,\ldots,X_n]$, W será una $\mathbb{F}_q$–hipersuperficie. De esta manera, trasladamos la cuestión a un enunciado de existencia de un punto q–racional (λ,γ) que no anule a un polinomio: el polinomio A obtenido en la Proposición 5.1.1. Dicha proposición nos facilita una condición de la regularidad para que los resultados anteriores sean válidos sobre $\mathbb{F}_q$.

Teorema 5.1.3. *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$–variedad equidimensional de dimensión r y grado δ. Si $q > 2(r+1)\delta^2$ existen formas lineales $Y_1,\ldots,Y_{r+1} \in \mathbb{F}_q[X_1,\ldots,X_n]$ tales que*

(i) *La extensión de anillos $\overline{\mathbb{F}}_q[Y_1,\ldots,Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$ es una extensión entera.*

(ii) *La función coordenada inducida por Y_{r+1} en $\overline{\mathbb{F}}_q[V]$ es un elemento primitivo de la extensión $\overline{\mathbb{F}}_q[Y_1,\ldots,Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$.*

(iii) *$W := \overline{\pi(V)}$ es una $\mathbb{F}_q$–hipersuperficie de grado δ birracionalmente equivalente a V.*

Demostración. Consideremos el polinomio A provisto por la Proposición 5.1.1. Sea $H := \{(\lambda,\gamma) \in \mathbb{A}^{(r+1)(n+1)} : A(\lambda,\gamma) = 0\}$ la hipersuperficie, de grado a lo sumo $2(r+1)\delta^2$, definida por A. La cantidad de puntos q–racionales de H es menor o igual que $2(r+1)\delta^2 q^{(r+1)(n+1)-1}$. Dado que $q > 2(r+1)\delta^2$ existe $(\lambda,\gamma) \in \mathbb{F}_q^{(r+1)(n+1)}$ tal que $A(\lambda,\gamma) \neq 0$. Definimos las formas lineales $Y = (Y_1,\ldots,Y_{r+1}) = \lambda X + \gamma \in \mathbb{F}_q[X_1,\ldots,X_n]$. Deducimos entonces las tres afirmaciones del enunciado del Teorema. En efecto, (i) y (ii) son consecuencias de la Proposición 5.1.1. En tanto que (iii) se deduce de 5.1.2 y del hecho de que W es una $\mathbb{F}_q$–hipersuperficie pues las formas lineales $Y_1,\ldots,Y_{r+1} \in \mathbb{F}_q[X_1,\ldots,X_n]$ (ver e.g., [Kun85]).

□

En el caso de una $\mathbb{F}_q$–variedad absolutamente irreducible, utilizando las mismas ideas de las Proposiciones 5.1.1 y 5.1.2, podemos obtener resultados similares con una condición de regularidad más baja que la del Teorema 5.1.3.

Teorema 5.1.4. *Sea V una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ. Si $q > r\delta$ existen formas lineales $Y_1,\dots,Y_{r+1} \in \mathbb{F}_q[X_1,\dots,X_n]$ tales que*

(i) *La extensión de cuerpos $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$ es separable y la forma lineal Y_{r+1} induce un elemento primitivo de la misma.*

(iii) *La $\mathbb{F}_q$–hipersuperficie $W := \overline{\pi(V)}$ tiene grado acotado por δ y es birracionalmente equivalente a V.*

Demostración. Dado que P_V es separable respecto de $\widetilde{Y}_{r+1}$, en el desarrollo de P_V en potencias de $\widetilde{Y}_{r+1}$ existe un monomio $\widetilde{A}_1\widetilde{Y}_{r+1}^{j_0}$, con j_0 no divisible por la característica de $\mathbb{F}_q$ y $\widetilde{A}_1 \in \overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}_1,\dots,\widetilde{Y}_r]$ no nulo. A su vez, consideremos un coeficiente $A_1 \in \overline{\mathbb{F}}_q[\Lambda^{(1)},\dots,\Lambda^{(r)},\Gamma_1,\dots,\Gamma_r]$ de un monomio nulo de $\widetilde{A}_1$, pensando $\widetilde{A}_1$ como un elemento de $\overline{\mathbb{F}}_q[\Lambda^{(1)},\dots,\Lambda^{(r)},\Gamma_1,\dots,\Gamma_r][\Lambda^{(r+1)},\Gamma_{r+1},\widetilde{Y}_1,\dots,\widetilde{Y}_r]$. Observemos que $\deg A_1 \leq r\delta$.

Sea $(\lambda,\gamma) \in \mathbb{A}^{r(n+1)}$ un elemento tal que $A_1(\lambda,\gamma) \neq 0$ y definamos las r formas lineales $Y := (Y_1,\dots,Y_r) := \lambda X + \gamma$. Por lo tanto, $P_V(\lambda,\Lambda^{(r+1)},\gamma,\Gamma_{r+1},Y_1,\dots,Y_r,\widetilde{Y}_{r+1})$ es un polinomio separable de $\overline{\mathbb{F}}_q(\Lambda^{(r+1)})[\widetilde{Y}_{r+1}]$. De aquí, vamos a demostrar que la extensión de cuerpos $\mathbb{F}_q(Y_1,\dots,Y_r) \hookrightarrow \mathbb{F}_q(V)$ es separable. En efecto, como el polinomio $A_1^* := \widetilde{A}_1(\lambda,\gamma,\Lambda^{(r+1)},\Gamma_{r+1})$ es un elemento no nulo de $\overline{\mathbb{F}}_q[\Lambda^{(r+1)},\Gamma_{r+1}]$, existen n vectores linealmente independientes $w_1,\dots,w_n \in \overline{\mathbb{F}}_q^n$ y elementos $a_1,\dots,a_n \in \overline{\mathbb{F}}_q$ tales que $A_1^*(w_k,a_k) \neq 0$ para cada $1 \leq k \leq n$. Considerando las n formas lineales $\ell_k := w_k X + a_k$, el polinomio $P_V(\lambda,\gamma,w_k,a_k,Y_1,\dots,Y_r,\ell_k)$ representa una ecuación separable no trivial para ℓ_k en la extensión $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$, que resulta una potencia del polinomio minimal de ℓ_k en esta extensión [Sam67]. Concluimos que cada ℓ_k es un elemento separable de la extensión $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$ y, como $\overline{\mathbb{F}}_q[\ell_1,\dots,\ell_n] = \overline{\mathbb{F}}_q[X_1,\dots,X_n]$, comprobamos que la extensión es separable. En particular, existen $\lambda_{r+1,1},\dots,\lambda_{r+1,n} \in \overline{\mathbb{F}}_q$ tales que la forma lineal $Y_{r+1} = \lambda_{r+1,1}X_1 + \cdots + \lambda_{r+1,n}X_n$ induce un elemento primitivo de la extensión. Entonces, bajo la proyección $\pi : V \to \mathbb{A}^{r+1}$ en $Y_1,\dots,Y_{r+1}$, demostramos, al igual que en la Proposición 5.1.2, que la hipersuperficie $\overline{\pi(V)}$ es birracionalmente equivalente a V. Del Lema 2.2.2 deducimos que tiene grado acotado por δ.

Mostremos, finalmente, que las formas lineales $Y_1,\dots,Y_{r+1}$ pueden elegirse con coeficientes en $\mathbb{F}_q$. Dado que $q > r\delta$, existe $(\lambda,\gamma) \in \mathbb{F}_q^{r(n+1)}$ que no anula al polinomio A_1, y a partir del cual definimos las formas $Y_1,\dots,Y_r$. A continuación, como $q > \delta$ podemos aplicar la versión efectiva del teorema del elemento primitivo que se presenta en [BG04], y asegurar la existencia de elementos $\lambda_{r+1,1},\dots,\lambda_{r+1,n} \in \mathbb{F}_q$ tales que la forma lineal $Y_{r+1} := \lambda_{r+1,1}X_1 + \cdots + \lambda_{r+1,n}X_n$ induce un elemento primitivo de $\overline{\mathbb{F}}_q(Y_1,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$. Concluimos que W es una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible pues el morfismo π se define mediante formas lineales en $\mathbb{F}_q[X_1,\dots,X_n]$. □

Una ventaja inmediata del Teorema 5.1.4 es que esta mejor condición de regularidad se traslada a la estimación que obtendremos.

5.2. Estimaciones para $\mathbb{F}_q$–variedades absolutamente irreducibles

Vamos a exhibir estimaciones explícitas sobre la cantidad de puntos q–racionales de una $\mathbb{F}_q$–variedad absolutamente irreducible. Las estimaciones que obtenemos son consecuencia de combinar la reducción al caso de una hipersuperficie de la Sección 5.1 con las estimaciones para hipersuperficies de la Sección 4.3.

Teorema 5.2.1. *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ. Si $q > r\delta$ es válida la siguiente estimación:*

$$\left||V(\mathbb{F}_q)| - q^r\right| \leq (\delta-1)(\delta-2)q^{r-\frac{1}{2}} + 5\delta^{\frac{13}{3}} q^{r-1}. \tag{5.4}$$

Demostración. En primer lugar, el teorema es válido en los casos $n = 1$, $\delta = 1$ ó $r = 0$ y, en el caso $n = 2$ y $r = 1$, no es otra cosa que la estimación de Hasse–Weil (1.2). Podemos pensar entonces que $n \geq 3$, $\delta \geq 2$ y $r > 0$.

Bajo la condición $q > r\delta$, el Teorema 5.1.4 muestra que la hipersuperficie $W = \overline{\pi(V)} \subset \mathbb{A}^{r+1}$ (birracionalmente equivalente a V bajo la proyección lineal definida por las formas lineales $Y_1, \ldots, Y_{r+1}$) es una $\mathbb{F}_q$–hipersuperficie de grado acotado por δ. Además, de la Proposición 5.1.2 deducimos que los puntos q–racionales de W satisfacen la siguiente estimación:

$$\left||V(\mathbb{F}_q)| - q^r\right| \leq \left||W(\mathbb{F}_q)| - q^r\right| + |(V \cap V_1)(\mathbb{F}_q)| + |(W \cap W_1)(\mathbb{F}_q)|,$$

donde $V_1 \subset \mathbb{A}^n$, y $W_1 \subset \mathbb{A}^{r+1}$ son las $\mathbb{F}_q$–hipersuperficies definidas en la sección anterior.

De la desigualdad de Bézout (2.1) y de la Proposición 3.1.3 deducimos las siguientes cotas superiores:

$$\begin{aligned} |(V \cap V_1)(\mathbb{F}_q)| &\leq \delta(\delta-1)q^{r-1}, \\ |(W \cap W_1)(\mathbb{F}_q)| &\leq \delta(\delta-1)q^{r-1}. \end{aligned} \tag{5.5}$$

Para estimar la cantidad de puntos q–racionales de W, basta tener presente que $W \subset \mathbb{A}^{r+1}$ es una $\mathbb{F}_q$–hipersuperficie absolutamente irreducible de grado δ. Por lo tanto, aplicando la estimación de la tercera línea de (4.15) obtenemos

$$\left||W(\mathbb{F}_q)| - q^r\right| \leq (\delta-1)(\delta-2)q^{r-\frac{1}{2}} + \left(\tfrac{8}{3}\delta^{\frac{13}{3}} + 4\delta^{\frac{11}{3}} + 2\delta^2 + \delta + \tfrac{7}{3}\right) q^{r-1}.$$

De esta última estimación y de (5.5), inmediatamente deducimos el resultado cuando $\delta \geq 3$. Cuando $\delta = 2$, combinamos (5.5) con la segunda línea de (4.16) y arribamos a la estimación enunciada. □

Si estimamos $\left||W(\mathbb{F}_q)|-q^r\right|$ usando el Teorema 4.3.3 en lugar del Teorema 4.3.2, obtenemos el siguiente resultado:

Corolario 5.2.2. *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ. Si $q > \max\{r\delta, 15\delta^{\frac{13}{3}}\}$ es válida la siguiente estimación:*

$$\left||V(\mathbb{F}_q)|-q^r\right| \leq (\delta-1)(\delta-2)q^{r-\frac{1}{2}}+7\delta^2 q^{r-1}.$$

Finalmente, del Corolario 4.3.7, una estimación en el caso que la característica de $\mathbb{F}_q$ es mayor que $2\delta^2$.

Corolario 5.2.3. *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ. Si la característica de $\mathbb{F}_q$ es mayor que $2\delta^2$ y $q > r\delta$ tenemos la estimación*

$$\left||V(\mathbb{F}_q)|-q^r\right| \leq (\delta-1)(\delta-2)q^{r-\frac{1}{2}}+4\delta^4 q^{r-1}.$$

Si además $q > 27\delta^4$ tenemos la estimación

$$\left||V(\mathbb{F}_q)|-q^r\right| \leq (\delta-1)(\delta-2)q^{r-\frac{1}{2}}+7\delta^2 q^{r-1}.$$

La estimación obtenida en el Teorema 5.2.1 nos permite, al mismo tiempo, disponer de una cota inferior no trivial sobre el número de puntos q–racionales de una $\mathbb{F}_q$–variedad absolutamente irreducible V de dimensión r y grado δ y, por lo tanto, asegurar la existencia de un punto q–racional de V, para $q > \max\{r\delta, 9\delta^{\frac{13}{3}}\}$. No obstante, argumentando de manera similar a la del Teorema 4.3.5, obtenemos un mejor resultado de existencia.

Corolario 5.2.4. *Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ. Si $q > \max\{r\delta, 2\delta^4\}$ entonces V tiene un punto q–racional.*

Demostración. Como $q > r\delta$, del Teorema 5.1.4 concluimos que existe una $\mathbb{F}_q$–hipersuperficie $W \subset \mathbb{A}^{r+1}$ absolutamente irreducible birracionalmente equivalente a V. Al mismo tiempo, de $q > 2\delta^4$ concluimos que existe un $\mathbb{F}_q$–plano $L \subset \mathbb{A}^{r+1}$ para el cual $W \cap L$ es una $\mathbb{F}_q$–curva absolutamente irreducible de $\mathbb{A}^{r+1}$. La estimación de Hasse–Weil (1.2) muestra que $|(W \cap L)(\mathbb{F}_q)| \geq q-(\delta-1)(\delta-2)q^{\frac{1}{2}}-\delta-1$. Además, de la desigualdad de Bézout deducimos que, si W_1 denota la $\mathbb{F}_q$–hipersuperficie de la Proposición 5.1.2, entonces $|W \cap L \cap W_1| \leq \delta(\delta-1)$, lo cual implica que $|(W \setminus W_1) \cap L)(\mathbb{F}_q)| \geq q-(\delta-1)(\delta-2)q^{\frac{1}{2}}-\delta^2-1$. Esta cantidad es estrictamente positiva para $q > 2\delta^4$ y así existe un punto q–racional de $W \setminus W_1$. Apelando nuevamente a la Proposición 5.1.2 concluimos que V tiene un punto q–racional. □

5.3. Estimaciones para $\mathbb{F}_q$–variedades arbitrarias

Este capítulo concluye con una estimación sobre la cantidad de puntos q–racionales de una $\mathbb{F}_q$–variedad arbitraria. La manera en que procedemos para obtener la estimación

es similar a la de la Sección 4.4.

Sea V una $\mathbb{F}_q$–variedad de dimensión r y grado δ y consideremos la descomposición de V en componentes $\mathbb{F}_q$–irreducibles:

$$V = V_1 \cup \cdots V_\sigma \cup V_{\sigma+1} \cup \cdots \cup V_\rho \cup V_{\rho+1} \cup \cdots \cup V_m.$$

Supongamos que el ordenamiento propuesto responde al criterio siguiente:

1. las componentes $V_1, \ldots, V_\sigma$ son absolutamente irreducibles y tienen dimensión r;
2. las componentes $V_{\sigma+1}, \ldots, V_\rho$ son absolutamente irreducibles y tienen dimensión acotada por $r-1$;
3. las componentes $V_{\sigma+1}, \ldots, V_\rho$ son relativamente irreducibles.

Denotamos por δ_i el grado de cada componente V_i y por Δ la suma de los grados de las componentes $V_1, \ldots, V_\sigma$, es decir $\Delta = \sum_{i=1}^{\sigma} \delta_i$.

Teorema 5.3.1. *Si $q > r\delta$ el número $|V(\mathbb{F}_q)|$ de puntos q–racionales de la variedad V satisface la siguiente estimación:*

$$\left||V(\mathbb{F}_q)| - \sigma q^r\right| \leq \operatorname{sign}(\sigma)(\Delta-1)(\Delta-2)q^{r-1/2} + \left(5\Delta^{\frac{13}{3}} + \delta^2\right)q^{r-1}, \tag{5.6}$$

donde $\operatorname{sign}(\sigma) := 0$ para $\sigma = 0$ y $\operatorname{sign}(\sigma) := 1$ en caso contrario.

Demostración. Como en la demostración del Teorema 4.4.1, escribimos $N := |V(\mathbb{F}_q)|$ y $N_i := |V_i(\mathbb{F}_q)|$. Luego, acotamos la diferencia $\left|N - \sigma q^r\right|$:

$$\left|N - \sigma q^r\right| \leq \sum_{i=1}^{\sigma} \left|N_i - q^r\right| + \left|N - \sum_{i=1}^{\sigma} N_i\right|.$$

Para cada $1 \leq i \leq \sigma$, V_i es una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ_i. Aplicando el Teorema 5.2.1 obtenemos que

$$\begin{aligned} \sum_{i=1}^{\sigma} \left|N_i - q^r\right| &\leq \sum_{i=1}^{\sigma} \left((\delta_i-1)(\delta_i-2)q^{r-1/2} + 5\delta_i^{\frac{13}{3}} q^{r-1}\right) \\ &\leq \operatorname{sign}(\sigma)(\Delta-1)(\Delta-2)q^{r-1/2} + 5\Delta^{\frac{13}{3}} q^{r-1}. \end{aligned} \tag{5.7}$$

Resta estimar el término $\left|N - \sum_{i=1}^{\sigma} N_i\right|$. Para cada $\sigma+1 \leq i \leq \rho$, la $\mathbb{F}_q$–variedad V_i tiene dimensión a lo sumo $r-1$ y grado δ_i; la Proposición 3.1.3 implica que $N_i \leq \delta_i q^{r-1}$. Por otro lado, para cada $\rho+1 \leq i \leq m$, la $\mathbb{F}_q$–variedad V_i es relativamente irreducible y por lo tanto la Proposición 3.1.5 muestra que $N_i \leq \delta_i^2 q^{r-1}/4$. Entonces tenemos que

$$N - \sum_{i=1}^{\sigma} N_i \leq \sum_{i=\sigma+1}^{m} N_i \leq q^{r-1} \sum_{i=\sigma+1}^{m} \delta_i^2 \leq \delta^2 q^{r-1}. \tag{5.8}$$

El Lema 3.1.3 implica que

$$\sum_{i=1}^{\sigma} N_i - N \leq \sum_{1 \leq i < j \leq \sigma} |(V_i \cap V_j)(\mathbb{F}_q)| \leq q^{r-1} \sum_{1 \leq i < j \leq \sigma} \delta_i \delta_j \leq \delta^2 q^{r-1}. \tag{5.9}$$

De las estimaciones (5.8) y (5.9) concluimos que $\left|N - \sum_{i=1}^{\sigma} N_i\right| \leq \delta^2 q^{r-1}$. Combinando esta estimación con (5.7) terminamos la demostración del teorema. □

6 Una estimación para una variedad intersección completa normal

Las estimaciones generalistas de los capítulos anteriores pueden no ser, y de hecho no son, las mejores estimaciones si consideramos variedades particulares. Es decir, la generalidad de la estimación puede no tomar en cuenta ciertas características geométricas de la variedad que podrían ser ventajosas a los fines de obtener mejores estimaciones. En ese sentido, en este capítulo, desarrollamos una versión efectiva del segundo Teorema de Bertini, y aplicamos los métodos precedentes para obtener una estimación para la cantidad de puntos q–racionales de una $\mathbb{F}_q$–variedad proyectiva intersección completa normal.

6.1. Sobre la existencia de buenas proyecciones lineales

Comenzamos recordando algunas definiciones y resultados que usaremos en este capítulo.

Sea $V \subset \mathbb{P}^n$ una K–variedad intersección completa. Sean $F_1, \ldots, F_{n-r} \in K[X_0, \ldots, X_n]$ los polinomios homogéneos que generan el ideal $I(V)$ de V. Denotamos por d_i el grado de cada F_i y por $d := \max_{1 \leq i \leq n-r} d_i$. Los grados de los polinomios dependen solamente de V y no del sistema de generadores. Ordenando los d_i de modo que $d_1 \geq d_2 \geq \cdots \geq d_{n-r}$, escribimos $\mathbf{d} := (d_1, \ldots, d_{n-r})$ y lo denominamos el *multigrado* de la intersección completa V. En particular, el grado de V es $\delta = \prod_{i=1}^{n-r} d_i$.

Recordemos que una K–variedad $V \subset \mathbb{P}^n$ irreducible es *normal* si para cada $x \in V$ existe un abierto U afín con $x \in U$ tal que el anillo de coordenadas afín $K[U]$ es integralmente cerrado. Una variedad no singular es normal y si V es una curva, normalidad y no singularidad son conceptos equivalentes. Recordamos el criterio de normalidad de Serre:

Una intersección completa $V \subset \mathbb{P}^n$ es normal si y solo si V es regular en codimensión 1 (i.e., la dimensión de singularidades de V tiene por lo menos codimensión 2 en V).

Enunciamos el teorema de conexión de Hartshorne tal como es citado en el texto de Kunz.

Teorema 6.1.1. *[Kun85, Ch. VI, Theorem 4.2.] Sea V una K–variedad proyectiva de dimensión positiva. Si V es intersección completa (con respecto a K) entonces,*

para cualquier K*–subvariedad* $W \subset V$ *de codimensión mayor o igual que 2,* $V \setminus W$ *es conexo en la* K*–topología (de Zariski). En particular,* V *es conexo.*

Como una consecuencia interesante de este resultado se tiene que una curva intersección completa normal $V \subset \mathbb{P}^n$ es absolutamente irreducible. En efecto, por el Teorema de Hartshorne la curva es conexa, luego, si tuviera componentes absolutamente irreducibles, los puntos de intersección serían puntos singulares, lo que contradiría la normalidad de la curva.

Consideremos una $\mathbb{F}_q$–variedad $V \subset \mathbb{P}^n$ absolutamente irreducible intersección completa de dimensión r y grado δ. La interpretación proyectiva del lema de normalización de Noether 2.1.3 asegura que para una elección genérica de variedades lineales L_r y L_{n-r-1} de $\mathbb{P}^n$ de dimensión r y $n-r-1$ respectivamente, tenemos las identidades

$$L_r \cap L_{n-r-1} = \emptyset, \qquad V \cap L_{n-r-1} = \emptyset.$$

Además, bajo la proyección central π_r desde L_{n-r-1}, la imagen de V es L_r y cada punto y de L_r tiene fibra finita. Finalmente, si $Y_0, \ldots, Y_r$ son formas lineales de $\overline{\mathbb{F}}_q[X_0, \ldots, X_n]$ que definen la variedad lineal L_{n-r-1} y definimos

$$\begin{array}{rccl} \pi_r : & V & \to & L_r \\ & x & \mapsto & (Y_0(x) : \cdots : Y_r(x)), \end{array}$$

el morfismo π_r es finito. Nuestro primer resultado justifica la posibilidad de una elección adecuada para la variedad lineal L_{n-r-1}:

Lema 6.1.2. *Existen índices* $0 \le i_{r+1} < \cdots < i_n \le n$ *tales que, definiendo* $Y_j := X_{i_j}$ *para* $r+1 \le j \le n$*, las formas lineales* $Y_{r+1}, \ldots, Y_n$ *son* $\overline{\mathbb{F}}_q$*–linealmente independientes y* $U := \{x \in V : (\partial F_i / \partial Y_{r+j})_{1 \le i,j \le n-r}(x) \neq 0\}$ *es un abierto Zariski no vacío de* V*.*

Demostración. Como V es absolutamente irreducible existen formas lineales $Y_0, \ldots, Y_r \in \overline{\mathbb{F}}_q[X_0, \ldots, X_n]$ tales que $\overline{\mathbb{F}}_q(Y_0, \ldots, Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$ es una extension algebraica separable. Al mismo tiempo, estas formas lineales pueden elegirse de modo tal que la proyección $\pi_r : V \to \mathbb{P}^r$ sea un morfismo finito. A fines de la argumentación, supongamos que hemos fijado estas formas lineales y sea $\lambda^{[0:r]} \in \overline{\mathbb{F}}_q^{(r+1)\times(n+1)}$ la matriz cuyas filas están formadas por los coeficientes de estas formas lineales.

Siguiendo [Sha94, II.6.3, Theorem 4] vemos que existe una fibra no ramificada $y := (y_0 : \cdots : y_r) \in \mathbb{P}^r$ de π_r (i.e., el número de imágenes inversas de y es igual al grado de la extensión de cuerpos $\overline{\mathbb{F}}_q(Y_0, \ldots, Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$). Sea $x \in \pi_r^{-1}(y)$ un elemento arbitrario. Como π_r es no ramificado en x entonces la diferencial $d_x\pi_r : T_xV \to T_y\mathbb{P}^r$ entre los espacios tangentes T_xV y $T_y\mathbb{P}^r$ a V en x y a $\mathbb{P}^r$ en y es inyectiva (ver [Dan94, §5, 5.2]).

Esto implica que la matriz de $(n+1)\times(n+1)$

$$D_r(x) := \begin{pmatrix} \lambda_{0,0} & \dots & \lambda_{0,n} \\ \vdots & & \vdots \\ \lambda_{r,0} & \dots & \lambda_{r,n} \\ \frac{\partial F_1}{\partial X_0}(x) & \dots & \frac{\partial F_1}{\partial X_n}(x) \\ \vdots & & \vdots \\ \frac{\partial F_{n-r}}{\partial X_0}(x) & \dots & \frac{\partial F_{n-r}}{\partial X_n}(x) \end{pmatrix},$$

es inversible. Considerando el desarrollo de Laplace del determinante de $D_r(x)$, concluimos que existen dos conjuntos disjuntos de índices $0 \le i_0 < i_1 < \cdots < i_r \le n$ y $0 \le i_{r+1} < \cdots < i_n \le n$ tales que cada una de las matrices siguientes son no singulares:

$$(\partial Y_i/\partial X_{i_j})_{0\le i,j\le r}, \quad \big((\partial F_i/\partial X_{i_{r+j}})(x)\big)_{1\le i,j\le n-r}.$$

Dado que la matriz $(\partial Y_i/\partial X_{i_j})_{0\le i,j\le r}$ es inversible deducimos que las formas lineales $Y_0,\dots,Y_r,X_{i_{r+1}},\dots,X_{i_n}$ son $\overline{\mathbb{F}}_q$–linealmente independientes. Definiendo $Y_j := X_{i_j}$ para $r+1 \le j \le n$, la matriz $\big((\partial F_i/\partial Y_{r+j})(x)\big)_{1\le i,j\le n-r}$ es no singular, lo cual implica que $U := \{x \in V : (\partial F_i/\partial Y_{r+j})_{1\le i,j\le n-r}(x) \ne 0\}$ es un abierto Zariski no vacío de V. □

Supongamos haber elegido formas lineales $Y_{r+1},\dots,Y_n$ que cumplen las condiciones del Lema 6.1.2. Nuestro próximo resultado provee una cota superior sobre el grado de la condición genérica que subyace a la elección de la variedad lineal L_r. Consideremos una matriz de indeterminadas $\Lambda := (\Lambda_{i,j})_{0\le i\le r,0\le j\le n}$; para cada $0 \le i \le r$ denotemos la i–ésima fila de Λ por $\Lambda^{(i)} := (\Lambda_{i,0},\Lambda_{i,1},\dots,\Lambda_{i,n})$ y definamos $\widetilde{Y} := (\widetilde{Y}_0,\dots,\widetilde{Y}_r) := \Lambda X$ con $X := (X_0,\dots,X_n)$.

Argumentando de modo similar al del Teorema 5.1.4 obtenemos la siguiente versión proyectiva del mismo:

Proposición 6.1.3. *Existe un polinomio no nulo $A \in \overline{\mathbb{F}}_q[\Lambda]$ de grado a lo sumo $(r+1)(2\delta+1)$ tal que para cada $\lambda \in \overline{\mathbb{F}}_q^{(r+1)(n+1)}$ con $A(\lambda) \ne 0$ definiendo las formas lineales $Y := (Y_0,\dots,Y_r) := \lambda X$, entonces, se verifican las siguientes condiciones:*

(i) *el morfismo $\pi_r : V \to \mathbb{P}^r$ definido por $Y_0,,\dots,Y_r$ es finito,*

(ii) *$\overline{\mathbb{F}}_q(Y_0,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$ es una extensión separable,*

(iii) *si $Y_{r+1},\dots,Y_n$ son las formas lineales del Lema 6.1.2, entonces $Y_0,\dots,Y_n$ son $\overline{\mathbb{F}}_q$–linealmente independientes.*

Del Lema 6.1.2 y la Proposición 6.1.3 deducimos el principal resultado de esta sección:

Corolario 6.1.4. *Sea $q > 2(r+1)(n-r)(d-1)\delta$. Entonces existen formas lineales $Y_0,\dots,Y_r \in \mathbb{F}_q[X_0,\dots,X_n]$ que satisfacen las siguientes condiciones:*

(i) *El morfismo* $\pi_r : V \to \mathbb{P}^r$ *definido por* $Y_0,,\ldots,Y_r$ *es finito,*

(ii) *Si* U *es el abierto del Lema 6.1.2, el morfismo* $\pi_{r-1} : V \setminus U \to \mathbb{P}^{r-1}$ *definido por* $Y_0,,\ldots,Y_{r-1}$ *es finito,*

(iii) $\overline{\mathbb{F}}_q(Y_0,\ldots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$ *es una extensión separable,*

(iv) $\overline{\mathbb{F}}_q(Y_0,\ldots,Y_{r-1}) \hookrightarrow \overline{\mathbb{F}}_q(\mathcal{C})$ *es separable para cada componente absolutamente irreducible* $\mathcal{C}$ *de* $V \setminus U$*,*

(v) *Si* $Y_{r+1},\ldots,Y_n$ *son las formas lineales del Lema 6.1.2, entonces* $Y_0,\ldots,Y_n$ *son* $\overline{\mathbb{F}}_q$*–linealmente independientes.*

Demostración. De la Proposición 6.1.3 se sigue que existe un polinomio $A \in \overline{\mathbb{F}}_q[\Lambda]$ de grado a lo sumo $(r+1)(2\delta+1)$ tal que, para cada $\lambda \in \overline{\mathbb{F}}_q^{(r+1)(n+1)}$ con $A(\lambda) \neq 0$, definiendo $Y := (Y_0,\ldots,Y_r) := \lambda X$, se verifican las condiciones (i), (iii) y (v). Consideremos la descomposición de $V \setminus U = \cup_{i=1}^s \mathcal{C}_i$ en componentes absolutamente irreducibles. Observemos que $\dim \mathcal{C}_i = r-1$ para cada $1 \leq i \leq s$. De la demostración del Teorema 5.1.4 concluimos que, para cada $1 \leq i \leq s$, existe un polinomio no nulo $A^{(i)} \in \overline{\mathbb{F}}_q[\Lambda]$ de grado a lo sumo $r(\deg \mathcal{C}_i + 1)$ tal que si $\lambda \in \overline{\mathbb{F}}_q^{(r+1)(n+1)}$ no anula a $A^{(i)}$, las formas lineales $Y := (Y_0,\ldots,Y_r) := \lambda X$ satisfacen la condición (ii) y (iv). Como $\sum_{i=1}^s \deg(\mathcal{C}_i) = \deg(V \setminus U) \leq (n-r)(d-1)\delta$, concluimos que el polinomio $A^* := A \cdot A^{(1)} \cdots A^{(s)}$ tiene grado a lo sumo $(r+1)(2\delta+1) + (r+1)(n-r)(d-1)\delta \leq 2(r+1)(n-r)(d-1)\delta$, y por lo tanto, si $\lambda \in \overline{\mathbb{F}}_q^{(r+1)(n+1)}$ no anula a $A^*(\lambda)$, las formas lineales $Y := (Y_0,\ldots,Y_r) := \lambda X$ satisfacen las condiciones (i)–(v). Aplicando la Proposición 3.1.3 existe $\lambda \in \mathbb{F}_q^{(r+1)(n+1)}$ tal que $A^*(\lambda) \neq 0$. Las formas lineales $Y := \lambda X$ verifican las condiciones del corolario. □

6.2. Una versión efectiva del segundo teorema de Bertini

Esta sección está destinada a presentar una versión efectiva del segundo teorema de Bertini. El segundo teorema de Bertini establece (ver e.g., [Sha94, II.6.2, Theorem 2]) que 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 cada $y \in U$. La versión que presentamos, además de ser efectiva, ya que proporciona una cota superior sobre el grado de la subvariedad de V_2 que define fibras singulares, es válida para variedades definidas sobre cuerpos de cualquier característica. Una versión efectiva de una forma débil del teorema de Bertini es presentada en [Bal03]. No obstante, la cota de grado es exponencialmente más alta que la nuestra.

Supongamos que $q > 2(r+1)(n-r)(d-1)\delta$ y sean $Y_0,\ldots,Y_n \in \mathbb{F}_q[X_0,\ldots,X_n]$ formas lineales que satisfacen las condiciones (i)–(v) del Corolario 6.1.4. Consideramos las proyecciones $\pi_r : V \to \mathbb{P}^r$ y $\pi_{r-1} : V \to \mathbb{P}^{r-1}$ definidas como $\pi_r(x) := (Y_0(x) : \cdots : Y_r(x))$ y

$\pi_{r-1}(x) := (Y_0(x) : \cdots : Y_{r-1}(x))$. El morfismo π_r está bien definido y es finito; π_{r-1} está bien definido fuera de la subvariedad de dimensión cero $\pi_r^{-1}(0:\cdots:0:1)$ y, de la elección de las formas lineales $Y_0,\ldots,Y_{r-1}$, deducimos que $\pi_{r-1}^{-1}(y)$ es una curva equidimensional de V para cada $y \in \mathbb{P}^{r-1}$. No solo vamos a probar que existe una subvariedad $W \subset \mathbb{P}^{r-1}$ propia tal que $\pi_{r-1}^{-1}(y)$ es no singular para cada $y \in U$ (hecho conocido) sino que además, vamos a proporcionar una estimación sobre el grado de W.

Para $x \in V$ e $y := \pi_{r-1}(x) \in \mathbb{P}^{r-1}$, denotamos por T_xV y $T_y\mathbb{P}^{r-1}$ los espacios tangentes a V en x y a $\mathbb{P}^{r-1}$ en y respectivamente. Por $d_x\pi_{r-1} : T_xV \to T_y\mathbb{P}^{r-1}$ denotamos la diferencial de π_{r-1} en x. El lema siguiente establece una condición suficiente para que la fibra $V_y := \pi_{r-1}^{-1}(y)$ correspondiente a $y \in \mathbb{P}^{r-1}$ sea no singular.

Lema 6.2.1. *Si para cada $x \in V_y$ se verifica que x es un punto regular de V y que $d_x\pi_{r-1}$ es suryectiva entonces V_y es una curva no singular.*

Demostración. Sea x un elemento arbitrario de V_y. Como la composición de $T_xV_y \hookrightarrow T_xV$ con $d_x\pi_{r-1}$ es la aplicación nula, concluimos que el espacio tangente T_xV_y a V_y en x está contenido en el núcleo de $d_x\pi_{r-1}$. Dado que $d_x\pi_{r-1}$ es suryectiva y que x es un punto regular de V obtenemos:

$$\dim T_xV_y \leq \dim \operatorname{Ker} d_x\pi_{r-1} = \dim T_xV - \dim T_y\mathbb{P}^{r-1} = \dim T_xV - (r-1) = 1.$$

Por otro lado, como cada componente de V_y tiene dimensión 1 entonces, para cada $x \in V_y$, la dimensión de T_xV_y es mayor o igual que 1. Es decir, todos los puntos de V_y son puntos regulares. □

A continuación damos una condición suficiente sobre x para que la diferencial $d_x\pi_{r-1}$ sea suryectiva.

Lema 6.2.2. *Sea $U = \{x \in V : \det(\partial F_i/\partial Y_{r+j})_{1\leq i,j\leq n-r}(x) \neq 0\}$ el abierto Zariski del Lema 6.1.2. Entonces $d_x\pi_{r-1}$ es suryectiva para cada $x \in U \setminus \pi_r^{-1}(0:\cdots:0:1)$.*

Demostración. Sea $x := (x_0 : \cdots : x_n) \in U$. Dado que x es un punto regular de V, de $\dim \operatorname{Ker} d_x\pi_{r-1} = r - \dim \operatorname{Im} d_x\pi_{r-1}$, observamos que la suryectividad de $d_x\pi_{r-1}$ es equivalente a la condición $\dim \operatorname{Ker} d_x\pi_{r-1} = 1$. Suponiendo que $Y_0(x) \neq 0$ podemos considerar la situación afín en la que π_{r-1} está localmente definido por $\pi_{r-1}(x) := (Y_1(x),\ldots,Y_{r-1}(x))$. En vistas de la definición de U, el núcleo $\operatorname{Ker} d_x\pi_{r-1}$ está representado por el espacio afín definido por las ecuaciones lineales $\overline{\mathbb{F}}_q$–linealmente independientes $\sum_{j=1}^{n}(\partial F_i/\partial Y_j)(x)(Y_j - Y_j(x)) = 0$ $(1 \leq i \leq n-r)$, $Y_k - Y_k(x) = 0$ $(1 \leq k \leq r-1)$. Por lo tanto $\operatorname{Ker} d_x\pi_{r-1}$ tiene dimensión 1. Esto completa la demostración. □

Finalmente, enunciamos nuestra versión efectiva del segundo teorema de Bertini.

Teorema 6.2.3. *Existe una subvariedad propia $W \subset \mathbb{P}^{r-1}$ de grado a lo sumo $2(n-r)^2(d-1)^2\delta$ tal que V_y es una curva no singular de grado a lo sumo δ para cada $y \notin W$.*

Demostración. Sea $Z \subset V$ el conjunto de puntos x tales que $d_x\pi_{r-1}$ no es suryectiva, y denotemos por V_{reg} y V_{sing} los subconjuntos de V de puntos regulares y puntos singulares, respectivamente. Podemos expresar Z como

$$Z = (Z \cap V_{reg}) \cup (Z \cap V_{sing}) = \overline{(Z \cap V_{reg})} \cup (Z \cap V_{sing}),$$

con $\overline{(Z \cap V_{reg})}$ la clausura Zariski (proyectiva) de $Z \cap V_{reg}$. El Lema 6.2.2 implica que $Z \subset V \setminus U$, i.e.,

$$Z \subset \{x \in V : F_1(x) = \cdots = F_{n-r}(x) = \det(\partial F_i/\partial Y_{r+j})_{1\le i,j\le n-r}(x) = 0\}.$$

Dado que V es normal, el conjunto de puntos singulares V_{sing} tiene codimensión al menos 2 en V y, por lo tanto, $Z \cap V_{sing}$ tiene dimensión a lo sumo $r-2$.

Afirmación. *Existe un cerrado $Z_{sing} \subset V$ de codimensión dos en V y de grado acotado por $(n-r)^2(d-1)^2\delta$ tal que $V_{sing} \subset Z_{sing}$.*

Demostración de la Afirmación. La matriz Jacobiana $(\partial F_i/\partial X_j)_{1\le i\le n-r,1\le j\le n+1}$ tiene $N_r := \binom{n+1}{n-r}$ menores maximales $M_1, \ldots, M_{N_r}$. Si $x \in V$ es un punto regular, existe entonces un menor M_j tal que $M_j(x) \neq 0$. En consecuencia, podemos elegir $\gamma_1, \ldots, \gamma_{N_r} \in \overline{\mathbb{F}}_q$, tales que $\sum_{j=1}^{N_r} \gamma_j M_j(x) \neq 0$. Sea $G := \sum_{j=1}^{n} \gamma_j M_j$. Del criterio del Jacobiano tenemos que $Z \cap V_{sing} \subset V \cap \{G = 0\} \subset V$; la irreducibilidad absoluta de V implica que $V \cap \{G = 0\}$ es una variedad proyectiva equidimensional de dimensión $r-1$.

Consideremos la descomposición de $V \cap \{G = 0\}$ en componentes absolutamente irreducibles, es decir $V \cap \{G = 0\} = \cup_{i=1}^{s} \mathcal{C}_i$. Todas las componentes $\mathcal{C}_i$ $(1 \le i \le s)$ intersecan el conjunto de puntos regulares V_{reg} pues la dimensión de V_{sing} es menor o igual que $r-2$. Como antes, podemos elegir entonces $x_i \in \mathcal{C}_i \cap V_{reg}$ y $\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_{N_r} \in \overline{\mathbb{F}}_q$ de modo que el polinomio $H := \sum_{j=1}^{N_r} \widetilde{\gamma}_j M_j$ no se anula en ninguno de los puntos x_i. Los polinomios G y H tienen grado acotado por $(n-r)(d-1)$.

Definimos la variedad $Z_{sing} := V \cap \{G = 0, H = 0\}$. Observemos que Z_{sing} es una variedad proyectiva equidimensional de dimensión $r-2$ que contiene a V_{sing} y cuyo grado es menor o igual que $(n-r)^2(d-1)^2\delta$. Así terminamos la demostración de la afirmación.

Afirmación. *Existe un cerrado $Z_{reg} \subset V$ de grado a lo sumo $(n-r)^2(d-1)^2\delta$ tal que $Z \cap V_{reg} \subset Z_{reg}$ y $\overline{\pi_{r-1}(Z_{reg})}$ es un cerrado propio de $\mathbb{P}^{r-1}$.*

Demostración de la Afirmación. Surgen dos posibilidades para el cerrado $\overline{Z \cap V_{reg}}$ o bien $\dim \overline{Z \cap V_{reg}} = r-1$ o, en su defecto, $\dim \overline{Z \cap V_{reg}} < r-1$.

Estudiamos, en primer lugar, qué ocurre cuando $\dim \overline{Z \cap V_{reg}} = r-1$. Expresamos $\overline{Z \cap V_{reg}}$ como unión de sus componentes absolutamente irreducibles $\overline{Z \cap V_{reg}} = \cup_{i=1}^{t} \mathcal{D}_i$ y nos encontramos con que la imagen por π_{r-1} de cada componente $\mathcal{D}_i$ es un cerrado propio de $\mathbb{P}^{r-1}$. En efecto, si para alguna componente $\mathcal{D}_i$ tuviéramos que $\pi_{r-1}(\mathcal{D}_i) = \mathbb{P}^{r-1}$ entonces $\dim \mathcal{D}_i = r-1$. En consecuencia, como $\mathcal{D}_i \subset Z \subset V \setminus U$, resultaría que $\mathcal{D}_i$ es una componente absolutamente irreducible de $V \setminus U$; por consiguiente, del Corolario 6.1.4, la extensión de cuerpos $\overline{\mathbb{F}}_q(Y_0, \ldots, Y_{r-1}) \hookrightarrow \overline{\mathbb{F}}_q(\mathcal{D}_i)$ sería una extensión separable. De este modo, aplicando [Sha94, II.6.2, Lemma 2] llegamos a una contradicción: existe un abierto Zariski no vacío O de $\mathcal{D}_i$ tal que $d_x\pi_{r-1}$ es suryectiva para cada $x \in O$. Así, para cada $1 \leq i \leq t$, necesariamente $\pi_{r-1}(\mathcal{D}_i)$ es un cerrado propio de $\mathbb{P}^{r-1}$.

Un punto regular $x \in V_{reg}$ pertenece a $Z \cap V_{reg}$ si y solo si $M(x)$ (la matriz Jacobiana de $F_1, \ldots, F_{n-r}, Y_0, \ldots, Y_{r-1}$ respecto de $X_0, \ldots, X_n$ evaluada en x) tiene rango menor que n. Si $x \in V_{reg}$ es un punto para el cual la diferencial $d_x\pi_{r-1}$ es suryectiva (por ejemplo, podemos tomar x en el abierto no vacío U del Lema 6.2.2), la matriz $M(x)$ tiene rango total n, con lo cual posee un menor no nulo de tamaño $n \times n$. Denotemos por $M^{(1)}, \ldots, M^{(n+1)}$ los menores maximales de la matriz M y definamos el polinomio $\widetilde{G} := \sum_{j=0}^{n+1} \eta_j M^{(j)}$ donde, para $1 \leq j \leq n+1$, los elementos $\eta_j \in \overline{\mathbb{F}}_q$ son tales que $\widetilde{G}(x) \neq 0$. Entonces $V \cap \{\widetilde{G} = 0\}$ es una variedad proyectiva equidimensional de dimensión $r-1$ que contiene a $Z \cap V_{reg}$ y por ende a $\overline{Z \cap V_{reg}}$.

Sea $V \cap \{\widetilde{G} = 0\} = \cup_{i=1}^{t'} \mathcal{E}_i$ la descomposición de $V \cap \{\widetilde{G} = 0\}$ en componentes absolutamente irreducibles. Nuevamente, como $\dim V_{sing} \leq r-2$ y cada componente $\mathcal{E}_i$ tiene dimensión $r-1$ para cada $1 \leq i \leq t'$, la intersección $\mathcal{E}_i \cap V_{reg}$ es no vacía. Supongamos que $\mathcal{E}_1, \ldots, \mathcal{E}_{t''}$ son las componentes contenidas en $\overline{Z \cap V_{reg}}$ para $t'' \leq t'$. Esto nos permite asegurar que para cada $t''+1 \leq i \leq t'$ existe un punto $x_i \in \mathcal{E}_i \cap (V_{reg} \setminus Z)$ y, con el mismo argumento de la afirmación anterior, que existen $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_{n+1} \in \overline{\mathbb{F}}_q$ tales que el polinomio $\widetilde{H} := \sum_{j=1}^{n+1} \widetilde{\eta}_j M_j$ no tiene como raíces a ninguno de los puntos $x_{t''+1}, \ldots, x_{n+1}$. Definimos la variedad $Z_{reg} := V \cap \{\widetilde{G} = 0, \widetilde{H} = 0\}$. Es una variedad proyectiva de dimensión $r-1$ cuyo grado verifica $\deg Z_{reg} \leq \delta \deg \widetilde{G} \deg \widetilde{H} \leq (n-r)^2(d-1)^2\delta$; además $Z \cap V_{reg} \subset Z_{reg} \subset V$. Al mismo tiempo, Z_{reg} puede expresarse en la forma $Z_{reg} = \cup_{i=1}^{t''} \mathcal{E}_i \cup \widetilde{Z}$ con $\dim \widetilde{Z} \leq r-2$ y $\dim \pi_{r-1}(\mathcal{E}_i) \leq r-2$ para $1 \leq i \leq t''$, lo cual demuestra que $\pi_{r-1}(Z_{reg})$ está estrictamente contenido en $\mathbb{P}^{r-1}$. Esto prueba la afirmación cuando $\dim \overline{Z \cap V_{reg}} = r-1$.

El análisis de la posibilidad $\dim \overline{Z \cap V_{reg}} < r-1$ es más sencillo ya que no tenemos que manipular componentes de $\overline{Z \cap V_{reg}}$ de dimensión $r-1$. Tomamos los polinomios $\widetilde{G}, \widetilde{H}$ e inmediatamente $\dim \overline{\pi_{r-1}(Z_{reg})} \leq r-2$. Demostramos la afirmación

Estamos en condiciones de demostrar completamente el teorema. De las afirmaciones previas se desprende que $Z \cup V_{sing} \subset Z_{sing} \cup Z_{reg}$ y que $Z_{sing} \cup Z_{reg}$ es una subvariedad propia de V de dimensión $r-1$ y grado a lo sumo $2(n-r)^2(d-1)^2\delta$. Además, $W := \overline{\pi_{r-1}(Z_{reg} \cup Z_{sing})}$ es una subvariedad propia de $\mathbb{P}^{r-1}$, la cual, Lema 2.2.2 mediante, tiene grado a lo sumo $2(n-r)^2(d-1)^2\delta$. Si $y \in \mathbb{P}^{r-1} \setminus W$ entonces cada $x \in V_y$ es un

punto regular de V que no pertenece a Z: en otras palabras, la diferencial $d_x\pi_{r-1}$ es suryectiva. El Lema 6.2.1 nos proporciona la no singularidad de la curva V_y. Que el grado es a lo sumo δ se deriva de la desigualdad de Bézout (2.1).

□

Dado que para cada $y \notin W$ la curva V_y es no singular e intersección completa, el teorema de conexión de Hartshorne implica que V_y es conexa y luego, absolutamente irreducible.

6.3. La estimación

En esta sección obtenemos una estimación sobre el número de puntos q–racionales de una $\mathbb{F}_q$–variedad $V \subset \mathbb{P}^n$ normal e intersección completa de dimensión r, grado δ y multigrado $\mathbf{d} := (d_1, \ldots, d_{n-r})$. La estimación toma como punto de partida la estimación de Deligne [Del74] sobre el número de puntos q–racionales de una $\mathbb{F}_q$–curva $C \subset \mathbb{P}^n$ intersección completa no singular de grado δ y multigrado $\mathbf{d}$:

$$\big||C(\mathbb{F}_q)| - p_1\big| \leq b_1'(n, \mathbf{d}) q^{1/2}, \tag{6.1}$$

donde $b_1'(n, \mathbf{d})$ denota el primer número de Betti primitivo de una intersección completa no singular $C \subset \mathbb{P}^n$ de dimensión 1 y multigrado $\mathbf{d}$. Es válida la desigualdad $b_1'(n, \mathbf{d}) \leq (\delta - 1)(\delta - 2)$, con igualdad si y solo si $n = 2$.

Denotemos por d el máximo de los grados de los polinomios que definen V y asumamos la condición de regularidad $q > 2(r+1)(n-r)(d-1)\delta$. Bajo esta condición existen formas lineales $Y_0, \ldots, Y_n \in \mathbb{F}_q[X_0, \ldots, X_n]$ que satisfacen las condiciones (i)–(v) del Corolario 6.1.4. Para cada $y \in \mathbb{P}^{r-1}(\mathbb{F}_q)$, denotamos por N_y el número de puntos q–racionales de la curva equidimensional $V_y := \pi_{r-1}^{-1}(y) \subset V$. Vamos a estimar $|V(\mathbb{F}_q)|$ en términos de las cantidades N_y.

Teorema 6.3.1. *Sea $V \subset \mathbb{P}^n$ una $\mathbb{F}_q$–variedad intersección completa normal de dimensión r, grado $\delta \geq 2$ y multigrado $\mathbf{d}$. Si $q > 2(r+1)(n-r)(d-1)\delta$, es válida la estimación*

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

donde $W \subset \mathbb{P}^{r-1}$ es la variedad del Teorema 6.2.3.

Demostración. Comencemos expresando $|V(\mathbb{F}_q)|$ en términos de las cantidades N_y con $y \in \mathbb{P}^{r-1}(\mathbb{F}_q)$:

$$|V(\mathbb{F}_q)| \;=\; \sum_{y \in \mathbb{P}^{r-1}(\mathbb{F}_q)} N_y + e, \tag{6.2}$$

donde e es el número de puntos q–racionales de $\pi_r^{-1}(0:\cdots:0:1)$. Como π_r es un morfismo finito y $\mathbb{P}^r$ es una variedad normal el cardinal de cada fibra de π_r es menor o igual que δ. En particular, $e \leq \delta$.

Si restamos p_r en ambos miembros de (6.2) y usamos que $p_r = p_1 p_{r-1} - q p_{r-2}$, obtenemos:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \sum_{y \in \mathbb{P}^{r-1}(\mathbb{F}_q)} |N_y - p_1| + q p_{r-2} + \delta. \tag{6.3}$$

Considerando la variedad $W \subset \mathbb{P}^{r-1}$ del Teorema 6.2.3, podemos descomponer la sumatoria de (6.3) del siguiente modo:

$$\sum_{y \in \mathbb{P}^{r-1}(\mathbb{F}_q)} |N_y - p_1| = \sum_{y \notin W(\mathbb{F}_q)} |N_y - p_1| + \sum_{y \in W(\mathbb{F}_q)} |N_y - p_1|.$$

La tarea se reduce entonces a estimar las cantidades $|N_y - p_1|$ bajo dos circunstancias diferentes: cuando y es un punto q–racional de W y cuando y es un punto q–racional de $\mathbb{P}^{r-1}$ que no pertenece a W.

Si $y \in W(\mathbb{F}_q)$, aplicando la Proposición 3.1.3 tenemos que $N_y \leq \delta p_1$ y $|W(\mathbb{F}_q)| \leq \deg W p_{r-2}$. De la condición $\delta \geq 2$, deducimos la desigualdad $|N_y - p_1| \leq (\delta - 1) p_1$ y, por lo tanto, la estimación

$$\sum_{y \in W(\mathbb{F}_q)} |N_y - p_1| \leq (\delta - 1) p_1 \cdot \deg W p_{r-2} \leq \delta \deg W q^{r-1}. \tag{6.4}$$

En el segundo caso –es decir, cuando y es un punto q–racional de $\mathbb{P}^{r-1}$ que no pertenece a W– el Teorema 6.2.3 asegura que la fibra V_y es una $\mathbb{F}_q$–curva intersección completa no singular en $\mathbb{P}^{n-r+1}$ de grado a lo sumo δ y multigrado $\mathbf{d}$. Aplicando la estimación (6.1) a esta curva, obtenemos que $|N_y - p_1| \leq b_1'(n-r+1, \mathbf{d}) q^{1/2}$, donde $b_1'(n-r+1, \mathbf{d})$ es el número de Betti correspondiente. Escribiendo $b_1' := b_1'(n-r+1, \mathbf{d})$ llegamos a la estimación

$$\sum_{y \notin W(\mathbb{F}_q)} |N_y - p_1| \leq b_1' q^{r-1/2} + b_1' p_{r-2} q^{1/2} \leq b_1' q^{r-1/2} + b_1' q^{r-1}. \tag{6.5}$$

Para concluir, simplemente combinamos (6.3), (6.4) y (6.5) con la acotación $q p_{r-2} + \delta \leq 2q^{r-1}$.

□

Ahora, si tenemos en cuenta que el grado de la variedad W obtenida en el Teorema 6.2.3 es menor o igual que $2(n-r)^2(d-1)^2\delta$, deducimos el siguiente corolario:

Corolario 6.3.2. *Bajo las mismas condiciones del Teorema 6.3.1 es válida la si-*

guiente estimación:

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

7 Búsqueda de puntos q–racionales: preparación de los datos de entrada

De aquí en más, nuestros esfuerzos se dirigen a calcular un punto q–racional de una $\mathbb{F}_q$–variedad $V \subset \mathbb{A}^n$ absolutamente irreducible de dimensión r y grado δ, definida por una sucesión regular reducida. Retomando lo hecho en el Capítulo 5, obtenemos cotas superiores sobre el grado de ciertas condiciones genéricas necesarias para el desarrollo del algoritmo. Además, determinamos la existencia de una variedad lineal afín $L \subset \mathbb{A}^n$ de codimensión $r-1$ de modo que $V \cap L$ es una curva absolutamente irreducible de $\mathbb{A}^n$ de grado δ. De esta manera reducimos el cálculo del punto q–racional de V al cálculo de un punto q–racional de una curva absolutamente irreducible.

7.1. Soluciones geométricas compatibles

Sea $V \subset \mathbb{A}^n$ una $\mathbb{F}_q$–variedad equidimensional de dimensión r y grado δ. Consideremos una solución geométrica de V, tal como fue definida en la sección 2.3. Es decir, tenemos variables $Y_1, \ldots, Y_n$ en posición de Noether respecto de V, con $Y_1, \ldots, Y_r$ variables libres, Y_{r+1} un elemento primitivo de la extensión entera de anillos $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$, el polinomio minimal $m \in \overline{\mathbb{F}}_q[Y_1, \ldots, Y_r, T]$ de Y_{r+1}, de grado a lo sumo δ, y las parametrizaciones

$$\frac{\partial m}{\partial Y_{r+1}}(Y_1, \ldots, Y_r, Y_{r+1}) Y_{r+k} - v_{r+k}(Y_1, \ldots, Y_r, Y_{r+1}) \in I(V) \quad (2 \leq k \leq n-r),$$

donde cada $v_{r+k} \in \overline{\mathbb{F}}_q[Y_1, \ldots, Y_r, T]$ tiene grado a lo sumo $\delta - 1$.

Bajo estas condiciones la proyección π en las formas $Y_1, \ldots, Y_r$ resulta un morfismo finito. Supongamos además que V está definida por una sucesión regular $F_1, \ldots, F_{n-r} \in \mathbb{F}_q[X_1, \ldots, X_n]$.

Definición 7.1.1. *Un punto* $P := (p_1, \ldots, p_r) \in \mathbb{A}^r$ *es un* punto de levantamiento *de* V *(respecto de* π*) si la matriz jacobiana de* $F_1, \ldots, F_{n-r}$ *con respecto a las variables dependientes* $Y_{r+1}, \ldots, Y_n$ *es inversible en cada* $x \in V_P := \pi^{-1}(P)$*. La fibra* $V_P := \pi^{-1}(P)$ *se denomina una* fibra de levantamiento *de* P*.*

Observemos que con esta definición, en particular, del lema 2.1.9 deducimos que P es un punto no ramificado de π.

Supongamos ahora que P es un punto de levantamiento de π que no anula el discriminante del polinomio m respecto de T. La solución geométrica de V induce una solución geométrica de la fibra de levantamiento V_P. Esta solución geométrica de V_P viene dada por las formas lineales $Y_{r+1},\dots,Y_n$, el polinomio minimal $m(P,T)$ de Y_{r+1} y las parametrizaciones

$$\frac{\partial m}{\partial Y_{r+1}}(P,Y_{r+1})Y_{r+2}-v_{r+2}(P,Y_{r+1}),\dots,\frac{\partial m}{\partial Y_{r+1}}(P,Y_{r+1})Y_n-v_n(P,Y_{r+1}).$$

Una solución geométrica de V de este tipo se dice *compatible* con P. Observemos que, en estas circunstancias, el grado de V_P, es decir, el cardinal de V_P es igual a δ, el grado de la variedad.

7.2. Los preparativos

Sea $V\subset\mathbb{A}^n$ una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión r y grado δ definida por polinomios $F_1,\dots,F_{n-r}\in\mathbb{F}_q[X_1,\dots,X_n]$ de grado acotado por d. De aquí en adelante supondremos que $n\geq 3$ y que $d\geq 2$. Supongamos que los polinomios forman una sucesión regular reducida: el ideal $(F_1,\dots,F_s)$ es radical para cada $s=1,\dots,n-r$.

Para cada $s=1,\dots,n-r$, cada uno de estos ideales intermedios define una $\mathbb{F}_q$–variedad V_s equidimensional de dimensión $n-s$. Vamos a denotar por δ_s el grado de V_s. Con esta notación, $V_{n-r}=V$ y $\delta_{n-r}=\delta$. Definimos también el *grado geométrico* Δ de V como el máximo de los grados de las variedades intermedias; en simbolos, $\Delta=\max_{1\leq s\leq n-r}\delta_s$.

Fijemos una serie de notaciones que utilizaremos a lo largo del desarrollo del algoritmo.Sea s un número natural fijo entre 1 y $n-r$. Supongamos que hemos realizado un cambio lineal de coordenadas de modo que las variables $Y_1,\dots,Y_n$ están en posición de Noether respecto a la $\mathbb{F}_q$–variedad V_s y que $Y_1,\dots,Y_{n-s}$ son variables libres. Por lo tanto, la proyección $\pi_s:V_s\to\mathbb{A}^{n-s}$ es un morfismo finito. Si, además, la forma lineal Y_{n-s+1} es un elemento primitivo de la extensión entera de anillos inducida $\overline{\mathbb{F}}_q[Y_1,\dots,Y_r]\hookrightarrow\overline{\mathbb{F}}_q[V]$, su minimal será denotado por $m^{(s)}$. Supongamos también que $P^{(s)}\in\mathbb{A}^{n-s}$ es un punto de levantamiento de π_s; vamos a denotar por $V_{P^{(s)}}:=\pi_s^{-1}(P^{(s)})$ la correspondiente fibra (de dimensión cero) de levantamiento.

Para poner en marcha el algoritmo aún resta determinar la posibilidad de obtener las siguientes dos condiciones:

1. una normalización de Noether simultánea de las variedades $V_1,\dots,V_{n-r}$ y elementos primitivos adecuados; es decir, un cambio de coordenadas lineal de modo que las nuevas variables $Y_1,\dots,Y_n$ estén en posición de Noether respecto de cada una de las variedades intermedias V_s, y que la forma lineal Y_{n-s+1} sea un elemento primitivo de la extensión de anillos $\overline{\mathbb{F}}_q[Y_1,\dots,Y_{n-s}]\hookrightarrow\overline{\mathbb{F}}_q[V_s]$.

2. puntos de levantamiento $P = (p_1, \ldots, p_{n-s}) \in \mathbb{A}^{n-s}$ de π_s tales que el vector $P^* = (p_1, \ldots, p_{n-s-1}) \in \mathbb{A}^{n-s-1}$, conformado por las primeras $n-s-1$ coordenadas de P, sea punto de levantamiento de π_{s+1} y tales que la fibra V_{P^*} tenga la siguiente propiedad: para cada $Q \in V_{P^*}$, el morfismo π_s es no ramificado en $\pi_s(Q)$.

Nuestra tarea consiste en la determinación de una cota superior sobre el grado de la condición genérica que se desprende de exigir estas condiciones.

Sea $\Lambda := (\Lambda_{ij})_{1 \le i \le n-s+1, 1 \le j \le n}$ una matriz de indeterminadas de $(n-s+1) \times n$, y sea $\Gamma := (\Gamma_1, \ldots, \Gamma_{n-s+1})$ un vector de indeterminadas. Definimos nuevas indeterminadas $\widetilde{Y} := \Lambda X + \Gamma = (\widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s+1})$. Para cada $(\lambda, \gamma) \in \mathbb{A}^{(n-s+1)(n+1)}$ escribimos $Y := \lambda X + \gamma := (Y_1, \ldots, Y_{n-s+1})$.

Para dar cuenta de la primera de las condiciones enunciadas, vamos a reformular la Proposición 5.1.1. Reescribimos su enunciado haciéndolo depender de s.

Proposición 7.2.1. *Existe un polinomio no nulo $A_s \in \overline{\mathbb{F}}_q[\Lambda, \Gamma]$ de grado a lo sumo $2(n-s+1)\delta_s^2$ tal que para cada $(\lambda, \gamma) \in \mathbb{A}^{(n-s+1)(n+1)}$ con $A_s(\lambda, \gamma) \neq 0$, el morfismo π_s es finito y la forma lineal Y_{n-s+1} induce un elemento primitivo de la extensión entera de anillos $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_{n-s}] \hookrightarrow \overline{\mathbb{F}}_q[V_s]$.*

La segunda condición es la que facilita la obtención de una solución geométrica de la variedad V_s de modo que ningún punto $P \in V_{P^{(s+1)}}$ anule el discriminante del correspondiente polinomio minimal $m^{(s)}$. De esta forma, no tendremos que tratar con multiplicidades durante el algoritmo.

Teorema 7.2.2. *Existe un polinomio no nulo $B_s \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s}]$, de grado acotado por $4(n-s+3)^2 n d \delta_s^2 \delta_{s+1}^2$ tal que si $(\lambda, \gamma, P) \in \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ es un punto que no anula a B_s, se satisfacen las siguientes condiciones:*

(i) *el morfismo $\pi_s : V_s \to \mathbb{A}^{n-s}$ es finito, $P \in \mathbb{A}^{n-s}$ es un punto de levantamiento de π_s y la forma lineal Y_{n-s+1} es un elemento primitivo de la fibra $\pi_s^{-1}(P)$.*

(ii) *El morfismo $\pi_{s+1} : V_{s+1} \to \mathbb{A}^{n-s-1}$ es finito, $P^* \in \mathbb{A}^{n-s-1}$ es un punto de levantamiento de π_{s+1} y la forma lineal Y_{n-s} es un elemento primitivo de la fibra $\pi_{s+1}^{-1}(P^*)$.*

(iii) *Cada punto $Q \in \pi_s\big(\pi_{s+1}^{-1}(P^*)\big)$ es un punto de levantamiento de π_s y la forma lineal Y_{n-s+1} es un elemento primitivo de $\pi_s^{-1}(Q)$.*

Con el objeto de facilitar la lectura de la demostración del teorema, enunciamos y demostramos una serie de lemas previos.

Sean A_s y A_{s+1} los polinomios que se obtienen al aplicar la Proposición 7.2.1 a las variedades V_s y V_{s+1} respectivamente.

Comenzamos con el siguiente resultado técnico. Es una versión simplificada de un resultado de [HMW01, Lemma 1 (iii)] con una mejor cota de grado.

Lema 7.2.3. *Sea* $H \in \overline{\mathbb{F}}_q[\Lambda,\Gamma,X]$ *un polinomio de grado a lo sumo* D. *Supongamos que la clausura Zariski* $\widehat{V}_s$ *de* $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{H = 0, A_s \neq 0\}$ *tiene dimensión menor o igual que* $(n-s+1)(n+2)-2$. *Consideremos el morfismo*

$$\begin{array}{rccc} \Phi^*: & \mathbb{A}^{(n-s+1)(n+1)} \times V_s & \to & \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s} \\ & (\lambda,\gamma,x) & \mapsto & \big(\lambda,\gamma,\lambda^* x+\gamma^*\big), \end{array}$$

donde λ^* *representa las primeras* $n-s$ *filas de* λ *y* γ^* *las primeras* $n-s$ *coordenadas de* γ. *Entonces la clausura Zariski de la imagen de* $\widehat{V}_s$ *bajo* Φ^* *está contenida en una hipersuperficie de* $\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ *de grado a lo sumo* $2(n-s+2)D\delta_s^2$.

Demostración. Si para cada $1 \leq k \leq n$, tomamos derivadas parciales con respecto a la variable $\Lambda_{n-s+1,k}$ como en (2.4) obtenemos la siguiente identidad en $\overline{\mathbb{F}}_q[\Lambda,\Gamma] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V_s]$:

$$\frac{\partial P_{V_s}}{\partial \widetilde{Y}_{n-s+1}}(\Lambda,\Gamma,\widehat{Y})\,\xi_k + \frac{\partial P_{V_s}}{\partial \Lambda_{n-s+1,k}}(\Lambda,\Gamma,\widehat{Y}) = 0, \tag{7.1}$$

donde $\widehat{Y} := \Lambda\xi+\Gamma$ y $\xi := (\xi_1,\ldots,\xi_n)$ es el vector de funciones coordenadas de V_s inducidas por X.

Denotemos por $\widehat{H}$ el elemento de $\overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}]$ obtenido al reemplazar en H cada X_k por $-(\partial P_{V_s}/\partial \widetilde{Y}_{n-s+1})^{-1}(\partial P_{V_s}/\partial \Lambda_{n-s+1,k})$ $(1 \leq k \leq n)$ y, luego, limpiar denominadores. Observemos que $\deg_{\widetilde{Y}} \widehat{H} = \deg_{\widetilde{Y}_{n-s+1}} \widehat{H} \leq D\delta_s$ y $\deg_{\Lambda,\Gamma} \widehat{H} \leq (n-s+1)D\delta_s$.

Sea $R := \mathrm{Res}_{\widetilde{Y}_{n-s+1}}(P_{V_s}, \widehat{H}) \in \overline{\mathbb{F}}_q[\Lambda,\Gamma,\widetilde{Y}_1,\ldots,\widetilde{Y}_{n-s}]$ la resultante de P_{V_s} y $\widehat{H}$ con respecto a $\widetilde{Y}_{n-s+1}$. Como la matriz de Sylvester de P_{V_s} y $\widehat{H}$ es una matriz de tamaño a lo sumo $(D+1)\delta_s \times (D+1)\delta_s$ con a lo sumo $D\delta_s$ columnas con coeficientes de P_{V_s} o entradas nulas, y a lo sumo δ_s columnas con coeficientes de $\widehat{H}$ o entradas nulas, el grado de R está acotado por $2(n-s+2)D\delta_s^2$. Por otro lado, de la identidad (7.1) y de las propiedades de la resultante concluimos que $R(\Lambda,\Gamma,\widetilde{Y}_1,\ldots,\widetilde{Y}_{n-s})$ se anula sobre la variedad $\widehat{V}_s$ y, dado que $\dim \widehat{V}_s \leq (n-s+1)(n+2)-2$, entonces $R(\Lambda,\Gamma,\widetilde{Y}_1,\ldots,\widetilde{Y}_{n-s}) \neq 0$ y por lo tanto, es la ecuación que define la hipersuperficie buscada. □

A partir de considerar los siguientes polinomios de $\overline{\mathbb{F}}_q[\Lambda,\Gamma,X]$

$$D_s := \det\begin{pmatrix} \Lambda_{1,1} & \cdots & \Lambda_{1,n} \\ \vdots & & \vdots \\ \Lambda_{n-s,1} & \cdots & \Lambda_{n-s,n} \\ \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_s}{\partial X_1} & \cdots & \frac{\partial F_s}{\partial X_n} \end{pmatrix}, D_{s+1} := \det\begin{pmatrix} \Lambda_{1,1} & \cdots & \Lambda_{1,n} \\ \vdots & & \vdots \\ \Lambda_{n-s-1,1} & \cdots & \Lambda_{n-s-1,n} \\ \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial F_{s+1}}{\partial X_1} & \cdots & \frac{\partial F_{s+1}}{\partial X_n} \end{pmatrix}$$

enunciamos los siguientes lemas

Lema 7.2.4. *La clausura Zariski $\widehat{V}_s$ del conjunto*

$$(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{D_s = 0, A_s \neq 0\}$$

es una subvariedad de $\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^n$ equidimensional de dimensión $(n-s+1)(n+2)-2$.

Demostración. Consideremos la descomposición de V_s en componentes irreducibles: $V_s = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_N$. Entonces

$$\mathbb{A}^{(n-s+1)(n+1)} \times V_s = \bigcup_{i=1}^{N} \mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{C}_i$$

es la descomposición de $\mathbb{A}^{(n-s+1)(n+1)} \times V_s$ en componentes irreducibles. Escribamos $\mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{C}$ para indicar una de estas componentes irreducibles y sea $x \in \mathcal{C}$ un punto no singular de V_s. Como $D_s(\Lambda, x) \neq 0$ existe $\lambda \in \mathbb{A}^{(n-s+1)n}$ tal que $D_s(\lambda, x) \neq 0$. Es decir, existe un punto $(\lambda, \gamma, x) \in \mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{C}$ que no pertenece a la hipersuperficie definida por D_s. Por otro lado, si 0 denota la matriz nula de $\mathbb{A}^{(n-s+1)n}$, entonces $D_s(0, x) = 0$ para todo $x \in V_s$. Es decir, la hipersuperficie $\{D_s = 0\}$ tiene intersección no vacía y propia con cada una de las componentes $\mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{C}$. En definitiva, esto muestra que $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{D_s = 0\}$ es una variedad equidimensional de dimensión $(n-s+1)(n+2)-2$ y, por lo tanto, la clausura Zariski del conjunto $\widehat{V}_s$ es vacía o una variedad equidimensional de dimensión $(n-s+1)(n+2)-2$. □

Con una demostración análoga tenemos también el siguiente lema.

Lema 7.2.5. *La clausura Zariski $\widehat{V}_{s+1}$ del conjunto*

$$(\mathbb{A}^{(n-s)(n+1)} \times V_{s+1}) \cap \{D_{s+1} = 0, A_{s+1} \neq 0\}$$

es una subvariedad de $\mathbb{A}^{(n-s)(n+1)} \times \mathbb{A}^n$ equidimensional de dimensión $(n-s)(n+2)-2$.

Consideremos los siguientes morfismos:

$$\begin{array}{rccc} \Phi_s : & \widehat{V}_s & \to & \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s} \\ & (\lambda, \gamma, x) & \mapsto & \big(\lambda, \gamma, Y_1(x), \ldots, Y_{n-s}(x)\big), \end{array}$$

$$\begin{array}{rccc} \Phi_{s+1} : & \widehat{V}_{s+1} & \to & \mathbb{A}^{(n-s)(n+1)} \times \mathbb{A}^{n-s-1} \\ & (\lambda^*, \gamma^*, x) & \mapsto & \big(\lambda^*, \gamma^*, Y_1(x), \ldots, Y_{n-s-1}(x)\big). \end{array}$$

De los Lemas 7.2.4 y 7.2.5 y luego, como consecuencia del Lema 7.2.3 deducimos que la clausura Zariski de $\mathrm{Im}\,\Phi_s$ está contenida en una hipersuperficie de $\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ de grado a lo sumo $2(n-s+2)n(d-1)\delta_s^2$, y que la clausura Zariski de $\mathrm{Im}\,\Phi_{s+1}$

está contenida en una hipersuperficie de $\mathbb{A}^{(n-s)(n+1)} \times \mathbb{A}^{n-s-1}$ de grado a lo sumo $2(n-s+1)n(d-1)\delta_{s+1}^2$. Estas hipersuperficies están definidas por polinomios $\widehat{B}_s \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s}]$ y $\widehat{B}_{s+1} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s-1}]$, respectivamente.

Sean $\rho_s, \rho_{s+1} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{n-s}]$ los discriminantes de las variedades V_s y V_{s+1}, definidos en la demostración de la Proposición 5.1.1. Recordemos que $\deg \rho_s \leq (n-s+2)(2\delta_s^2 - \delta_s)$ y $\deg \rho_{s+1} \leq (n-s+1)(2\delta_{s+1}^2 - \delta_{s+1})$.

Lema 7.2.6. *La clausura Zariski del conjunto*

$$(\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}) \cap \{\rho_s \widehat{B}_s = 0, A_{s+1} \neq 0\}$$

tiene dimensión a lo sumo $(n-s+1)(n+2)-3$.

Demostración. En primer lugar, la aplicación Φ_s puede ser regularmente extendida a $\mathbb{A}^{(n-s+1)(n+1)} \times V_s$. De la definición de A_s, deducimos que esta extensión induce un morfismo finito, al que también denotaremos por Φ_s, abuso de notación mediante:

$$\begin{array}{rcl} \Phi_s : (\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{A_s \neq 0\} & \to & (\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}) \cap \{A_s \neq 0\} \\ (\lambda, \gamma, x) & \mapsto & \big(\lambda, \gamma, Y_1(x), \ldots, Y_{n-s}(x)\big) \end{array}$$

Como $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{D_s = 0, A_s \neq 0\}$ es una subvariedad equidimensional de $(\mathbb{A}^{(n-s+1)(n+1)} \times V_s) \cap \{A_s \neq 0\}$ de dimensión $(n-s+2)(n+1)-2$, vemos que $\Phi_s(\{D_s = 0\})$ es una hipersuperficie de $(\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}) \cap \{A_s \neq 0\})$ definida, por lo tanto, por el polinomio $\widehat{B}_s$. Es decir, tenemos la identidad $\Phi_s(\{D_s = 0, A_s \neq 0\}) = \{\widehat{B}_s = 0, A_s \neq 0\}$.

Observemos que la hipersuperficie $\{A_s = 0\}$ no contiene ninguna de las componentes irreducibles de $\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}$. Esto implica que para cada componente irreducible $\mathcal{D}$ de $\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}$ el conjunto $\mathcal{D} \cap \{A_s \neq 0\}$ es denso en $\mathcal{D}$. Supongamos, por el momento, que existe una componente irreducible $\mathcal{D}$ de $\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}$ contenida en $\Phi_s^{-1}(\{\rho_s \widehat{B}_s = 0\})$. Entonces

$$\mathcal{D} \cap \{A_s \neq 0\} \subset \Phi_s^{-1}(\{\rho_s \widehat{B}_s = 0\}) \cap \{A_s \neq 0\} = \Phi_s^{-1}(\{\rho_s \widehat{B}_s = 0\} \cap \{A_s \neq 0\}),$$

lo que implica

$$\Phi_s(\mathcal{D} \cap \{A_s \neq 0\}) \subset \Phi_s \circ \Phi_s^{-1}(\{\rho_s \widehat{B}_s = 0\} \cap \{A_s \neq 0\}) \subset \{\rho_s \widehat{B}_s = 0\} \cap \{A_s \neq 0\}.$$

Concluimos que $\Phi_s(\mathcal{D}) \subset \{\rho_s \widehat{B}_s = 0\}$; pero esta conclusión es errónea. En efecto, podemos escribir $\mathcal{D} = \mathbb{A}^{(n-s+1)(n+1)} \times \mathcal{D}_0$ donde $\mathcal{D}_0$ es una componente irreducible de V_{s+1}. Sea $x \in \mathcal{D}_0$ un punto no singular de V_{s+1} y de V_s. Para una elección genérica de un punto $(\lambda, \gamma) \in \mathbb{A}^{(n-s+1)(n+1)}$, la fibra $V_s \cap \{\lambda^* X + \gamma^* = \lambda^* x + \gamma^*\}$ es no ramificada (ver e.g., [Mum95, §5A]) y la forma lineal $\lambda^{(n-s+1)} X + \gamma_{n-s+1}$ separa sus puntos. Esto muestra

que cualquier punto $y \in V_s \cap \{\lambda^* X + \gamma^* = \lambda^* x + \gamma^*\}$ satisface las condiciones $D_s(\lambda,\gamma,y) \neq 0$ y $\rho_s(\lambda,\gamma,y) \neq 0$. Por lo tanto el punto $(\lambda,\gamma,\lambda^* x + \gamma^*)$ pertenece a $\Phi_s(\mathcal{D}) \setminus \{\rho_s \widehat{B}_s = 0\}$, lo que contradice la condición $\Phi_s(\mathcal{D}) \subset \{\rho_s \widehat{B}_s = 0\}$. De esta forma completamos la demostración del lema. □

Ahora sí, pasamos a demostrar el Teorema 7.2.2.

Demostración del Teorema 7.2.2. Del Lema 7.2.6 y del Lema 7.2.3 deducimos que la imagen del morfismo

$$\begin{aligned}\Psi_s : (\mathbb{A}^{(n-s+1)(n+1)} \times V_{s+1}) \cap \{\rho_s \widehat{B}_s = 0, A_{s+1} \neq 0\} &\to \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s-1} \\ (\lambda,\gamma,x) &\mapsto \big(\lambda,\gamma,Y_1(x),\ldots,Y_{n-s-1}(x)\big)\end{aligned}$$

está contenida en una hipersuperficie de $\mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s-1}$ de grado a lo sumo $4(n-s+2)^2 n d \delta_s^2 \delta_{s+1}^2$. Sea $\widetilde{B}_s$ el polinomio que define esta hipersuperficie.

Estamos en condiciones de definir el polinomio del enunciado del teorema. Definimos $B_s := A_s A_{s+1} \rho_s \rho_{s+1} \widehat{B}_s \widehat{B}_{s+1} \widetilde{B}_s$. Considerando las cotas de grado de cada uno de sus factores, el polinomio B_s tiene grado acotado por $4(n-s+3)^2 n d \delta_s^2 \delta_{s+1}^2$. Sea $(\lambda,\gamma,P) \in \mathbb{A}^{(n-s+1)(n+1)} \times \mathbb{A}^{n-s}$ un punto tal que $B_s(\lambda,\gamma,P) \neq 0$. Afirmamos que (λ,γ,P) satisface las condiciones (i), (ii) y (iii) del enunciado del Teorema 7.2.2. Denotemos por (λ^*,γ^*) las primeras $n-s$ filas de (λ,γ) y por P^* el vector formado por las primeras $n-s-1$ coordenadas de P. Como $A_s(\lambda,\gamma) A_{s+1}(\lambda^*,\gamma^*) \neq 0$, de la Proposición 7.2.1 concluimos que las proyecciones π_s y π_{s+1} son morfismos finitos.

Dado que $A_s(\lambda,\gamma) \neq 0$, la condición $\widehat{B}_s(\lambda,\gamma,P) \neq 0$ implica que $D_s(\lambda,\gamma,x) \neq 0$ para cada $x \in \pi_s^{-1}(P)$. Por lo tanto, P es un punto de levantamiento de π_s. De manera similar mostramos que P^* es un punto de levantamiento de π_{s+1}.

Finalmente, las condiciones $\rho_s(\lambda,\gamma,P) \neq 0$ y $\rho_{s+1}(\lambda^*,\gamma^*,P^*) \neq 0$ muestran que Y_{n-s+1} y Y_{n-s} son elementos primitivos de $\pi_s^{-1}(P)$ y $\pi_{s+1}^{-1}(P^*)$, respectivamente. Por otro lado, las condiciones $\widetilde{B}_s(\lambda,\gamma,P^*) \neq 0$ y $A_{s+1}(\lambda^*,\gamma^*) \neq 0$ implican que, para cada $x \in \pi_{s+1}^{-1}(P^*)$, tenemos que $(\rho_s \widehat{B}_s)\big(\lambda,\gamma,P^*,Y_{n-s}(x)\big) \neq 0$. Dado que $A_s(\lambda,\gamma) \neq 0$, deducimos que $D_s(\lambda,\gamma,Q) \neq 0$ y que $\rho_s(\lambda,\gamma,\pi_s(Q)) \neq 0$ para cada $Q \in \pi_s^{-1}(P^*,Y_{n-s}(x))$ con $x \in \pi_{s+1}^{-1}(P^*)$. Esto muestra la condición (iii) del enunciado del Teorema 7.2.2.

□

La ventaja de tener a disposición el resultado anterior es que nos va a permitir determinar de antemano las formas lineales y los puntos de levantamiento necesarios en cada etapa de algoritmo. Es decir, eligiendo adecuadamente $(\lambda,\gamma,P) \in \mathbb{A}^{n(n+1)} \times \mathbb{A}^{n-1}$ quedan determinadas n formas lineales $\lambda X + \gamma = (Y_1,\ldots,Y_n)$ y un punto $P = (p_1,\ldots,p_{n-1})$ tales que para cada $s = 1,\ldots,n-r$ se satisfacen simultáneamente *todas* las condiciones enunciadas en el Teorema 7.2.2. Posteriormente, determinaremos un cuerpo finito donde esta elección puede llevarse a cabo con buena probabilidad de éxito. En el próximo teorema

brindamos una cota superior sobre el grado de un polinomio cuya no anulación implica los resultados mencionados.

Teorema 7.2.7. *Existe un polinomio* $B \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \tilde{Y}]$ *de grado acotado por* $4n^4 d\Delta^4$ *tal que para cada* $(\lambda, \gamma, P) \in \mathbb{A}^{n(n+1)} \times \mathbb{A}^{n-1}$ *con* $B(\lambda, \gamma, P) \neq 0$ *se verifican simultáneamente las condiciones del Teorema 7.2.2 para cada* $s = 1, \ldots, n-r-1$.

Demostración. Para cada $1 \leq s \leq n-r-1$, consideramos el polinomio $B_s \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \tilde{Y}]$ proporcionado por el Teorema 7.2.2 y definimos $B := \det \Lambda \prod_{s=1}^{n-r-1} B_s$. Teniendo en cuenta las cotas de grado de sus factores, el polinomio B tiene grado acotado por $4n^4 d\Delta^4$.

Sea $(\lambda, \gamma, P) \in \mathbb{A}^{n(n+1)} \times \mathbb{A}^{n-1}$ un punto que no anula al polinomio B. Como $\det \lambda \neq 0$ entonces $Y = \lambda X + \gamma$ es un cambio lineal de coordenadas. Dado que $B_s(\lambda, \gamma, P) \neq 0$ para cada s, son válidas las condiciones enunciadas en el Teorema 7.2.2. □

Sin embargo, dado que V es una $\mathbb{F}_q$–variedad estamos interesados en obtener formas lineales $Z_1, \ldots, Z_{r+1} \in \mathbb{F}_q[X_1, \ldots, X_n]$ y un punto $P \in \mathbb{F}_q^r$ de modo que la proyección $\pi : V \to \mathbb{A}^r$ en $Z_1, \ldots, Z_r$ sea un morfismo finito, que P sea punto de levantamiento y que la forma Z_{r+1} sea un elemento primitivo de la fibra $\pi^{-1}(P)$. La existencia de estas formas lineales y del punto P no puede ser garantizada a menos que el cuerpo finito $\mathbb{F}_q$ tenga suficiente cantidad de elementos. Por lo tanto, deberíamos encontrar una condición genérica cuyo grado proporcione la regularidad necesaria para que estos hechos puedan acontecer sobre $\mathbb{F}_q$. El resultado siguiente proporciona una tal condición genérica que depende del grado de la variedad δ mas que del grado geométrico Δ.

Corolario 7.2.8. *Si* $q > (r+2)(2nd\delta^2 - \delta)$ *existen formas lineales* $Z_1, \ldots, Z_{r+1} \in \mathbb{F}_q[X_1, \ldots, X_n]$ *y un punto* $P \in \mathbb{F}_q^r$ *tales que el morfismo proyección* $\pi : V \to \mathbb{A}^r$ *en* $Z_1, \ldots, Z_r$ *es finito,* $P \in \mathbb{A}^r$ *es un punto de levantamiento de* π *y* Z_{r+1} *es un elemento primitivo de la fibra* $\pi^{-1}(P)$.

Demostración. Consideremos el polinomio $\widehat{B} := A_{n-r} \widehat{B}_{n-r} \rho_{n-r} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_r]$, donde A_{n-r} es el polinomio de la Proposición 7.2.1 para $s = n-r$, $\widehat{B}_{n-r}$ es el polinomio de la prueba del Teorema 7.2.2 con $s = n-r-1$ y ρ_{n-r} es el discriminante correspondiente (en este caso Λ es una matriz de indeterminadas de tamaño $(r+1) \times n$ y Γ es un vector de $r+1$ indeterminadas). Observemos que $\deg \widehat{B} \leq (r+2)(2nd\delta^2 - \delta)$. Como la cantidad de elementos de $\mathbb{F}_q$ es mayor que $(r+2)(2nd\delta^2 - \delta)$ de la Proposición 3.1.3 deducimos que podemos elegir $(\lambda, \gamma, P) \in \mathbb{F}_q^{(r+1)(n+1)} \times \mathbb{F}_q^r$ que no anula a $\widehat{B}$ y mediante el cual definimos las formas lineales $\lambda X + \gamma = (Z_1, \ldots, Z_{r+1})$. Argumentando de manera similar al último parágrafo de la demostración del Teorema 7.2.2 tenemos que las formas lineales $Z_1, \ldots, Z_{r+1}$ y el punto P satisfacen las condiciones enunciadas. □

7.3. Reducción al caso bidimensional

En esta sección culminamos nuestras consideraciones sobre la preparación de los datos de entrada, reduciendo el problema de calcular un punto q–racional de la $\mathbb{F}_q$–variedad absolutamente irreducible V al de calcular un punto q–racional de una $\mathbb{F}_q$–curva absolutamente irreducible. Para esto, disponemos del primer teorema de Bertini (ver e.g., [Sha94, §II.6.1, Theorem 1]), el cual afirma que la intersección de V con una variedad lineal genérica $L \subset \mathbb{A}^n$ de dimensión $n-r+1$ es una curva absolutamente irreducible.Vamos a exhibir una cota superior para el grado de la condición genérica que subyace a la elección de L.

Sea $(\lambda,\gamma,P) \in \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^r$ tal que $\widehat{B}(\lambda,\gamma,P) \neq 0$, donde $\widehat{B}$ es el polinomio del Corolario 7.2.8. Sea $(Z_1,\ldots,Z_{r+1}) = \lambda X + \gamma$ y sean $Y_{r+2},\ldots,Y_n$ formas lineales tales que $Z_1,\ldots,Z_{r+1},Y_{r+2},\ldots,Y_n$ son $\overline{\mathbb{F}}_q$–linealmente independientes, y sea $P := (p_1,\ldots,p_r)$. La proyección $\pi : V \to \mathbb{A}^r$ definida por $\pi(x) := \big(Z_1(x),\ldots,Z_r(x)\big)$ es un morfismo finito, y por lo tanto la imagen $W := \widetilde{\pi}(V)$ de V bajo la aplicación $\widetilde{\pi} : V \to \mathbb{A}^{r+1}$ definida por $\widetilde{\pi}(x) := \big(Z_1(x),\ldots,Z_{r+1}(x)\big)$ es una hipersuperficie de $\mathbb{A}^{r+1}$. La elección de las formas lineales $Z_1,\ldots,Z_{r+1}$ implica que esta hipersuperficie tiene grado δ y está definida por un polinomio $m \in \overline{\mathbb{F}}_q[Z_1,\ldots,Z_{r+1}]$, mónico en Z_{r+1}.

Teorema 7.3.1. *Sean $\Omega := (\Omega_1,\ldots,\Omega_r)$ y T nuevas indeterminadas. Existe un polinomio no nulo $C \in \overline{\mathbb{F}}_q[\Omega]$ de grado a lo sumo $2\delta^4$ tal que si $\omega := (\omega_1,\ldots,\omega_r) \in \mathbb{A}^r$ no anula a C y $L_\omega \subset \mathbb{A}^n$ es la variedad lineal de dimensión $n-r+1$ parametrizada por $Z_k = \omega_k T + p_k$ $(1 \leq k \leq r)$, entonces $V \cap L_\omega$ es una variedad afín absolutamente irreducible de dimensión 1.*

Demostración. De la Proposición 5.1.2 deducimos que V es birracionalmente equivalente a la hipersuperficie $W \subset \mathbb{A}^{r+1}$ definida por el polinomio $m(Z_1,\ldots,Z_{r+1})$. Como V es absolutamente irreducible, W lo es y, por lo tanto, m es un polinomio absolutamente irreducible. Siguiendo a [Kal95], consideramos $\widetilde{m} \in \overline{\mathbb{F}}_q[\Omega,T][Z_{r+1}]$ el polinomio definido como $\widetilde{m} := m\big(\Omega_1 T + p_1,\ldots,\Omega_r T + p_r, Z_{r+1}\big)$. Observemos que $\widetilde{m}$ es un elemento mónico de $\overline{\mathbb{F}}_q[\Omega,T][Z_{r+1}]$

La demostración de la Proposición 5.1.1 muestra que la elección de P implica que el discriminante del polinomio $m(P,Z_{r+1})$ es no nulo; pero $\widetilde{m}(\Omega,0,Z_{r+1}) = m(P,Z_{r+1})$, con lo cual $\widetilde{m}(\Omega,0,Z_{r+1})$ es un elemento separable de $\overline{\mathbb{F}}_q[\Omega][Z_{r+1}]$.

Aplicando [Kal95, Theorem 5] concluimos que existe un polinomio $C \in \overline{\mathbb{F}}_q[\Omega]$ de grado acotado por $\frac{3}{2}\delta^4 - 2\delta^3 + \frac{1}{2}\delta^2 \leq 2\delta^4$ tal que para $\omega \in \mathbb{A}^r$ con $C(\omega) \neq 0$, el polinomio $\widetilde{m}(\omega,T,Z_{r+1})$ es absolutamente irreducible. De aquí deducimos immediatamente el teorema. □

8 Una fibra de levantamiento de V definida sobre una extensión de $\mathbb{F}_q$

Este capítulo marca el inicio concreto de nuestro algoritmo para calcular un punto q–racional de una $\mathbb{F}_q$–variedad V absolutamente irreducible definida por una sucesión regular de $\mathbb{F}_q[X_1,\ldots,X_n]$. A partir de las cotas de grado sobre las condiciones genéricas que atraviesan este proceso, vamos a considerar una extensión finita K de $\mathbb{F}_q$, y obtener una sección lineal de dimensión cero definida sobre K de nuestra variedad de entrada V. Este procedimiento (recursivo) constituye la primera etapa del algoritmo.

8.1. Sobre el modelo algorítmico y el costo de las operaciones

Los algoritmos en teoría de eliminación se describen usualmente codificando polinomios multivariados por el vector de todos sus coeficientes, no nulos en el caso ralo (sparse). Esta descripción conlleva una dificultad, en cierto modo insalvable: un polinomio genérico en n indeterminadas de grado d tiene $\binom{d+n}{n} = O(d^n)$ coeficientes no nulos, con lo cual la representación densa o rala de polinomios multivariados requiere tamaño exponencial y su manipulación requiere usualmente un número exponencial de operaciones aritméticas con respecto a n y a d. Para evitar estos contratiempos es que codificaremos los datos de entrada, de salida y todos los resultados intermedios de nuestros cálculos por medio de *esquemas de evaluación* o, su equivalente en inglés, straight–line programs (cf. [vzG86], [Hei89], [Str90], [Par95], [BCS97]).

Definición 8.1.1. *Sea* K *un cuerpo arbitrario. Un* straight–line program β *en el cuerpo* $K(X_1,\ldots,X_n)$ *es una sucesión finita de funciones racionales* $(F_1,\ldots,F_k) \in K(X_1,\ldots,X_n)^k$ *tales que para cada* $1 \leq i \leq k$, F_i *es un elemento de* $\{X_1,\ldots,X_n\}$, *o bien un elemento de* K *(un* parámetro*), o existen* $1 \leq i_1, i_2 < i$ *tales que* $F_i = F_{i_1} \circ_i F_{i_2}$, *donde* $\circ_i$ *representa alguna de las operaciones aritméticas* $+,-,\times,\div$.

Decimos que un straight–line program β es *libre de divisiones* si $\circ_i$ es diferente de $\div$ para $1 \leq i \leq k$.

Surge naturalmente la necesidad de «medir» la complejidad de β. Una medida adecuada para este fin es el *tiempo* (cf. [vzG86], [BCS97], [Sav98]). Definimos el tiempo como la cantidad total de operaciones aritméticas realizadas durante la evaluación del

straight–line program. Decimos que el straight–line program β *calcula*, *representa* o *evalúa* un subconjunto S de $K(X_1,\ldots,X_n)$ si $S \subset \{F_1,\ldots,F_k\}$.

Sin embargo, un modelo de computación basado solo en straight–line programs presenta algunas limitaciones ya que nuestro modelo incluye decisiones y selecciones (sujetas a su vez, a previas decisiones). Consideraremos entonces *redes aritméticas*, que son straight–line programs con *ramificaciones* (*branchings*). El tiempo de evaluación de una red aritmética se define de manera análoga al caso de straight–line programs (ver e.g., [vzG86], [BCS97] para más precisiones sobre la noción de red aritmética).

Otra cuestión a resolver cuando trabajamos con polinomios con coeficientes en un cuerpo K es el *identity testing problem*, el cual, en forma general puede enunciarse del siguiente modo:

Problema. *Dado un polinomio* $F \in K[X_1,\ldots,X_n]$ *(representado mediante una cierta estructura de datos) decidir si representa la función nula sobre* K.

Los primeros trabajos que dieron cuenta de este problema (presentando algoritmos probabilísticos para su tratamiento) fueron publicados de manera casi simultánea por R. Zippel [Zip79] y J. Schwartz [Sch80]. En este trabajo, seguimos sus ideas, haciendo un uso constante de lo que se conoce como Lema de Zippel-Schwartz, ya enunciado como Teorema 3.3.3, y que ahora reenunciamos.

Teorema 8.1.2. *Sea* $F \in \mathbb{F}_q[X_1,\ldots,X_n]$ *un polinomio de grado a lo sumo* d *y sea* $\mu > 0$. *Si* K *es una extensión finita de* $\mathbb{F}_q$ *tal que* $|K| > \mu d$ *entonces la probabilidad de elegir al azar* $a \in K^n$ *tal que* $F(a) \neq 0$ *es mayor que* $1 - 1/\mu$.

En cuanto al costo de las operaciones aritméticas que llevaremos a cabo, consideramos para cada $m \in \mathbb{N}$ la constante $M(m) := m \log^2 m \log\log m$. Esta constante está relacionada con el costo de las operaciones básicas de enteros y polinomios.

Los algoritmos a los que recurrimos (algoritmo de Euclides, cálculo de resultantes, interpolación, factorización de polinomios univariados sobre un cuerpo finito, etc.) y los correspondientes resultados de complejidad, son los que se presentan en el texto [vzGG99]. También constituyen buenas referencias los textos [BP94], [GCL92], [BCS97].

La multiplicación, división y máximo común divisor de enteros de talla bit m es de orden $O(M(m))$. Si R es un anillo conmutativo, el número de operaciones aritméticas en R de la multiplicación y la división de polinomios de $R[T]$, de grado a lo sumo m, puede llevarse a cabo con $O(m \log m \log\log m)$.

El máximo común divisor de dos polinomios, de grado a lo sumo m, sobre un cuerpo K puede efectuarse con $O(M(m))$ operaciones aritméticas en K. El cálculo de resultantes e interpolación tiene la misma complejidad.

Un elemento cualquiera de un cuerpo finito $\mathbb{F}_q$ tiene talla bit $O(\log q)$. En particular, una operación aritmética en un cuerpo finito $\mathbb{F}_q$ puede realizarse en forma determinística con $O(M(\log q))$ operaciones bit.

8.2. Una solución geométrica de V

El Teorema 7.2.7 muestra la existencia de un polinomio B en $n(n+1)+n-1$ indeterminadas, de grado acotado por $4n^4d\Delta^4$, de modo que, cada vez que tomamos $(\lambda,\gamma,P)\in \mathbb{A}^{n(n+1)}\times\mathbb{A}^{n-1}$ con $B(\lambda,\gamma,P)\neq 0$, definiendo las formas lineales $\lambda X+\gamma=(Y_1,\ldots,Y_n)$, y escribiendo $P=(p_1,\ldots,p_{n-1})$, logramos que para cada $s=1,\ldots,n-r-1$ se verifica simultáneamente:

- El morfismo $\pi_s: V_s\to\mathbb{A}^{n-s}$, la proyección en las formas lineales $Y_1,\ldots,Y_{n-s}$, es finito y la forma lineal Y_{n-s+1} induce un elemento primitivo de la extensión entera de anillos $\overline{\mathbb{F}}_q[Y_1,\ldots,Y_{n-s}]\hookrightarrow\overline{\mathbb{F}}_q[V_s]$.
- El punto $P^{(s)}:=(p_1,\ldots,p_{n-s})\in\mathbb{A}^{n-s}$ conformado por las primeras $n-s$ coordenadas de P es un punto de levantamiento de π_s y Y_{n-s+1} es un elemento primitivo de la fibra $\pi_s^{-1}(P^{(s)})$.
- Cada punto $Q\in\pi_s\big(\pi_{s+1}^{-1}(P^{(s+1)})\big)$ es un punto de levantamiento de π_s y la forma lineal Y_{n-s+1} es un elemento primitivo de $\pi_s^{-1}(Q)$.

Consideremos un cuerpo finito K, que extiende a $\mathbb{F}_q$, de cardinal mayor que $60n^4d\Delta^4$. Considerando la cantidad de elementos de K y el Teorema 8.1.2 concluimos que la probabilidad de elegir $(\lambda,\gamma,P)\in K^{n(n+1)}\times K^{n-1}$ que no anule al polinomio B es mayor o igual que $14/15$. Supongamos entonces haber elegido $(\lambda,\gamma,P)\in K^{n(n+1)}\times K^{n-1}$.

Notemos que, como las formas lineales $Y_1,\ldots,Y_n$ pertenecen a $K[Y_1,\ldots,Y_n]$ y $P\in K^{n-1}$, cada una de las fibras de levantamiento $V_{P^{(s)}}$ es una K–variedad.

Todavía resta introducir algunas notaciones. El polinomio minimal de la función coordenada inducida por Y_{n-s+1} en la extensión entera $\overline{\mathbb{F}}_q[Y_1,\ldots,Y_{n-s}]\hookrightarrow\overline{\mathbb{F}}_q[V_s]$ será denotado por $m^{(s)}$. Es un elemento de $\overline{\mathbb{F}}_q[Y_1,\ldots,Y_{n-s+1}]$ de grado δ_s y define una K–hipersuperficie de $\mathbb{A}^{n-s+1}$ birracionalmente equivalente a V_s, con lo cual podemos suponer entonces que $m^{(s)}$ pertenece a $K[Y_1,\ldots,Y_{n-s+1}]$. De la demostración de la Proposición 5.1.2 concluimos que existe una solución geométrica de V_s conformada por $m^{(s)}$ y por polinomios $v_{n-s+2}^{(s)},\ldots,v_n^{(s)}$ en $K[Y_1,\ldots,Y_{n-s+1}]$.

Esta solución geométrica de V_s resulta compatible con $P^{(s)}$, ya que el discriminante de $m^{(s)}$ respecto de Y_{n-s+1} no se anula en $P^{(s)}$. De este modo, los polinomios $m^{(s)}(P^{(s)},Y_{n-s+1}),v_{n-s+k}^{(s)}(P^{(s)},Y_{n-s+1})$ $(2\leq k\leq s)$ forman una solución geométrica de la fibra $V_{P^{(s)}}$ con Y_{n-s+1} como elemento primitivo y el grado de $V_{P^{(s)}}$ es igual a δ_s.

En las circunstancias anteriores, vamos a exhibir un algoritmo que calcula una solución geométrica de una fibra de levantamiento K–definible $V_{P^{(n-r)}}$ de la variedad V. Este algoritmo que calcula una solución geométrica de $V_{P^{(n-r)}}$ es un procedimiento recursivo que procede en $r-1$ pasos. En el paso s–ésimo calculamos una solución geométrica de la fibra de levantamiento $V_{P^{(s+1)}}$ a partir de una solución geométrica de la fibra de levantamiento $V_{P^{(s)}}$. Este cálculo se divide en dos etapas principales:

1. La primera, que podemos denominar *De la fibra a la curva*, es la más sencilla. Aplicando la versión efectiva del operador de Newton de [GLS01], «levantamos» la solución geométrica de la fibra $V_{P^{(s)}}$ a una solución geométrica de la siguiente K–variedad equidimensional de dimensión 1 (ver la Sección 8.3):

$$W_{P^{(s+1)}} := V_s \cap \{Y_1 = p_1, \ldots, Y_{n-s-1} = p_{n-s-1}\}.$$

   La variedad $W_{P^{(s+1)}}$ se denomina una *curva de levantamiento*. La curva $W_{P^{(s+1)}}$ puede describirse como el conjunto de ceros comunes de los polinomios $Y_1 - p_1, \ldots, Y_{n-s-1} - p_{n-s-1}, F_1, \ldots, F_s$ y, en particular, la fibra $V_{P^{(s)}}$ está contenida en $W_{P^{(s+1)}}$.

2. La segunda etapa, denominada *De la curva a la fibra*, consiste en construir a partir de la solución geométrica de la curva $W_{P^{(s+1)}}$ obtenida en la primera etapa, una solución geométrica para la fibra de levantamiento $V_{P^{(s+1)}} = W_{P^{(s+1)}} \cap V(F_{s+1})$. Esto lo haremos del siguiente modo: calculamos la ecuación minimal de Y_{n-s-1} en $V_{P^{(s+1)}}$ (ver la Sección 8.4.1) y posteriormente, obtenemos las parametrizaciones por los ceros de esta ecuación minimal aplicando una versión efectiva del clásico Shape Lemma (ver la Sección 8.4.2).

Un punto importante en nuestro algoritmo es que en todo momento tratamos con polinomios en una o dos variables. Esto permite tratar con la escritura densa de los mismos sin aumentar la complejidad.

8.3. De la fibra a la curva

En esta sección describimos como calcular una solución geométrica de la curva de levantamiento $W_{P^{(s+1)}}$ a partir de una solución geométrica de la fibra de levantamiento $V_{P^{(s)}}$. Fijemos entonces s con $1 \leq s \leq n-r-1$.

Consideremos los polinomios $m^{(s)}(P^{(s)}, Y_{n-s+1}), v^{(s)}_{n-s+k}(P^{(s)}, Y_{n-s+1})$ $(2 \leq k \leq s)$, los cuales forman una solución geométrica de $V_{P^{(s)}}$ con Y_{n-s+1} como elemento primitivo.

Obtendremos una solución geométrica de $W_{P^{(s+1)}}$ aplicando el operador de Newton–Hensel global de [GLS01]. De acuerdo a las hipótesis sobre la curva $W_{P^{(s+1)}}$, la proyección de $W_{P^{(s+1)}}$ en $\mathbb{A}^1$ definida por Y_{n-s} y el punto de levantamiento $P^{(s)}$, tenemos que $W_{P^{(s+1)}}$ consiste de δ_s «ramas» analíticas que están sobre $Y_{n-s} = p_{n-s}$. La intersección de cada una de estas «ramas» con el hiperplano $Y_{n-s} = p_{n-s}$ consiste de un punto distinto de la fibra de levantamiento $V_{P^{(s)}}$. En consecuencia, por la no ramificación de $P^{(s)}$ tenemos que, aplicando el operador de Newton–Hensel usual no arquimediano en el anillo $\overline{\mathbb{F}}_q[\![Y_{n-s} - p_{n-s}]\!]$, a partir de cada punto de $V_{P^{(s)}}$ es posible obtener aproximaciones (no arquimedianas) de orden de precisión arbitrario de la correspondiente rama de la curva $W_{P^{(s+1)}}$.

El apelativo global del operador de Newton–Hensel de [GLS01] tiene que ver con que éste calcula simultáneamente aproximaciones de todas las ramas de $W_{P^{(s+1)}}$ que están sobre $Y_{n-s} = p_{n-s}$. En lo que sigue, vamos a aplicar este operador a fin de calcular el polinomio minimal $m_F \in \overline{\mathbb{F}}_q[Y_{n-s}, Y_{n-s+1}]$ de un elemento $F \in \overline{\mathbb{F}}_q[W_{P^{(s+1)}}]$ en la extensión de anillos $\overline{\mathbb{F}}_q[Y_{n-s}] \hookrightarrow \overline{\mathbb{F}}_q[W_{P^{(s+1)}}]$. Dado que conocemos cotas sobre el grado del polinomio minimal m_F, aunque trabajemos con series de potencias truncadas, podemos garantizar que después de un número, fijado de antemano, de iteraciones, llegamos a la solución correcta.

Para poder aplicarlo es necesario que $W_{P^{(s+1)}}$ satisfaga ciertas condiciones geométricas adecuadas. Denotamos por I_s el siguiente ideal de $K[Y_1, \ldots, Y_n]$:

$$I_s := (F_1(Y_1, \ldots, Y_n), \ldots, F_s(Y_1, \ldots, Y_n), Y_1 - P_1, \ldots, Y_{n-s-1} - P_{n-s-1}).$$

Nuestro próximo resultado muestra que estamos en condiciones de aplicar el operador de Newton global a la fibra de levantamiento $V_{P^{(s)}}$ para obtener una solución geométrica de la curva $W_{P^{(s+1)}}$.

Lema 8.3.1. *$W_{P^{(s+1)}}$ es una K–variedad equidimensional de dimensión 1 y grado δ_s definida por el ideal radical I_s.*

Demostración. Probamos, en primer lugar, que $W_{P^{(s+1)}}$ es una curva mostrando que los polinomios que definen el ideal I_s forman una sucesión regular de $K[Y_1, \ldots, Y_n]$. Sea L^n la variedad lineal definida por el sistema de ecuaciones $Y_1 = p_1, \ldots, Y_{n-s-1} = p_{n-s-1}$ en $\mathbb{A}^n$ y, para cada $1 \leq i \leq s$, sea L^{n-i} la variedad lineal definida por el mismo sistema de ecuaciones en $\mathbb{A}^{n-i}$. Observemos que para $1 \leq i \leq s$ tenemos que

$$\{F_j(P^{(s+1)}, Y_{n-s}, \ldots, Y_n) = 0; 1 \leq j \leq i\} = V_i \cap L^n = \pi_i^{-1}(L^{n-i}).$$

Como π_i es un morfismo finito, tenemos que $\dim V_i \cap L^n = \dim L^{n-i} = n - i - (n - s - 1) = s + 1 - i$ para $1 \leq i \leq s$. Esto implica que $W_{P^{(s+1)}} = V_s \cap L^n$ es equidimensional de dimensión 1.

Mostramos, a continuación, que la curva $W_{P^{(s+1)}}$ tiene grado δ_s. De la Desigualdad de Bézout (2.1) deducimos fácilmente que $\deg W_{P^{(s+1)}} \leq \delta_s$. Como π_s es un morfismo finito, la restricción $\pi_s|_{W_{P^{(s+1)}}} : W_{P^{(s+1)}} \to L^{n-s}$ también lo es. Además, el punto $P^{(s)}$ es un punto de levantamiento, con lo cual

$$|(\pi_s|_{W_{P^{(s+1)}}})^{-1}(P^{(s)})| = |\pi_s^{-1}(P^{(s)})| = \delta_s.$$

En consecuencia,

$$\delta_s = |\pi_s^{-1}(P^{(s)})| = |W_{P^{(s+1)}} \cap \{Y_{n-s} = p_{n-s}\}| \leq \deg W_{P^{(s+1)}} \leq \delta_s.$$

Es decir, $W_{P^{(s+1)}}$ tiene grado δ_s.

Resta probar que I_s es un ideal radical. Como $P^{(s)}$ es un punto de levantamiento del morfismo π_s, del Lema 2.1.9 concluimos que el determinante de la matriz

$$\left(\partial F_i(P^{(s+1)}, Y_{n-s}, \ldots, Y_n)/\partial Y_{n-s+j}\right)_{1\leq i,j\leq s}$$

no se anula en ningún punto de $V_{P^{(s)}} = W_{P^{(s+1)}} \cap \{Y_{n-s} = p_{n-s}\}$. Más aún, de $|V_{P^{(s)}}| = \delta_s = \deg W_{P^{(s+1)}}$, podemos afirmar que la variedad lineal $\{Y_{n-s} = p_{n-s}\}$ interseca cada componente irreducible de $W_{P^{(s+1)}}$. Entonces la función coordenada de $W_{P^{(s+1)}}$ definida por el determinante de la matriz precedente no es un divisor de 0 en $\overline{\mathbb{F}}_q[W_{P^{(s+1)}}]$ y de [Eis95, Theorem 18.15] concluimos que I_s es radical.

□

Estamos ahora en condiciones de exhibir un algoritmo que calcula una solución geométrica de la curva de levantamiento $W_{P^{(s+1)}}$ a partir de una solución geométrica de la fibra $V_{P^{(s)}}$.

Proposición 8.3.2. *Teniendo como datos de entrada*

- *un straight–line program que evalúa los polinomios* $F_1, \ldots, F_s$ *en tiempo* $\mathcal{T}$,
- *la representación densa de elementos de* $K[Y_{n-s+1}]$ *que forman una solución geométrica de* $V_{P^{(s)}}$,

puede calcularse en forma determinística la representación densa de polinomios de $K[Y_{n-s}, Y_{n-s+1}]$ *que constituyen una solución geométrica de* $W_{P^{(s+1)}}$ *con* $O\big((n\mathcal{T} + n^5)M(\delta_s)^2\big)$ *operaciones en* K.

Demostración. En primer lugar, la curva de levantamiento $W_{P^{(s+1)}}$ es naturalmente isomorfa a la curva $W^*_{P^{(s+1)}} \subset \mathbb{A}^{s+1}$, mediante la proyección en $\mathbb{A}^{s+1}$ definida por $Y_{n-s}, \ldots, Y_n$. Esta proyección permite identificar la fibra de levantamiento $V_{P^{(s)}}$ con la variedad

$$V^*_{P^{(s)}} := W^*_{P^{(s+1)}} \cap \{Y_{n-s} = p_{n-s}\}.$$

Más aún, la fibra genérica de la proyección $\widehat{\pi}_{s+1} : W^*_{P^{(s+1)}} \to \mathbb{A}^1$ inducida por Y_{n-s} tiene cardinal δ_s –decimos que la proyección es un morfismo finito genéricamente no ramificado de grado δ_s. En particular, la fibra $V^*_{P^{(s)}}$ es no ramificada y tiene cardinal δ_s.

Los polinomios $m^{(s)}(P^{(s)}, Y_{n-s+1}), \nu^{(s)}_{n-s+k}(P^{(s)}, Y_{n-s+1})$ $(2 \leq k \leq s)$, introducidos antes del enunciado del Lema 8.3.1, forman una solución geométrica de $V^*_{P^{(s)}}$. Estamos en condiciones entonces de aplicar el operador de Newton global de [GLS01, II.4] y concluir que existe una red aritmética β en K que calcula una solución geométrica de $W^*_{P^{(s+1)}}$, que es, al mismo tiempo, una solución geométrica de $W_{P^{(s+1)}}$. Como la solución geométrica

de $V^*_{P(s)}$ consiste de polinomios univariados con coeficientes en K, la solución geométrica de $W_{P(s+1)}$ también está formada por polinomios con coeficientes en K.

La evaluación de la red aritmética β requiere $O\big((n\mathcal{T}+n^5)M(\delta_s)^2\big)$ operaciones aritméticas en K.

□

8.4. De la curva a la fibra

8.4.1. La intersección

Si bien ya disponemos de un elemento primitivo de la fibra $V_{P(s+1)}$, para llevar adelante el algoritmo necesitaremos cambiar de elemento primitivo y calcular los correspondientes minimales de estos elementos primitivos. En esta sección, entonces, mostramos un algoritmo que calcula la ecuación minimal del elemento de $\overline{\mathbb{F}}_q[V_{P(s+1)}]$ inducido por la forma lineal $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$ para una elección adecuada de $\lambda \in K$.

Con el objeto de facilitar la lectura, en esta sección aligeraremos la notación del siguiente modo:

- el punto de levantamiento $P^{(s+1)}$ será denotado por P;
- la fibra de levantamiento $V_{P(s+1)}$ será denotada por V_P;
- la curva de levantamiento $W_{P(s+1)}$ será denotada por W_P.

Sin embargo, los resultados obtenidos se enunciarán en términos de $P^{(s+1)}$, $V_{P(s+1)}$ y $W_{P(s+1)}$. La notación establecida será utilizada tanto en las argumentaciones previas y posteriores, como durante el transcurso de la demostración de los mismos.

Dado $\lambda \in \mathbb{A}^1$ consideramos la forma lineal $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$ y la proyección $\pi_\lambda : W_P \to \mathbb{A}^1$ definida por $\pi_\lambda(x) := \mathcal{L}_\lambda(x)$. Nuestro próximo resultado proporciona una condición suficiente (y consistente) sobre λ, que asegura que reemplazar la variable Y_{n-s} por $\mathcal{L}_\lambda$ no modifica la situación obtenida en la Sección 7.2, es decir π_λ es un morfismo finito y cada elemento de $\pi_\lambda(V_P)$ define una fibra no ramificada de π_λ. Para eso introducimos una indeterminada Λ.

Lema 8.4.1. *Existe un polinomio no nulo $E_s \in \overline{\mathbb{F}}_q[\Lambda]$ de grado acotado por $4\Delta^3$, tal que para cada $\lambda \in \mathbb{A}^1$ con $E_s(\lambda) \neq 0$ se verifican las siguientes condiciones:*

(i) *La proyección $\pi_\lambda : W_{P(s+1)} \to \mathbb{A}^1$ definida por $\mathcal{L}_\lambda$ es un morfismo finito.*

(ii) *$\mathcal{L}_\lambda$ separa los puntos de la fibra de levantamiento $V_{P(s+1)}$.*

(iii) *Cada elemento de $\pi_\lambda(V_{P(s+1)})$ es un punto de levantamiento de π_λ.*

Demostración. La elección de las formas lineales $Y_1,\dots,Y_{n-s+1}$ y del punto P implica que la función coordenada definida por Y_{n-s+1} es un elemento primitivo de la extensión entera de anillos $\overline{\mathbb{F}}_q[Y_{n-s}] \hookrightarrow \overline{\mathbb{F}}_q[W_P]$, cuyo polinomio minimal es $m^{(s)}(P,Y_{n-s+1})$. Además, $\overline{\mathbb{F}}_q[W_P]$ es un $\overline{\mathbb{F}}_q[Y_{n-s}]$–módulo libre de rango δ_s.

En primer lugar, vamos a determinar una condición genérica para (i). Consideremos la forma lineal $\mathcal{L}_\Lambda := Y_{n-s} + \Lambda Y_{n-s+1}$ y denotemos por $m_\Lambda^{(s)}$ el siguiente elemento de $K[\Lambda, Y_1,\dots,Y_{n-s-1},\mathcal{L}_\Lambda,Y_{n-s+1}]$:

$$m_\Lambda^{(s)} := m^{(s)}(Y_1,\dots,Y_{n-s-1},\mathcal{L}_\Lambda - \Lambda Y_{n-s+1},Y_{n-s+1}).$$

Como $m^{(s)}$ tiene grado δ_s y $\mathcal{L}_\Lambda - \Lambda Y_{n-s+1}$ es lineal tanto en $\mathcal{L}_\Lambda, Y_{n-s+1}$ como en $\mathcal{L}_\lambda,\Lambda$, entonces

$$\deg_{\mathcal{L}_\Lambda,Y_{n-s+1}} m_\Lambda^{(s)} \le \delta_s, \quad \deg_{\mathcal{L}_\Lambda,\Lambda} m_\Lambda^{(s)} \le \delta_s.$$

Evaluando $m_\Lambda^{(s)}$ en P podemos escribir:

$$m_\Lambda^{(s)}(\Lambda,P,\mathcal{L}_\Lambda,Y_{n-s+1}) = a_{\delta_s}(\Lambda)Y_{n-s+1}^{\delta_s} + a_{\delta_s-1}(\Lambda,\mathcal{L}_\Lambda)Y_{n-s+1}^{\delta_s-1} + \cdots + a_0(\Lambda,\mathcal{L}_\Lambda),$$

donde $a_{\delta_s},\dots,a_0$ son elementos de $K[\Lambda,\mathcal{L}_\Lambda]$ de grado acotado por δ_s. Dado que

$$m_\Lambda^{(s)}(0,P,Y_{n-s},Y_{n-s+1}) = m^{(s)}(P,Y_{n-s},Y_{n-s+1})$$

y que $m^{(s)}(P,Y_{n-s},Y_{n-s+1})$ es un elemento mónico de $K[Y_{n-s}][Y_{n-s+1}]$ de grado δ_s en Y_{n-s+1}, concluimos que el coeficiente principal a_{δ_s} es un elemento no nulo de $K[\Lambda]$ (de grado acotado por δ_s). Probaremos luego que si $\lambda \in \mathbb{A}^1$ y $a_{\delta_s}(\lambda) \neq 0$ entonces se cumple la condición (i).

Supongamos que $V_P := \{Q_1,\dots,Q_{\delta_{s+1}}\}$ y consideremos el polinomio

$$E_{s,1}(\Lambda) = \prod_{1\le j<k\le\delta_{s+1}} \big(\mathcal{L}_\Lambda(Q_j) - \mathcal{L}_\Lambda(Q_k)\big).$$

Como Y_{n-s} separa los puntos de la fibra de levantamiento V_P, entonces $\mathcal{L}_\Lambda(Q_j) - \mathcal{L}_\Lambda(Q_k) \neq 0$ para $1 \le j < k \le \delta_{s+1}$, y por lo tanto $E_{s,1}$ es un elemento no nulo de $\overline{\mathbb{F}}_q[\Lambda]$ de grado a lo sumo δ_{s+1}^2. Mostraremos luego que si $\lambda \in \mathbb{A}^1$ y $E_{s,1}(\lambda) \neq 0$ entonces se cumple la condición (ii).

Finalmente, analizamos (iii). Consideremos la hipersuperficie de $\mathbb{A}^2$ definida por el siguiente polinomio:

$$m_{\mathcal{L}_\Lambda}^{(s+1)}(\Lambda,\mathcal{L}_\Lambda) := \prod_{1\le j\le\delta_{s+1}} (\mathcal{L}_\Lambda - \mathcal{L}_\Lambda(Q_j)) \in K[\Lambda,\mathcal{L}_\Lambda].$$

Esta hipersuperficie tiene grado δ_{s+1} y contiene al conjunto de puntos de la forma

$\big(\lambda, \mathcal{L}_\lambda(x)\big)$ con $\lambda \in A^1$ y $x \in V_P$. Afirmamos que $m^{(s+1)}_{\mathcal{L}_\Lambda}$ y el discriminante $\rho^{(s)}_\Lambda(\Lambda, P, \mathcal{L}_\Lambda) \in K[\Lambda, \mathcal{L}_\Lambda]$ del polinomio $m^{(s)}_\Lambda(\Lambda, P, \mathcal{L}_\Lambda, Y_{n-s+1})$ introducido anteriormente no tienen factores en común, no triviales, en $K(\Lambda)[\mathcal{L}_\Lambda]$. Supongamos, por el contrario, que tienen un factor común no trivial en $K(\Lambda)[\mathcal{L}_\Lambda]$. Dado que $m^{(s+1)}_{\mathcal{L}_\Lambda}$ es un elemento mónico de $K[\Lambda][\mathcal{L}_\Lambda]$, en realidad existe un factor común $h \in K[\Lambda, \mathcal{L}_\Lambda] \setminus K[\Lambda]$ no divisible por Λ. Teniendo en cuenta que $m^{(s+1)}_{\mathcal{L}_\Lambda}(0, Y_{n-s}) = m^{(s+1)}(P, Y_{n-s})$ y que $\rho^{(s)}_\Lambda(0, P, Y_{n-s})$ es igual al discriminante $\rho^{(s)}(P, Y_{n-s})$ de $m^{(s)}(P, Y_{n-s}, Y_{n-s+1})$ con respecto a Y_{n-s+1}, vemos que $h(0, Y_{n-s})$ es un factor común no trivial de $\rho^{(s)}(P, Y_{n-s})$ y $m^{(s+1)}(P, Y_{n-s})$. Sea $\alpha \in \overline{\mathbb{F}}_q$ una raíz de $h(0, Y_{n-s})$ y sea Q un punto de V_P tal que $\alpha = Y_{n-s}(Q)$. Luego, $(p_1, \ldots, p_{n-s-1}, \alpha) = \pi_s(Q)$ y el polinomio $m^{(s)}(\pi_s(Q), Y_{n-s+1})$ (de grado δ_s) no tiene δ_s raíces, dado que $\rho^{(s)}(\pi_s(Q)) = 0$. Es decir, o bien $\pi_s(Q)$ no es un punto de levantamiento de π_s, o bien Y_{n-s+1} no es un elemento primitivo de $\pi_s^{-1}(\pi_s(Q))$, contradiciendo la condición (iii) del Teorema 7.2.2. Esto prueba nuestra afirmación.

La resultante $E_{s,2} \in K[\Lambda]$ de $m^{(s+1)}_{\mathcal{L}_\Lambda}(\Lambda, \mathcal{L}_\Lambda)$ y $\rho^{(s)}_\Lambda(\Lambda, P, \mathcal{L}_\Lambda)$ con respecto a $\mathcal{L}_\Lambda$ es un elemento no nulo de $\overline{\mathbb{F}}_q[\Lambda]$ de grado a lo sumo $2(2\delta_s - 1)\delta_s\delta_{s+1}$ que proporciona una condición genérica necesaria para que se cumpla (iii).

Definimos entonces $E_s := a_{\delta_s} E_{s,1} E_{s,2}$. De las cotas de grado de cada uno de sus factores deducimos que E_s tiene grado menor o igual que $4\Delta^3$. Tomemos $\lambda \in \mathbb{A}^1$ que no anula a E_s y consideramos la forma lineal $\mathcal{L}_\lambda := Y_{n-s} + \lambda Y_{n-s+1}$. Definimos el siguiente polinomio de $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_{n-s-1}, \mathcal{L}_\lambda, Y_{n-s+1}]$:

$$m^{(s)}_\lambda := m^{(s)}_\Lambda(\lambda, Y_1, \ldots, Y_{n-s-1}, \mathcal{L}_\lambda, Y_{n-s+1}).$$

Estamos en condiciones de mostrar que se verifican (i), (ii) y (iii) del enunciado del Lema.

Comencemos mostrando la validez de (i). Para eso vamos a mostrar que $\overline{\mathbb{F}}_q[\mathcal{L}_\lambda] \hookrightarrow \overline{\mathbb{F}}_q[W_P]$ es una extensión entera de anillos. Escribimos $\ell_\lambda = y_{n-s} + \lambda y_{n-s+1}$, donde ℓ_λ, y_{n-s} y y_{n-s+1} denotan las funciones coordenadas de $\overline{\mathbb{F}}_q[W_P]$ inducidas por $\mathcal{L}_\lambda$, Y_{n-s} y Y_{n-s+1} respectivamente. De la identidad $m^{(s)}(P, y_{n-s}, y_{n-s+1}) = 0$ en $\overline{\mathbb{F}}_q[W_P]$, deducimos que $m^{(s)}_\lambda(\lambda, P, \ell_\lambda, y_{n-s+1}) = 0$ en $\overline{\mathbb{F}}_q[W_P]$ y, como $a_{\delta_s}(\lambda) \neq 0$, tenemos que $m^{(s)}_\lambda(P, \mathcal{L}_\lambda, Y_{n-s+1}) \in \overline{\mathbb{F}}_q[\mathcal{L}_\lambda][Y_{n-s+1}]$ representa una ecuación de dependencia entera sobre $\overline{\mathbb{F}}_q[\mathcal{L}_\lambda]$ para y_{n-s+1}. Por otro lado, el morfismo $\pi_\lambda : W_P \to \mathbb{A}^1$ resulta dominante (si así no fuera, la proyección de W_P en $\mathbb{A}^1$ definida por Y_{n-s} no sería dominante) con lo cual $\overline{\mathbb{F}}_q[\mathcal{L}_\lambda] \hookrightarrow \overline{\mathbb{F}}_q[\ell_\lambda, y_{n-s+1}]$ es inyectiva y, por lo tanto, es una extensión entera de anillos. Finalmente, la extensión $\overline{\mathbb{F}}_q[\ell_\lambda, y_{n-s+1}] \hookrightarrow \overline{\mathbb{F}}_q[W_P]$ es entera y por lo tanto, $\overline{\mathbb{F}}_q[\mathcal{L}_\lambda] \hookrightarrow \overline{\mathbb{F}}_q[W_P]$ es una extensión entera de anillos.

En segundo lugar, fácilmente mostramos que se verifica (ii). La forma $\mathcal{L}_\lambda$ separa los puntos de la fibra V_P pues $E_{s,1}(\lambda) = \prod_{1 \le i < j \le \delta_{s+1}} \big(\mathcal{L}_\lambda(Q_i) - \mathcal{L}_\lambda(Q_j)\big) \neq 0$.

Por último, nos abocamos a (iii). Sea Q un punto cualquiera de V_P. De $E_{s,2}(\lambda) \neq 0$,

el discriminante $\rho_\lambda^{(s)}(P,\mathcal{L}_\lambda)$ de $m_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$ con respecto a Y_{n-s+1} no se anula en $\mathcal{L}_\lambda(Q)$. Por lo tanto $m_\lambda^{(s)}(P,\mathcal{L}_\lambda(Q),Y_{n-s+1})$ tiene δ_s raíces distintas en $\overline{\mathbb{F}}_q$ y, en consecuencia, la fibra $\pi_\lambda^{-1}(\mathcal{L}_\lambda(Q))$ tiene δ_s puntos distintos; en otras palabras, es una fibra no ramificada.

□

Teniendo en cuenta que el cuerpo K tiene más de $60n^4d\Delta^4$ elementos, el Teorema 8.1.2 asegura que podemos elegir $\lambda\in K$ con probabilidad al menos $1-1/60n^4$ de obtener $E_s(\lambda)\neq 0$. Supongamos entonces que hemos elegido $\lambda\in K$ con la propiedad esperada y consideremos la correspondiente forma lineal $\mathcal{L}_\lambda := Y_{n-s}+\lambda Y_{n-s+1}$. A continuación presentamos un algoritmo que calcula la ecuación minimal de la función coordenada de $V_{P^{(s+1)}}$ inducida por $\mathcal{L}_\lambda$.

El inverso de $(\partial m_\lambda^{(s)}/\partial Y_{n-s+1})(P,\mathcal{L}_\lambda,Y_{n-s+1})$ módulo $m_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$ es un elemento de $K(\mathcal{L}_\lambda)[Y_{n-s+1}]$ de grado a lo sumo δ_s-1. Para cada $2\leq k\leq s$ representemos por $w_{n-s+k}^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})\in K(\mathcal{L}_\lambda)[Y_{n-s+1}]$ el resto módulo $m_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})$ de

$$v_{n-s+k}^{(s)}(P,\mathcal{L}_\lambda-\lambda Y_{n-s+1},Y_{n-s+1})(\partial m_\lambda^{(s)}/\partial Y_{n-s+1})^{-1}(P,\mathcal{L}_\lambda,Y_{n-s+1}).$$

Sean

$$f_{s+1} := F_{s+1}\big(P,\mathcal{L}_\lambda,Y_{n-s+1},w_{n-s+2}^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1}),\ldots,w_n^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1})\big),$$

y

$$g_{s+1} := \mathrm{Res}_{Y_{n-s+1}}\big(m_\lambda^{(s)}(P,\mathcal{L}_\lambda,Y_{n-s+1}),f_{s+1}\big), \tag{8.1}$$

donde $\mathrm{Res}_{Y_{n-s+1}}(f,g)$ denota la resultante de f y g con respecto a Y_{n-s+1}.

Observemos que $f_{s+1}\in K(\mathcal{L}_\lambda)[Y_{n-s+1}]$ es un polinomio de grado a lo sumo $d\delta_s$ en Y_{n-s+1} y que los denominadores de sus coeficientes son divisores de un polinomio de $K[\mathcal{L}_\lambda]$ de grado acotado por $(2\delta_s-1)\delta_s$. Por otro lado, de [GLS01, Corollary 2] se sigue que g_{s+1} es un elemento de $K[\mathcal{L}_\lambda]$ de grado a lo sumo $d\delta_s$. Nuestro próximo resultado muestra que podemos calcular de manera eficiente la ecuación minimal de $\mathcal{L}_\lambda$ en $K[V_P]$.

Proposición 8.4.2. *Teniendo como datos de entrada*

- *un straight–line program que representa a* F_{s+1} *en tiempo* $\mathcal{T}$,
- *una solución geométrica de la curva* $W_{P^{(s+1)}}$,
- $\lambda\in K$ *que verifica las condiciones del Lema 8.4.1,*

puede calcularse con $O\big((\mathcal{T}+n)M(d\delta_s)M(\delta_s)\big)$ *operaciones en* K *la representación densa del polinomio minimal* $m_{\mathcal{L}_\lambda}^{(s+1)}(P^{(s+1)},\mathcal{L}_\lambda)\in K[\mathcal{L}_\lambda]$ *de la función coordenada de* $V_{P^{(s+1)}}$ *inducida por* $\mathcal{L}_\lambda$, *con probabilidad de éxito mayor o igual que* $1-1/45n^3$.

Demostración. Sea $\lambda \in K$ un elemento que satisface las condiciones del Lema 8.4.1. En [HMW01, Lemma 8] se prueba la siguiente identidad:

$$m_{\mathcal{L}_\lambda}^{(s+1)}(P, \mathcal{L}_\lambda) = \frac{g_{s+1}}{\gcd(g_{s+1}, g'_{s+1})}.$$

Esta identidad permite reducir de manera eficiente el cálculo de $m_{\mathcal{L}_\lambda}^{(s+1)}(P, \mathcal{L}_\lambda)$ al del polinomio g_{s+1} de (8.1). A su vez, éste puede definirse como la resultante con respecto a la variable Y_{n-s+1} de dos elementos de $K(\mathcal{L}_\lambda)[Y_{n-s+1}]$ de grados acotados por δ_s y $\delta_s - 1$: $m_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ y el resto de f_{s+1} módulo $m_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$. Esta resultante se calcula aplicando el Algoritmo de Euclides Extendido (en forma abreviada, EEA) en $K(\mathcal{L}_\lambda)[Y_{n-s+1}]$ con $O\big(M(\delta_s)\big)$ operaciones aritméticas en $K(\mathcal{L}_\lambda)$ (ver [vzGG99, Corollary 11.16]). Además, el cálculo de f_{s+1} requiere la inversión modular de $(\partial m_\lambda^{(s)}/\partial Y_{n-s+1})^{-1}(P, \mathcal{L}_\lambda, Y_{n-s+1})$, que se calcula aplicando el EEA en $K(\mathcal{L}_\lambda)[Y_{n-s+1}]$ a los polinomios $m_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ y $(\partial m_\lambda^{(s)}/\partial Y_{n-s+1})(P, \mathcal{L}_\lambda, Y_{n-s+1})$.

Para calcular la representación densa de g_{s+1}, aplicaremos el EEA sobre un anillo de series de potencias $K[\![\mathcal{L}_\lambda - \alpha]\!]$, con $\alpha \in K$ un elemento tal que todos los elementos de $K[\mathcal{L}_\lambda]$ invertidos durante la ejecución del EEA sean unidades del anillo $K[\![\mathcal{L}_\lambda - \alpha]\!]$. Para que el algoritmo sea «efectivo», durante su ejecución calcularemos aproximaciones adecuadas en $K[\mathcal{L}_\lambda]$ de los resultados intermedios de nuestros cálculos, que son obtenidos truncando los desarrollos en series de potencias de $K[\![\mathcal{L}_\lambda - \alpha]\!]$ de estos resultados intermedios. Por lo tanto, tenemos que determinar el grado de precisión requerido para que, truncando las series de potencias obtengamos el resultado correcto.

De modo similar a la demostración de [vzGG99, Theorem 6.52], deducimos que todos los denominadores de los elementos de $K(\mathcal{L}_\lambda)$ que aparecen durante la aplicación del EEA a $m_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ y f_{s+1} son divisores de a lo sumo $\delta_s + 1$ polinomios de $K[\mathcal{L}_\lambda]$ de grado acotado por $(d\delta_s + \delta_s)(2\delta_s - 1)\delta_s$. Por otro lado, los denominadores que aparecen durante la aplicación del EEA a $m_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ y $(\partial m_\lambda^{(s)}/\partial Y_{n-s+1})(P, \mathcal{L}_\lambda, Y_{n-s+1})$ son divisores de a lo sumo $\delta_s + 1$ polinomios de $K[Y_{n-s}]$ de grado acotado por $(2\delta_s - 1)\delta_s$. Por lo tanto, el producto de todos los denominadores que aparecen durante las dos aplicaciones del EEA tiene grado acotado por $(d\delta_s + \delta_s + 1)(2\delta_s - 1)\delta_s(\delta_s + 1) \leq 4d\delta_s^4$. Como el cuerpo K tiene cardinal mayor que $60n^4 d\Delta^4$, del Teorema 8.1.2 concluimos que existe $\alpha \in K$ que no anula ninguno de los denominadores que aparecen como resultado intermedio del EEA. Más aún, la probabilidad de elegir al azar tal $\alpha \in K$ es al menos $1 - 1/45n^3$.

Como la salida de nuestro algoritmo es un polinomio de grado a lo sumo $d\delta_s$, bastará calcular las series de potencias que aparecen como resultados intermedios a orden $d\delta_s + 1$.

Finalmente, mostramos que las operaciones descritas previamente se llevan a cabo con las estimaciones de complejidad enunciadas.

En primer lugar, calculamos el inverso de $(\partial m_\lambda^{(s)}/\partial Y_{n-s+1})(P, \mathcal{L}_\lambda, Y_{n-s+1})$ módulo

$m_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$, calculamos $w_{n-s+k}^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$ para $2 \leq k \leq s$, luego calculamos f_{s+1} módulo $m_\lambda^{(s)}(P, \mathcal{L}_\lambda, Y_{n-s+1})$, y finalmente calculamos g_{s+1}. Todos estos cálculos se pueden llevar a cabo con $O\big((\mathcal{T}+n)M(\delta_s)\big)$ operaciones aritméticas en $K(\mathcal{L}_\lambda)$. Cada una de estas operaciones aritméticas se realiza en el anillo de series de potencias $K[\![\mathcal{L}_\lambda - \alpha]\!]$ a precisión $d\delta_s + 1$ con $O\big(M(d\delta_s)\big)$ operaciones aritméticas en K. En suma, el cálculo de g_{s+1} se realiza con $O\big((\mathcal{T}+n)M(d\delta_s)M(\delta_s)\big)$ operaciones aritméticas en K.

Finalmente, calculamos $g_{s+1}/\gcd(g_{s+1}, g'_{s+1})$ con $O\big(M(d\delta_s)\big)$ operaciones en K. □

El algoritmo delineado en la Proposición 8.4.2 no solo extiende el algoritmo de [GLS01, Algorithm II.7] a cuerpos finitos, sino que también proporciona estimaciones sobre la probabilidad de las elecciones que tienen lugar (no presentes en este último). Al mismo tiempo las estimaciones de complejidad de la Proposición 8.4.2 mejoran ostensiblemente las de [HMW01, Proposition 1].

8.4.2. Una solución geométrica de $V_{P^{(s+1)}}$

En esta sección vamos a presentar un algoritmo que calcula una parametrización de las variables $Y_{n-s+1}, \ldots, Y_n$ por los ceros de $m^{(s+1)}(P^{(s+1)}, Y_{n-s})$, completando de este modo, el s–ésimo paso recursivo del algoritmo principal.

Como en la sección anterior, para simplificar notaciones vamos a denotar el punto de levantamiento $P^{(s+1)}$ por P, la fibra de levantamiento $V_{P^{(s+1)}}$ por V_P y la curva de levantamiento $W_{P^{(s+1)}}$ por W_P.

Comenzamos discutiendo cómo obtener la parametrización de Y_{n-s+1} por los ceros de $m^{(s+1)}(P, Y_{n-s})$. Recordemos que tal parametrización está representada por

$$\frac{\partial m^{(s+1)}}{\partial Y_{n-s}}(P, Y_{n-s})Y_{n-s+1} - v_{n-s+1}^{(s+1)}(P, Y_{n-s}),$$

con $v_{n-s+1}^{(s+1)}(P, Y_{n-s})$ un polinomio con coeficientes en K de grado a lo sumo $\delta_{s+1} - 1$.

Sean λ_1 y λ_2 dos elementos no nulos de K que satisfacen las condiciones del Lema 8.4.1 y consideremos las correspondientes formas lineales $\mathcal{L}_i := Y_{n-s} + \lambda_i Y_{n-s+1}$, con $i = 1, 2$. Supongamos que disponemos de las ecuaciones minimales $m_1^{(s+1)}(P, \mathcal{L}_1)$, $m_2^{(s+1)}(P, \mathcal{L}_2)$ y $m^{(s+1)}(P, Y_{n-s})$ de $\mathcal{L}_1$, $\mathcal{L}_2$ e Y_{n-s} sobre $\overline{\mathbb{F}}_q[V_P]$, respectivamente (estas ecuaciones se calculan aplicando el algoritmo de la Proposición 8.4.2). Considerando estos polinomios como elementos de $K[Y_{n-s}, Y_{n-s+1}]$, supongamos además que $\mathcal{L}_2$ separa los ceros comunes de $m^{(s+1)}(P, Y_{n-s})$ y $m_1^{(s+1)}(P, \mathcal{L}_1)$. Argumentando como en la demostración del Lema 8.4.1, concluimos que existe un polinomio no nulo $\widehat{E}_s \in \overline{\mathbb{F}}_q[\Lambda]$ de grado acotado por Δ^4 tal que para cada λ_2 con $\widehat{E}_s(\lambda_2) \neq 0$, la forma lineal $\mathcal{L}_2$ satisface nuestra suposición.

Consideremos la siguiente K–variedad de dimensión 0:

$$W_{s+1} := \{(x_1, x_2) \in \mathbb{A}^2 : m^{(s+1)}(P, x_1) = 0, m_i^{(s+1)}(P, x_1 + \lambda_i x_2) = 0 \text{ para } i = 1, 2\}.$$

Si $\widetilde{\pi}_s : V_P \to \mathbb{A}^2$ representa la proyección en las formas lineales Y_{n-s}, Y_{n-s+1}, la variedad W_{s+1} es la imagen de $\widetilde{\pi}_s$. En efecto, como los ceros de cada uno de los minimales $m^{(s+1)}(P, T), m_1^{(s+1)}(P, T)$ y $m_2^{(s+1)}(P, T)$ se obtienen evaluando la forma lineal correspondiente en los puntos de la fibra V_P, tenemos que $\widetilde{\pi}_s(V_P) \subset W_{s+1}$. Por otro lado, la forma $\mathcal{L}_2$ separa los ceros comunes de $m^{(s+1)}(P, Y_{n-s})$ y $m_1^{(s+1)}(P, \mathcal{L}_1)$, y el polinomio $m_2^{(s+1)}(P, \mathcal{L}_2)$, de grado δ_{s+1}, se anula en el conjunto $\mathcal{L}_2\big(\widetilde{\pi}_s(V_P)\big)$ de cardinal δ_{s+1}. Concluimos que $W_{s+1} = \widetilde{\pi}_s(V_P)$.

La forma lineal Y_{n-s} separa los puntos de V_P con lo cual también separa los puntos de W_{s+1}. Esta es una variedad de dimensión 0 y grado δ_{s+1}. Aplicando la versión clásica del Shape Lemma a W_{s+1} (ver e.g., [CLO98]), vemos que existe un polinomio $w_{n-s+1} \in K[Y_{n-s}]$ de grado a lo sumo $\delta_{s+1} - 1$ tal que $Y_{n-s+1} - w_{n-s+1}(Y_{n-s})$ se anula en la variedad W_{s+1}.

Sea $\alpha \in \overline{\mathbb{F}}_q$ una raíz arbitraria de $m^{(s+1)}(P, Y_{n-s})$ y sea $\beta := w_{n-s+1}(\alpha)$. Como Y_{n-s} separa los puntos de W_{s+1} deducimos que (α, β) es el único punto de W_{s+1} cuya coordenada Y_{n-s} es igual a α. En consecuencia, $Y_{n-s+1} = \beta$ es la única raíz en común entre $m_1^{(s+1)}(P, \alpha + \lambda_1 Y_{n-s+1})$ y $m_2^{(s+1)}(P, \alpha + \lambda_2 Y_{n-s+1})$. El polinomio $m_2^{(s+1)}(P, \alpha + \lambda_2 Y_{n-s+1})$ no tiene factores múltiples –vista la elección de λ_2– y. por lo tanto, tenemos la siguiente identidad en $K(\alpha)[Y_{n-s+1}]$:

$$\gcd\Big(m_1^{(s+1)}(P, \alpha + \lambda_1 Y_{n-s+1}), m_2^{(s+1)}(P, \alpha + \lambda_2 Y_{n-s+1})\Big) = Y_{n-s+1} - \beta. \tag{8.2}$$

Consideremos la descomposición en factores irreducibles en $K[Y_{n-s}]$ del polinomio minimal $m^{(s+1)}(P, Y_{n-s})$:

$$m^{(s+1)}(P, Y_{n-s}) = h_1 \cdots h_N.$$

Podemos pensar que cada factor irreducible $h_j \in K[Y_{n-s}]$ se corresponde con una K–componente irreducible $\mathcal{C}_j$ de W_{s+1}. Si $\alpha_j \in \overline{\mathbb{F}}_q$ es una raíz arbitraria de h_j, tenemos el isomorfismo $K(\alpha_j) \simeq K[Y_{n-s}]/h_j(Y_{n-s})$. De (8.2), deducimos que existe un polinomio $v_j \in K[Y_{n-s}]$ de grado a lo sumo $\deg h_j - 1$, a partir del cual establecemos la siguiente identidad en $(K[Y_{n-s}]/h_j(Y_{n-s}))[Y_{n-s+1}]$:

$$\gcd\Big(m_1^{(s+1)}(P, Y_{n-s} + \lambda_1 Y_{n-s+1}), m_2^{(s+1)}(P, Y_{n-s} + \lambda_2 Y_{n-s+1})\Big) = Y_{n-s+1} - v_j(Y_{n-s}). \tag{8.3}$$

Deducimos entonces que $Y_{n-s+1} - v_j(Y_{n-s}) \equiv 0 \bmod I(\mathcal{C}_j)$ y, por lo tanto, que para

cada $1 \leq j \leq N$ tenemos que

$$h'_j\Big(\prod_{i\neq j} h_i\Big)(Y_{n-s+1} - v_j) \in I(W_{s+1}) \subset I(V_P).$$

Naturalmente, llegamos al polimomio que estamos buscando:

$$v^{(s+1)}_{n-s+1}(P, Y_{n-s}) := \sum_{1\leq j\leq N} h'_j v_j \prod_{i\neq j} h_i \mod m^{(s+1)}(P, Y_{n-s}). \tag{8.4}$$

De su propia definición, resulta que el polinomio $v^{(s+1)}_{n-s+1}(P, Y_{n-s})$ es un elemento de $K[Y_{n-s}]$ de grado a lo sumo $\delta_{s+1} - 1$, y que

$$\frac{\partial m^{(s+1)}}{\partial Y_{n-s}}(P, Y_{n-s})Y_{n-s+1} - v^{(s+1)}_{n-s+1}(P, Y_{n-s}) = \sum_{j=1}^{N} h'_j\Big(\prod_{i\neq j} h_i\Big)(Y_{n-s+1} - v_j)$$

pertenece al ideal $I(V_P)$. En suma, representa la parametrización de Y_{n-s+1} por los ceros de $m^{(s+1)}(P, Y_{n-s})$.

Estimamos la complejidad y la probabilidad de éxito del algoritmo recién descrito.

Lema 8.4.3. *El algoritmo recién descrito calcula*

- *el polinomio minimal* $m^{(s+1)}(P^{(s+1)}, Y_{n-s})$ *de la función coordenada inducida por* Y_{n-s} *en* $K[V_{P^{(s+1)}}]$*;*
- *la parametrización de* Y_{n-s+1} *por los ceros de* $m^{(s+1)}(P^{(s+1)}, Y_{n-s})$*,*

con $O\big((\mathcal{T} + n)M(\Delta)\big(M(d\Delta) + \log(q\Delta)\big)\big)$ *operaciones en* K *y probabilidad de éxito al menos* $1 - 1/60n$*.*

Demostración. Sea E_s el polinomio del enunciado del Lema 8.4.1 y sea $\widehat{E}_s$ el polinomio introducido al inicio de esta sección. Recordemos que $\deg E_s \leq 4\Delta^3$ y $\deg \widehat{E}_s \leq \Delta^4$. Aplicando el Teorema 8.1.2 elegimos λ_1 y λ_2 elementos distintos de K tales que $E_s(\lambda_1)E_s(\lambda_2)\widehat{E}_s(\lambda_2) \neq 0$ con probabilidad de éxito al menos $1 - 1/72n^3$. Una vez elegidos estos valores quedan determinadas las formas lineales $\mathcal{L}_i = Y_{n-s} + \lambda_i Y_{n-s+1}$ con $i = 1, 2$. El algoritmo presentado en la Proposición 8.4.2, nos permite calcular las ecuaciones minimales $m^{(s+1)}(P, Y_{n-s}), m_1^{(s+1)}(P, \mathcal{L}_1)$ y $m_2^{(s+1)}(P, \mathcal{L}_2)$ de $Y_{n-s}, \mathcal{L}_1$ y $\mathcal{L}_2$, respectivamente, con $O\big((\mathcal{T} + n)M(d\delta_s)M(\delta_s)\big)$ operaciones en K y con probabilidad de éxito al menos $1 - 1/15n^3$ (esta probabilidad proviene de aplicar tres veces este algoritmo).

La factorización en $K[Y_{n-s}]$ del minimal $m^{(s+1)}(P, Y_{n-s})$ puede llevarse a cabo con $O\big(\log(n)\big(M(\delta^2_{s+1}) + M(\delta_{s+1})\log(q\Delta)\big)\big)$ operaciones en K y con probabilidad de éxito al menos $1 - 1/16n^3$ (ver [vzGG99, Corollary 14.30]).

Finalmente, para calcular los polinomios $v_1, \ldots, v_N$ de (8.3) y el polinomio $v^{(s+1)}_{n-s+1}$ de (8.4), aplicamos el Algoritmo de Euclides extendido. Esto se lleva a cabo en forma

determinística con $O(\delta_{s+1}M(\delta_s))$ operaciones en K (ver [vzGG99, Corollary 11.16]). Sumando las estimaciones de complejidad y probabilidad de cada paso del algoritmo, obtenemos el resultado enunciado. □

Resta obtener las parametrizaciones de las variables $Y_{n-s+2},\dots,Y_n$.

Lema 8.4.4. *Dada una solución geométrica de $W_{P^{(s+1)}}$ y la salida del algoritmo del Lema 8.4.3, los polinomios $v_{n-s+2}^{(s+1)}(P^{(s+1)},Y_{n-s}),\dots,v_n^{(s+1)}(P^{(s+1)},Y_{n-s})$ que parametrizan las variables $Y_{n-s+2},\dots,Y_n$ por los ceros de $m^{(s+1)}(P^{(s+1)},Y_{n-s})$ pueden calcularse en forma determinística con $O(s\Delta M(\Delta))$ operaciones en K.*

Demostración. En primer lugar, escribimos $m'(P,Y_{n-s})$ para representar el inverso de la derivada $(\partial m^{(s+1)}/\partial Y_{n-s})(P,Y_{n-s})$ módulo $m^{(s+1)}(P,Y_{n-s})$; es un polinomio con coeficientes en K de grado a lo sumo δ_{s+1}.

A partir de la parametrización de Y_{n-s+1}, escribiendo

$$w_{n-s+1}(P,Y_{n-s}) := m'(P,Y_{n-s})v_{n-s+1}^{(s+1)}(P,Y_{n-s})$$

tenemos que $Y_{n-s+1}-w_{n-s+1}(P,Y_{n-s})$ pertenece al ideal $I(V_P)$. Observemos que como los polinomios que conforman la solución geométrica de $W_{P^{(s+1)}}$ pertenecen al ideal $I(V_P)$, reemplazando en ellos Y_{n-s+1} por w_{n-s+1} obtenemos nuevos polinomios que también pertenecen al ideal $I(V_P)$.

Deducimos de la condición (iii) del Teorema 7.2.2 que el discriminante $\rho^{(s)}(P,Y_{n-s})$ no tiene raíces en común con $m^{(s+1)}(P,Y_{n-s})$. Esto implica que la clase del polinomio $(\partial m^{(s)}/\partial Y_{n-s+1})\big(P,Y_{n-s},w_{n-s+1}\big)$ es una unidad del anillo $K[Y_{n-s}]/\big(m^{(s+1)}(P,Y_{n-s})\big)$. En consecuencia, si $b_{n-s+1}\in K[Y_{n-s}]$ denota su inverso módulo $m^{(s+1)}(P,Y_{n-s})$, se desprende que $Y_{n-s+k}-b_{n-s+1}\cdot v_{n-s+k}^{(s)}\big(P,Y_{n-s},w_{n-s+1}\big)$ pertenece al ideal $I(V_P)$. Escribiendo entonces

$$w_{n-s+k} := b_{n-s+1}\cdot v_{n-s+k}^{(s)}\big(P,Y_{n-s},w_{n-s+1}\big)\quad (2\le k\le s), \tag{8.5}$$

tenemos que los polinomios $Y_{n-s+2}-w_{n-s+2},\dots,Y_n-w_n$ pertenecen a $I(V_P)$. Multiplicando w_{n-s+k} por $(\partial m^{(s+1)}/\partial Y_{n-s})(P,Y_{n-s})$ $(2\le k\le s)$, y reduciendo módulo $m^{(s+1)}(P,Y_{n-s})$, obtenemos los polinomios $v_{n-s+k}^{(s+1)}\in K[Y_{n-s}]$ $(2\le k\le s)$ que estamos buscando.

Estimemos el costo de las operaciones realizadas. Calculamos con $O(M(\delta_s))$ operaciones en K el polinomio $m'(P,Y_{n-s})$. Los polinomios b_{n-s+1} y w_{n-s+k} $(2\le k\le s)$ de (8.5) pueden calcularse con $O(s\delta_s M(\delta_{s+1}))$ operaciones en K. Finalmente, los polinomios $v_{n-s+k}^{(s+1)}(P,Y_{n-s})$ $(2\le k\le s)$ pueden calcularse con la misma complejidad. □

En definitiva, como consecuencia de la Proposición 8.4.2 y los Lemas 8.4.3 y 8.4.4,

podemos presentar un algoritmo para calcular los polinomios

$$m^{(s+1)}(P, Y_{n-s}), v^{(s+1)}_{n-s+k}(P, Y_{n-s}) \in K[Y_{n-s}], (1 \leq k \leq s)$$

que forman una solución geométrica de V_P. La proposición siguiente resume las estimaciones de complejidad y probabilidad de este algoritmo.

Proposición 8.4.5. *El algoritmo subyacente a la Proposición 8.4.2 y los Lemas 8.4.3 y 8.4.4 tiene como entrada*

- *un straight–line program en tiempo $\mathcal{T}$ que representa el polinomio F_{s+1},*
- *los polinomios $m^{(s)}(P^{(s+1)}, Y_{n-s}, Y_{n-s+1})$ y $v^{(s)}_{n-s+k}(P^{(s+1)}, Y_{n-s}, Y_{n-s+1})$ $(2 \leq k \leq s)$, que forman una solución geométrica de la curva de levantamiento $W_{P^{(s+1)}}$ calculada en la Proposición 8.3.2,*

y devuelve una solución geométrica de la fibra de levantamiento $V_{P^{(s+1)}}$ con $O\big((\mathcal{T} + n)M(\Delta)\big(M(d\Delta) + \log(q\Delta)\big)\big)$ operaciones en K, con probabilidad de éxito al menos $1 - 1/60n$.

El algoritmo precedente extiende al caso de característica positiva los algoritmos de [HMW01] y [GLS01], tiene una mejor complejidad asintótica (en términos del número de operaciones aritméticas realizadas) que [HMW01], y similar a la de [GLS01]. También hemos contribuido a este último al proveer estimaciones sobre la probabilidad de éxito del algoritmo, estimaciones que no estaban explicitadas en [GLS01]. Finalmente, es importante señalar que, gracias a nuestro preprocesamiento, hemos simplificado notablemente los algoritmos de [HMW01] y [GLS01].

8.5. Una solución geométrica de V definida sobre K

En esta sección, estamos en condiciones de describir el algoritmo que calcula una solución geométrica K–definible de nuestra variedad de entrada V. Recordemos que el cuerpo K es una extensión finita de $\mathbb{F}_q$ y que $|K| > 60n^4 d\Delta^4$. Para un punto (λ, γ, P) elegido al azar en $K^{n(n+1)} \times K^{n-1}$, si B es el polinomio del Teorema 7.2.7, deducimos que $B(\lambda, \gamma, P)$ es distinto de cero con probabilidad al menos $14/15$. Supongamos entonces que hemos elegido este punto. Por lo tanto, podemos aplicar de manera recursiva los algoritmos presentados en las Proposiciones 8.3.2 y 8.4.5, que calculan sucesivamente una solución geométrica de la curva de levantamiento $W_{P^{(s+1)}}$, y de la fibra de levantamiento $V_{P^{(s+1)}}$. De esta manera, al final del $(n-r-1)$–ésimo paso recursivo obtenemos una solución geométrica de la fibra de levantamiento $V_{P^{(n-r)}}$. Para simplificar, de ahora en adelante la denotaremos V_P. Teniendo en cuenta las estimaciones de complejidad y probabilidad de las Proposiciones 8.3.2 y 8.4.5, obtenemos el siguiente teorema:

Teorema 8.5.1. *El algoritmo descrito anteriormente calcula una solución geométrica, definida sobre* K*, de la fibra de levantamiento* V_P *del sistema de entrada* $F_1 = \cdots = F_{n-r} = 0$*, con* $O\big((n\mathcal{T}+n^5)M(\Delta)\big(M(d\Delta)+\log(q\Delta)\big)\big)$ *operaciones en* K *y devuelve el resultado correcto con probabilidad al menos* $1-1/12$*.*

La estimación de complejidad del Teorema 8.5.1 mejora de manera significativa la estimación de complejidad $O(d^{n^2})$ de [HW99], la estimación $O(d^{2r})$ de [HW00] y las estimaciones de los algoritmos que utilizan bases de Gröbner. Señalemos también que combinando este algoritmo con técnicas de levantamiento p–ádico, como las de [GLS01], para una elección adecuada del primo p, se obtiene un algoritmo probabilístico eficiente para calcular una solución geométrica de una variedad equidimensional sobre $\mathbb{Q}$ definida por una sucesión regular reducida.

9 Una fibra de levantamiento de V definida sobre $\mathbb{F}_q$

El objetivo de este capítulo es el de caracterizar el pasaje de la solución geométrica de la fibra V_P definida sobre K –esta solución geométrica fue obtenida en el capítulo anterior– a una solución geométrica de una fibra de levantamiento de una proyección $\mathbb{F}_q$–definible, con un punto de levantamiento con coordenadas en $\mathbb{F}_q$ y un elemento primitivo dado por una forma lineal con coeficientes en $\mathbb{F}_q$. El polinomio minimal de la forma lineal tendrá coeficientes en $\mathbb{F}_q$ mientras que las parametrizaciones de las variables dependientes tendrán coeficientes en K.

Para eso vamos a «deformar» las formas lineales $Y_1,\ldots,Y_r$ en nuevas formas lineales $Z_1,\ldots,Z_r \in \mathbb{F}_q[X_1,\ldots,X_n]$. La deformación se define como una homotopía del estilo $(1-T)Y_j + TZ_j$ para $1 \leq j \leq r+1$, donde T es una nueva indeterminada. El cálculo de esta solución geométrica tiene un doble interés: por un lado, nos permitirá obtener un punto q–racional de V y por otro, permite que la condición de regularidad bajo la cual el algoritmo funciona correctamente, dependa solo del grado de la variedad δ y no del grado geométrico Δ.

9.1. Formas lineales definidas sobre $\mathbb{F}_q$

Sea $(\lambda,\gamma,P) \in K^{n(n+1)} \times K^r$ el punto fijado en la Sección 8.2 y consideremos las formas lineales $Y_1,\ldots,Y_n$ y el punto $P := (p_1,\ldots,p_r)$ que quedan determinados.

Si M es una matriz de $m \times n$ vamos a denotar por $M^{[1:i]}$ la submatriz de M de tamaño $i \times n$, formada por las primeras i filas de M $(1 \leq i \leq m)$.

Introducimos una matriz de indeterminadas $\Lambda = (\Lambda_{ij})_{1\leq i\leq r+1, 1\leq j\leq n}$ de tamaño $(r+1)\times n$, un vector de indeterminadas $\Gamma := (\Gamma_1,\ldots,\Gamma_{r+1})$ y formas lineales genéricas $\widetilde{Y} := (\widetilde{Y}_1,\ldots,\widetilde{Y}_{r+1}) := \Lambda X + \Gamma$.

Lema 9.1.1. *Si $q > 8n^2d\delta^4$ es posible elegir en forma aleatoria, con probabilidad de éxito mayor o igual que 1- 1/16 un punto (ν,η,Q) en $\mathbb{F}_q^{(r+1)(n+1)} \times \mathbb{F}_q^r$ de modo que, definiendo las formas lineales $Z := (Z_1,\ldots,Z_{r+1}) := \nu X + \eta$,*

1. *los conjuntos de formas lineales $Z_1,\ldots,Z_r,Y_{r+1},\ldots,Y_n$ y $Z_1,\ldots,Z_{r+1}$, $Y_{r+2},\ldots,Y_n$ inducen cambios lineales de coordenadas;*

2. *el morfismo* $\pi: V \to \mathbb{A}^r$ *definido por* $Z_1, \ldots, Z_r$ *es finito,* Q *es punto de levantamiento de* π *y* Z_{r+1} *es un elemento primitivo de la fibra de levantamiento* $V_Q := \pi^{-1}(Q)$.

Demostración. Vamos a considerar dos matrices de tamaño $n \times n$. Una de ellas, Δ_1, es la matriz que tiene a $\Lambda^{[1:r]}$ como submatriz de $r \times n$ en sus primeras r filas y los coeficientes de las formas lineales $Y_{r+1}, \ldots, Y_n$ en las últimas $n-r$ filas; la otra, Δ_2, es la matriz que tiene a $\Lambda^{[1:r+1]}$ como submatriz de $(r+1) \times n$ en sus primeras $r+1$ filas y los coeficientes de las formas lineales $Y_{r+1}, \ldots, Y_n$ en las últimas $n-r-1$ filas. Al mismo tiempo, volvemos al polinomio $\widehat{B}$, el polinomio obtenido en el Corolario 7.2.8. Definimos el polinomio $B' := \det(\Delta_1)\det(\Delta_2)\widehat{B} \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_r]$. El grado de B' es menor o igual que $2(r+2)nd\delta^2$ y $\mathbb{F}_q$ tiene más de $8n^2d\delta^4$ elementos; en consecuencia, el Teorema 8.1.2 asegura que podemos elegir aleatoriamente un elemento (ν, η, Q) en $\mathbb{F}_q^{(r+1)(n+1)} \times \mathbb{F}_q^r$ con probabilidad al menos $1 - 1/16$ de no anular a B'.

Luego de realizada la elección podemos mostrar que se cumplen las condiciones enunciadas en el Lema. Que $\det(\Delta_1\Delta_2(\nu))$ sea distinto de cero implica que los conjuntos de formas lineales inducen cambios lineales de coordenadas. Por otro lado, como $\widehat{B}(\nu, \eta, Q)$ es distinto de cero del Corolario 7.2.8, deducimos que se verifica la segunda condición del enunciado del lema. □

Elegimos $(\nu, \eta, Q) \in \mathbb{F}_q^{(r+1)(n+1)} \times \mathbb{F}_q^r$ que satisfaga las condiciones del Lema 9.1.1. En otras palabras, disponemos de una matriz ν de tamaño $(r+1) \times n$ con coeficientes en $\mathbb{F}_q$ y un vector $\eta := (\eta_1, \ldots, \eta_{r+1}) \in \mathbb{F}_q^{r+1}$ –los cuales dan lugar a las formas lineales $Z_1, \ldots, Z_{r+1}$– y de un punto de levantamiento $Q := (q_1, \ldots, q_r) \in \mathbb{F}_q^r$.

Introducimos ahora nueva indeterminada T y definimos una matriz $\widehat{\Lambda} \in K[T]^{n \times n}$ y un vector columna $\widehat{\Gamma} \in K[T]^n$ del siguiente modo:

$$\begin{aligned} \widehat{\Lambda} &:= (1-T)\lambda + T\Delta_1(\nu^{[1:r]}), \\ \widehat{\Gamma} &:= (1-T)\gamma^t + T(\eta_1, \ldots, \eta_r, \gamma_{r+1}, \ldots, \gamma_n)^t. \end{aligned}$$

Sea $W \subset \mathbb{A}^n\big(\overline{\mathbb{F}_q(T)}\big)$ la variedad que definen $F_1, \ldots, F_{n-r}$ en $\overline{\mathbb{F}_q(T)}^n$. Escribimos $\widehat{Z} := (\widehat{Z}_1, \ldots, \widehat{Z}_n) := \widehat{\Lambda}X + \widehat{\Gamma}$ y $\widehat{P} := (\widehat{p}_1, \ldots, \widehat{p}_r) := (1-T)P + TQ$. Como $\widehat{\Lambda}$ es un elemento inversible de $\overline{\mathbb{F}_q(T)}^{n \times n}$, tenemos que $X = \widehat{\Lambda}^{-1}(\widehat{Z} - \widehat{\Gamma})$; de aquí, cada uno de los polinomios $\widehat{F}_j := F_j(\widehat{\Lambda}^{-1}(\widehat{Z} - \widehat{\Gamma}))$ es un elemento de $\overline{\mathbb{F}}_q(T)[\widehat{Z}_1, \ldots, \widehat{Z}_n]$, para $1 \le j \le n-r$. Observemos que el punto $(\widehat{\Lambda}, \widehat{\Gamma}, \widehat{P}) \in \mathbb{A}^{n(n+1)}\big(\overline{\mathbb{F}_q(T)}\big) \times \mathbb{A}^r\big(\overline{\mathbb{F}_q(T)}\big)$ no anula al polinomio $\widehat{B}$ del enunciado del Corolario 7.2.8. Entonces, reemplazando el cuerpo $\overline{\mathbb{F}}_q$ por $\overline{\mathbb{F}_q(T)}$, de este Corolario 7.2.8 se desprende que la extensión de anillos $\overline{\mathbb{F}_q(T)}[\widehat{Z}_1, \ldots, \widehat{Z}_r] \hookrightarrow \overline{\mathbb{F}_q(T)}[X_1, \ldots, X_n]/(F_1, \ldots, F_{n-r})$ es entera , que $\widehat{P}$ es un punto de levantamiento de la proyección lineal $\pi^e : W \to \overline{\mathbb{F}_q(T)}^r$ definida por $\widehat{Z}_1, \ldots, \widehat{Z}_r$, y que $\widehat{Z}_{r+1} = Y_{r+1}$ es un elemento primitivo de la fibra de levantamiento $W_{\widehat{P}} := (\pi^e)^{-1}(\widehat{P})$.

Denotemos por $\widehat{m}_{\widehat{Z}_{r+1}} := \widehat{m}_{\widehat{Z}_{r+1}}(\widehat{P}, \widehat{Z}_{r+1}) \in \overline{\mathbb{F}_q(T)}[\widehat{Z}_{r+1}]$ la ecuación minimal de $\widehat{Z}_{r+1}$ en $\overline{\mathbb{F}_q(T)}[W_{\widehat{P}}]$. Como $W_{\widehat{P}}$ y $\widehat{Z}_{r+1}$ son $K(T)$–definibles, vemos que $\widehat{m}_{\widehat{Z}_{r+1}}$ es un elemento de $K(T)[\widehat{Z}_{r+1}]$. Es más, nuestra elección de $\widehat{P}$ y $\widehat{Z}_1, \ldots, \widehat{Z}_{r+1}$ implica que $\widehat{m}_{\widehat{Z}_{r+1}}$ es un elemento separable de $K(T)[\widehat{Z}_{r+1}]$ de grado δ. Llamemos $\widehat{\rho} \in K[T]$ al producto entre su denominador y el numerador del discriminante de $\widehat{m}_{\widehat{Z}_{r+1}}$ con respecto a $\widehat{Z}_{r+1}$. Vamos a trabajar en el anillo local $K[T]_{\widehat{\rho}}$, pero previamente necesitamos el siguiente resultado:

Lema 9.1.2. *Los polinomios* $\widehat{F}_1(\widehat{P}, Y_{r+1}, \ldots, Y_n), \ldots, \widehat{F}_{n-r}(\widehat{P}, Y_{r+1}, \ldots, Y_n)$ *forman una sucesión regular y generan un radical ideal* $\widehat{I}_{\widehat{P}}$ *de* $K[T]_{\widehat{\rho}}[Y_{r+1}, \ldots, Y_n]$. *Además la extensión de anillos*

$$K[T]_{\widehat{\rho}} \hookrightarrow K[T]_{\widehat{\rho}}[Y_{r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}} \tag{9.1}$$

es una extensión entera de rango δ.

Demostración. Supongamos que la sucesión no es regular. Entonces existe $1 \leq j \leq n-r$ tal que $\widehat{F}_j(\widehat{P}, Y_{r+1}, \ldots, Y_n)$ es un divisor de cero módulo el ideal generado por los polinomios $\widehat{F}_1(\widehat{P}, Y_{r+1}, \ldots, Y_n), \ldots, \widehat{F}_{j-1}(\widehat{P}, Y_{r+1}, \ldots, Y_n)$. Si reemplazamos $T = 0$ en estos polinomios, el polinomio $F_j(P, Y_{r+1}, \ldots, Y_n)$ es un divisor de cero módulo el ideal generado por $F_1(P, Y_{r+1}, \ldots, Y_n), \ldots, F_{j-1}(P, Y_{r+1}, \ldots, Y_n)$, contradiciendo el Lema 8.3.1. Por lo tanto, $\widehat{F}_1(\widehat{P}, Y_{r+1}, \ldots, Y_n), \ldots, \widehat{F}_{n-r}(\widehat{P}, Y_{r+1}, \ldots, Y_n)$ constituyen una sucesión regular. De manera similar mostramos que el determinante de la matriz jacobiana de los polinomios $\widehat{F}_1(\widehat{P}, Y_{r+1}, \ldots, Y_n), \ldots, \widehat{F}_{n-r}(\widehat{P}, Y_{r+1}, \ldots, Y_n)$ respecto de $Y_{r+1}, \ldots, Y_n$ no es un divisor de cero módulo el ideal $\widehat{I}_{\widehat{P}}$. De [Eis95, Theorem 18.15] concluimos que el ideal $\widehat{I}_{\widehat{P}}$ es radical.

Observemos que, dado que estamos considerando polinomios con coeficientes en el anillo $K[T]_{\widehat{\rho}}$, el elemento $\widehat{m}_{\widehat{Z}_{r+1}} \in K[T]_{\widehat{\rho}}[\widehat{Z}_{r+1}]$ proporciona una ecuación de dependencia entera para la función coordenada $\widehat{z}_{r+1}$ inducida por $\widehat{Z}_{r+1}$ en la extensión de anillos (9.1) y, por lo tanto, la extensión de anillos $K[T]_{\widehat{\rho}} \hookrightarrow K[T]_{\widehat{\rho}}[\widehat{z}_{r+1}]$ es entera.

Si denotamos por $\xi_1, \ldots, \xi_n$ las funciones coordenadas de $K[T]_{\widehat{\rho}}[Y_{r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}}$ inducidas por $X_1, \ldots, X_n$ y argumentamos como en (5.2) de la demostración de la Proposición 5.1.1, probamos la existencia de polinomios $\widehat{P}_1, \ldots, \widehat{P}_n \in K[T]_{\widehat{\rho}}[\widehat{Z}_{r+1}]$ tales que $\xi_k = \widehat{P}_k(\widehat{z}_{r+1})$ $(1 \leq k \leq n)$ y que hacen que la extensión $K[T]_{\widehat{\rho}}[\widehat{z}_{r+1}] \hookrightarrow K[T]_{\widehat{\rho}}[\xi_1, \ldots, \xi_n]$ $= K[T]_{\widehat{\rho}}[Y_{r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}}$ sea una extensión entera de anillos. En suma, la extensión (9.1) es entera.

Resta mostrar que $K[T]_{\widehat{\rho}}[Y_{r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}}$ es un $K[T]_{\widehat{\rho}}$–módulo libre de rango δ. El rango es a lo sumo δ y, dado que $\widehat{m}_{\widehat{Z}_{r+1}}(\widehat{P}, \widehat{Z}_{r+1})$ es la ecuación de dependencia entera minimal de $\widehat{z}_{r+1}$ en la extensión (9.1), y tiene justamente grado δ, concluimos que el rango de $K[T]_{\widehat{\rho}}[Y_{r+1}, \ldots, Y_n]/\widehat{I}_{\widehat{P}}$ como $K[T]_{\widehat{\rho}}$–módulo libre es δ. □

Consideremos la variedad afín equidimensional $\widehat{V} \subset \mathbb{A}^{n-r+1}$ definida por el ideal $\widehat{I}_{\widehat{P}}$ y sea $\widehat{\pi} : \widehat{V} \to \mathbb{A}^1$ el morfismo inducido por la proyección en la coordenada T. Del Lema

9.1.2 se desprende que $\widehat{V}$ es una variedad de dimensión 1 y grado δ, y que $\widehat{\pi}$ es un morfismo dominante.

Lema 9.1.3. *Una solución geométrica de la fibra V_Q con Y_{r+1} como elemento primitivo puede calcularse con $O\big((n\mathcal{T}+n^5)M(\delta)^2\big)$ operaciones en K.*

Demostración. Observemos en primer lugar que $\widehat{V}\cap\{T=0\}=\{0\}\times V_P$ y que $T=0$ es punto de levantamiento del morfismo $\widehat{\pi}$. En este caso, dado que el morfismo $\widehat{\pi}$ es dominante, aplicamos el operador de Newton–Hensel de [Sch03] y calculamos polinomios $\widehat{m}(T,Y_{r+1})$, $\widehat{v}_{r+k}(T,Y_{r+1})$ $(2\le k\le n-r)$ que forman una solución geométrica de $\widehat{V}$ con un costo de $O\big((n\mathcal{T}+n^5)M(\delta)^2\big)$ operaciones en K.

Como $T=1$ también es un punto de levantamiento del morfismo $\widehat{\pi}$, la solución geométrica es compatible con $T=1$ lo que nos permite evaluarla en $T=1$ y, de esa manera, obtener polinomios $\widehat{m}(1,Y_{r+1})$, $\widehat{v}_{r+k}(1,Y_{r+1})$ $(2\le k\le n-r)$ que constituyen una solución geométrica de la fibra de levantamiento $\widehat{V}\cap\{T=1\}=\{1\}\times V_Q$, y por ende de V_Q, con Y_{r+1} como elemento primitivo. □

9.2. Un algoritmo para una solución geométrica de una fibra $\mathbb{F}_q$–definible

Finalmente, en esta sección mostramos cómo obtener una solución geométrica de la fibra de levantamiento V_Q con la forma lineal $Z_{r+1}\in\mathbb{F}_q[X_1,\dots,X_n]$ como elemento primitivo. En particular, el polinomio minimal de Z_{r+1} tendrá coeficientes en $\mathbb{F}_q$, lo que resultará fundamental al momento de calcular el punto q–racional de V.

Proposición 9.2.1. *Sea $q>8n^2d\delta^4$. Dado como dato de entrada*

- *un straight–line program en tiempo $\mathcal{T}$ que representa los polinomios de entrada $F_1,\dots,F_{n-r}$,*
- *los polinomios $m^{(n-r)}(P,Y_{r+1})$, $v_{r+k}^{(n-r)}(Y_{r+1})$ $(2\le k\le n-r)$, calculados en el Teorema 8.5.1, que constituyen una solución geométrica de la fibra de levantamiento V_P,*

pueden calcularse polinomios $m(Q,Z_{r+1})\in\mathbb{F}_q[Z_{r+1}]$, $v_{r+k}(Q,Z_{r+1})\in K[Z_{r+1}]$ $(2\le k\le n-r)$ que forman una solución geométrica de la fibra de levantamiento V_Q con $O\big((n\mathcal{T}+n^5)M(\delta)^2\big)$ operaciones en K. El algoritmo proporciona el resultado correcto con probabilidad de éxito al menos 1-1/16.

Demostración. Aplicando el Lema 9.1.3 calculamos polinomios $\widehat{m}(1,Y_{r+1})$,$\widehat{v}_{r+k}(1,Y_{r+1})$ $(2\le k\le n-r)$ que constituyen una solución geométrica de la fibra de levantamiento V_Q con Y_{r+1} como elemento primitivo con $O\big((n\mathcal{T}+n^5)M(\delta)^2\big)$ operaciones sobre K.

Sin embargo, necesitamos una solución geométrica de V_Q con Z_{r+1} como elemento primitivo. Tenemos entonces que calcular el minimal de Z_{r+1} –el cual tendrá coeficientes en $\mathbb{F}_q$– y las parametrizaciones de las variables $Y_{r+1},\dots,Y_n$ por los ceros de dicho minimal. La forma de proceder remeda lo que hemos hecho en los diferentes capítulos en los que se desarrolló el algoritmo.

Abordamos en primer lugar, el cálculo del minimal $m(Q,Z_{r+1})$ de Z_{r+1}. Para eso, definimos para cada $2\le k\le n-r$, el polinomio $\widehat{w}_{r+k}(1,Y_{r+1})\in K[Y_{r+1}]$:

$$\widehat{w}_{r+k}(1,Y_{r+1}) := (\partial\widehat{m}/\partial Y_{r+1})^{-1}(1,Y_{r+1})\cdot\widehat{v}_{r+k}(1,Y_{r+1}) \mod \widehat{m}(1,Y_{r+1}).$$

Con esta definición, la identidad $Y_{r+k}=\widehat{w}_{r+k}(1,Y_{r+1})$ es válida en $K[V_Q]$. Si escribimos $Z_{r+1}=\alpha_1Z_1+\cdots+\alpha_rZ_r+\alpha_{r+1}Y_{r+1}+\cdots+\alpha_nY_n$, de la identidad

$$\operatorname{Res}\left(\widehat{m}(1,Y_{r+1}),g\right)=\prod_{x\in V_Q} g(Y_{r+1}(x)),$$

deducimos que la ecuación minimal que verifica la forma lineal $Z_{r+1}+TY_{r+1}$ en $\overline{\mathbb{F}}_q[T]\otimes_{\mathbb{F}_q}\overline{\mathbb{F}}_q[V_Q]$ se puede expresar como

$$\begin{aligned} &m_{Z_{r+1}+TY_{r+1}}(Q,T,S)=\\ &\qquad=\operatorname{Res}_U\Big(\widehat{m}(1,U),S-\sum_{k=1}^{r}\alpha_kq_k-(\alpha_{r+1}+T)U-\sum_{k=r+2}^{n}\alpha_k\widehat{w}_k(1,U)\Big), \end{aligned} \tag{9.2}$$

donde, recordemos, $Q=(q_1,\dots,q_r)$. Siguiendo [ABRW96], como en la demostración de la Proposición 5.1.1, tenemos la siguiente congruencia:

$$\begin{aligned} m_{Z_{r+1}+TY_{r+1}}(Q,T,Z_{r+1}) &\equiv m(Q,Z_{r+1})+\\ &\quad+T\Big(\partial m/\partial Z_{r+1}(Q,Z_{r+1})Y_{r+1}-v_{r+1}(Q,Z_{r+1})\Big) \mod (T^2). \end{aligned}$$

Aquí $m(Q,Z_{r+1})$ representa el polinomio minimal de la función coordenada definida por Z_{r+1} en $K[V_Q]$ y la identidad $(\partial m/\partial Z_{r+1})(Q,Z_{r+1})Y_{r+1}=v_{r+1}(Q,Z_{r+1})$ es válida en $K[V_Q]$. Es decir, calculando el minimal de $Z_{r+1}+TY_{r+1}$ calculamos, al mismo tiempo, el polinomio minimal de Z_{r+1} y la parametrización de Y_{r+1} en términos de Z_{r+1}.

La resultante (9.2) se calcula por interpolación en la variable S, a orden T^2. De esta forma reducimos el problema al cálculo de δ resultantes de polinomios univariados de $K[T]$ de grado a lo sumo 1. Usando algoritmos rápidos para resultantes univariadas e interpolación sobre K (ver e.g., [BP94], [vzGG99]), concluimos que la representación densa de $m(Q,Z_{r+1})$ y $v_{r+1}(Q,Z_{r+1})$ puede calcularse en forma determinística con $O(\delta M(\delta))$ operaciones aritméticas sobre K.

Resta calcular los polinomios $v_{r+2}(Q,Z_{r+1}),\dots,v_n(Q,Z_{r+1})$ que parametrizan las variables $Y_{r+2},\dots,Y_n$ por los ceros de $m(Q,Z_{r+1})$. En primer lugar, vamos a calcular

polinomios $w_{r+2}(Q,Z_{r+1}),\ldots,w_n(Q,Z_{r+1})$ con coeficientes en K de grado acotado por $\delta-1$ tales que $Y_{r+k}=w_{r+k}(Q,Z_{r+1})$ en $K[V_Q]$ para $k=2,\ldots,n-r$. Luego, multiplicando por $(\partial m/\partial Z_{r+1})(Q,Z_{r+1})$ y reduciendo modularmente, obtenemos los polinomios $v_{r+2}(Q,Z_{r+1}),\ldots,v_n(Q,Z_{r+1})$.

El polinomio $w_{r+1}(Q,Z_{r+1})$ se calcula como el resto de $(\partial m/\partial Z_{r+1})^{-1}(Q,Z_{r+1})\cdot v_{r+1}(Q,Z_{r+1})$ módulo $m(Q,Z_{r+1})$. Recordemos que en $K[V_Q]$, tenemos las siguientes identidades:

$$Y_{r+1}=w_{r+1}(Z_{r+1}),\quad Y_{r+k}=\widehat{w}_{r+k}(1,Y_{r+1})(2\le k\le r).$$

De aquí, vemos que para $2\le k\le n-r$, cada polinomio $w_{r+k}(Q,Z_{r+1})$ coincide con el resto de $\widehat{w}_{r+k}\big(1,v_{r+1}(Z_{r+1})\big)$ módulo $m(Q,Z_{r+1})$. Los polinomios $w_{r+k}(Q,Z_{r+1})$ $(2\le k\le n-r)$ pueden entonces calcularse con $O(\delta M(\delta))$ operaciones aritméticas en K.

Para terminar la demostración, basta reunir los resultados parciales de complejidad y probabilidad de cada paso del algoritmo. □

En este punto es preciso detenerse, y hacer hincapié en algunos aspectos relevantes del algoritmo. En vistas de las condiciones que, necesariamente, deben imponerse de acuerdo al algoritmo que hemos desarrollado, podríamos haber determinado entonces que el mismo funciona correctamente si q es mayor que $60n^4d\Delta^4$. Ahora, esto hubiera acarreado el hecho de que la regularidad dependiera de Δ, el grado geométrico de V, y tendríamos dos consecuencias, digamos, no deseadas: por un lado Δ puede ser mucho más grande que δ, el grado de V; por otro, acaso una cuestión de índole filosófica: el cuerpo K es un cuerpo auxiliar (es decir, cualquier otro cuerpo cuyo cardinal verificara la condición requerida serviría), no desempeña ningún rol importante para encontrar un punto q–racional y, por lo tanto, no sería natural que la condición de regularidad dependiera de los grados de las variedades intermedias.

10 Cálculo de un punto q–racional de V

En este capítulo termina de configurarse el algoritmo probabilístico que calcula un punto q–racional de la variedad V.

Sea K la extensión finita de $\mathbb{F}_q$ introducida en la Sección 8.2 y consideremos las formas lineales $Z_1,\dots,Z_{r+1},Y_{r+2},\dots,Y_n$ encontradas en el capítulo anterior, las cuales conforman un conjunto linealmente independiente. La proyección lineal $\pi: V \to \mathbb{A}^r$ determinada por $Z_1,\dots,Z_r$ es un morfismo finito y $Q := (q_1,\dots,q_r) \in \mathbb{F}_q^r$ es un punto de levantamiento de π. Finalmente, supongamos que hemos calculado, Proposición 9.2.1 mediante, los polinomios $m(Q,Z_{r+1}) \in \mathbb{F}_q[Z_{r+1}]$, $v_{r+k}(Q,Z_{r+1}) \in K[Z_{r+1}]$ $(2 \le k \le n-r)$ que forman una solución geométrica de la fibra de levantamiento V_Q.

10.1. Una solución geométrica de una curva plana

Dado $\omega := (\omega_1,\dots,\omega_r) \in \mathbb{A}^r$ consideramos la variedad lineal $L_\omega \subset \mathbb{A}^n$ parametrizada por las ecuaciones $Z_1 = \omega_1 T + Q_1,\dots,Z_r = \omega_r T + Q_r$ y definimos la variedad $C_\omega := V \cap L_\omega$. Si bien C_ω es una curva contenida en V, no obstante, puede pensarse como una curva de $\mathbb{A}^{n-r+1}$ definida por los polinomios

$$F_1(\omega T + Q, Z_{r+1}, Y_{r+2},\dots,Y_n),\dots,F_{n-r}(\omega T + Q, Z_{r+1}, Y_{r+2},\dots,Y_n).$$

Bajo esta interpretación, consideramos $\pi_\omega : C_\omega \to \mathbb{A}^1$ la proyección inducida por T.

Lema 10.1.1. *La variedad C_ω es una variedad equidimensional de dimensión 1 y grado δ, el morfismo π_ω es finito y 0 es un punto no ramificado de π_ω.*

Demostración. La variedad lineal L_ω, como subvariedad de $\mathbb{A}^r$, tiene dimensión 1; como π es un morfismo finito y $C_\omega = \pi^{-1}(L_\omega)$ concluimos que $\dim C_\omega = \dim_{\mathbb{A}^r} L_\omega = 1$. Además, C_ω está definida por $n-r$ polinomios en $\mathbb{A}^{n-r+1}$, y por lo tanto no tiene componentes irreducibles de dimensión 0; es decir, C_ω es equidimensional de dimensión 1.

La finitud del morfismo π_ω proviene del hecho que $\overline{\mathbb{F}}_q[T] \hookrightarrow \overline{\mathbb{F}}_q[C_\omega]$ es una extensión entera de anillos; esto, a su vez, proviene del hecho que la extensión de anillos $\overline{\mathbb{F}}_q[Z_1,\dots,Z_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$ es entera pues π es un morfismo finito.

Observemos que $\pi_\omega^{-1}(0) = V_Q$. Por lo tanto, usando que Q es punto de levantamiento

de π y aplicando la Desigualdad de Bézout tenemos

$$\delta = \deg V_Q \leq \deg C_\omega \leq \deg V = \delta.$$

Por lo tanto, $\deg C_\omega = \delta$ y 0 es un punto no ramificado de π_ω. □

Denotemos por $m(\omega T + Q, Z_{r+1}) \in \mathbb{F}_q[T, Z_{r+1}]$ el polinomio minimal de (la función coordenada definida por) Z_{r+1} en la extensión entera $\overline{\mathbb{F}}_q[T] \hookrightarrow \overline{\mathbb{F}}_q[C_\omega]$. La notación elegida para el minimal de Z_{r+1} pone de manifiesto la dependencia del mismo de los puntos ω y Q; asumimos esta dependencia a lo largo del capítulo y escribimos $h(T, Z_{r+1}) := m(\omega T + Q, Z_{r+1})$.

Consideremos entonces el morfismo $\widetilde{\pi}_\omega : C_\omega \to \mathbb{A}^2$ definido por la proyección en T, Z_{r+1}. La clausura de la imagen de C_ω es una curva plana W_ω definida, justamente, por el polinomio $h(T, Z_{r+1})$.

De la Proposición 5.1.2 deducimos que $\widetilde{\pi}_\omega$ induce una equivalencia birracional $\widetilde{\pi}_\omega : C_\omega \to W_\omega$, definida sobre $W_\omega \setminus \widetilde{W}_\omega$ ($\widetilde{W}_\omega$ es la curva definida por $\partial h/\partial Z_{r+1}$), que puede expresarse en términos de los polinomios que constituyen una solución geométrica de la curva C_ω.

Trasladamos así, el problema de calcular un punto q–racional de C_ω al de calcular un punto q–racional de $W_\omega \setminus \widetilde{W}_\omega$. Usando la inversa birracional definida a partir de la solución geométrica, aunque no necesariamente $\mathbb{F}_q$–definible, obtenemos un punto q–racional de C_ω y por lo tanto uno de V. (El morfismo $\widetilde{\pi}_\omega$ es $\mathbb{F}_q$–definible y como Z_{r+1} es una forma lineal con coeficientes en $\mathbb{F}_q$, la preimagen de un punto q–racional de $W_\omega \setminus \widetilde{W}_\omega$ es un punto q–racional de C_ω.)

Estaríamos tentados a pensar que el problema se resuelve calculando una solución geométrica de la curva C_ω. No es suficiente pues, para que este procedimiento sea viable, necesitamos que la curva W_ω tenga al menos un punto q–racional; y no podemos asegurarlo si al menos no tiene una componente absolutamente irreducible definida sobre $\mathbb{F}_q$. Más aún, no queda claro siquiera que una curva absolutamente irreducible tenga un punto q–racional; sin embargo, bajo una condición de regularidad adecuada (la del Capítulo 9) vamos a poder garantizar que la curva W_ω tiene puntos q–racionales. En primer lugar, vamos a elegir $\omega \in \mathbb{A}^r$ de modo que la curva W_ω sea absolutamente irreducible. Sea entonces $C \in \overline{\mathbb{F}}_q[\Omega_1, \ldots, \Omega_r]$ el polinomio de grado acotado por $2\delta^4$ del Teorema 7.3.1. Este teorema asevera que para cada $\omega \in \mathbb{F}_q^r$ con $C(\omega) \neq 0$, la curva W_ω es absolutamente irreducible.

Como en el Capítulo 9 supongamos que $q > 8n^2 d\delta^4$. Podemos elegir aleatoriamente ω en $\mathbb{F}_q^r$ para el cual $C(\omega) \neq 0$ con probabilidad al menos $1 - 1/72$. Supongamos entonces que hemos elegido ω. Resumimos las consideraciones anteriores en el siguiente resultado.

Proposición 10.1.2. *Sea* $q > 8n^2 d\delta^4$. *A partir de*

- *un straight–line program que evalúa los polinomios* $F_1,\dots,F_{n-r}$ *en tiempo* $\mathcal{T}$,
- *la representación densa de polinomios de* $K[Z_{r+1}]$ *que forman una solución geométrica, provista por la Proposición 9.2.1, de una fibra de levantamiento* V_Q,

puede calcularse en forma determinística la representación densa de elementos $m(\omega T+Q,Z_{r+1})\in\mathbb{F}_q[T,Z_{r+1}]$, $v_{r+k}(\omega T+Q,Z_{r+1})\in K[T,Z_{r+1}]$ $(2\le k\le n-r)$, *que constituyen una solución geométrica de la curva absolutamente irreducible* C_ω, *con* $O\big((n\mathcal{T}+n^5)M(\Delta)^2\big)$ *operaciones en* K.

Demostración. Argumentando como en la demostración del Lema 8.3.1, los polinomios

$$F_1(\omega T+Q,Z_{r+1},Y_{r+2},\dots,Y_n),\dots,F_{n-r}(\omega T+Q,Z_{r+1},Y_{r+2},\dots,Y_n)$$

forman una sucesión regular y generan un ideal radical de $\mathbb{F}_q[T,Z_{r+1},Y_{r+2},\dots,Y_n]$. Aplicando el algoritmo de la Proposición 8.3.2 obtenemos, con la cantidad de operaciones indicada, polinomios $m(\omega T+Q,Z_{r+1})\in\mathbb{F}_q[T,Z_{r+1}]$, $v_{r+k}(\omega T+Q,Z_{r+1})\in K[T,Z_{r+1}]$ $(2\le k\le n-r)$, que conforman una solución geométrica de la curva C_ω. □

10.2. Calculando un punto racional de C_ω

En esta sección ponemos en marcha la discusión de la sección anterior mostrando un algoritmo probabilístico que calcula un punto q–racional de la curva C_ω. Para eso, supongamos que estamos en las condiciones de la sección anterior: elegimos $\omega\in\mathbb{F}_q^r$ tal que la curva plana W_ω definida por $h(T,Z_{r+1})\in\mathbb{F}_q[T,Z_{r+1}]$ es absolutamente irreducible de grado δ. Consideremos, además, la curva plana $\widetilde{W}_\omega$ definida por $\partial h/\partial Z_{r+1}$.

Recordemos que nuestra tarea consiste en hallar un punto en $(W_\omega\setminus\widetilde{W}_\omega)(\mathbb{F}_q)$. Las condiciones impuestas sobre $\mathbb{F}_q$ garantizan, por un lado, que el conjunto $(W_\omega\setminus\widetilde{W}_\omega)(\mathbb{F}_q)$ es no vacío, y, por el otro, que existe buena probabilidad de elegir un punto al azar en $(W_\omega\setminus\widetilde{W}_\omega)(\mathbb{F}_q)$.

Lema 10.2.1. *Si* $q>8n^2d\delta^4$, *entonces*

$$|(W_\omega\setminus\widetilde{W}_\omega)(\mathbb{F}_q)|\ge q-q^{1/2}\delta^2-\delta^2. \tag{10.1}$$

En particular, existe al menos un punto q*–racional de* $W_\omega\setminus\widetilde{W}_\omega$, *y por lo tanto de* V.

Demostración. De la estimación de Hasse–Weil (1.2) deducimos que la cantidad de puntos q–racionales de W_ω satisface la siguiente estimación:

$$\big||W_\omega(\mathbb{F}_q)|-q\big|\le\delta^2q^{1/2}.$$

En particular, deducimos la cota inferior $|W_\omega(\mathbb{F}_q)| \geq q - \delta^2 q^{1/2}$.

La variedad $W_\omega \cap \widetilde{W}_\omega$ tiene dimensión 0 y grado acotado por $\delta(\delta-1)$. De aquí, la siguiente cota superior para la cantidad de puntos q–racionales: $|(W_\omega \cap \widetilde{W}_\omega)(\mathbb{F}_q)| \leq \delta(\delta-1)$. Combinando la cota inferior anterior con esta cota superior obtenemos la cota inferior de (10.1).

Finalmente, la cota inferior de (10.1) es un número positivo pues $q > 8n^2 d\delta^4$. En suma, $W_\omega \setminus \widetilde{W}_\omega$ tiene un punto q–racional. □

Con la certeza de que $\big(W_\omega \setminus \widetilde{W}_\omega\big)(\mathbb{F}_q)$ es no vacío podemos abordar la tarea de hallar uno de sus elementos. En realidad, la tarea consiste en hallar un cero $(a,b) \in \mathbb{F}_q^2$ del polinomio $h(T, Z_{r+1})$ que no sea cero de $\partial h/\partial Z_{r+1}$. Para eso, trataremos de encontrar, en primer lugar, $a \in \mathbb{F}_q$ de modo que el polinomio univariado $h(a, Z_{r+1})$ tenga una raíz b en $\mathbb{F}_q$ y que lleve a que el punto (a,b) pertenezca a $\big(W_\omega \setminus \widetilde{W}_\omega\big)(\mathbb{F}_q)$ (verificamos si $h(a, Z_{r+1})$ es libre de cuadrados). La cuestión probabilística que atraviesa este procedimiento surge, entonces, de la necesidad de estimar la cantidad de elecciones de $a \in \mathbb{F}_q$ necesarias para que $h(a, Z_{r+1})$ tenga una raíz b en $\mathbb{F}_q$ tal que $(a,b) \in \big(W_\omega \setminus \widetilde{W}_\omega\big)(\mathbb{F}_q)$.

Para cada $a \in \mathbb{F}_q$, el polinomio $h(a, Z_{r+1})$ tiene a lo sumo δ raíces en $\overline{\mathbb{F}}_q$; en otras palabras, cada $a \in \mathbb{F}_q$ da lugar a lo sumo a δ puntos $(a,b) \in W_\omega \setminus \widetilde{W}_\omega$. Esta observación y (10.1) permiten la siguiente estimación:

$$|\{a \in \mathbb{F}_q : (W_\omega \setminus \widetilde{W}_\omega)(\mathbb{F}_q) \cap \{T = a\} \neq \emptyset\}| \geq \frac{q - q^{1/2}\delta^2 - \delta^2}{\delta}.$$

Deducimos la siguiente cota inferior para la probabilidad de elegir $a \in \mathbb{F}_q$ que origine un punto q–racional $(a,b) \in W_\omega \setminus \widetilde{W}_\omega$:

$$\text{Prob}\left(\{a \in \mathbb{F}_q : (W_\omega \setminus \widetilde{W}_\omega)(\mathbb{F}_q) \cap \{T = a\} \neq \emptyset\}\right) \geq \frac{q - q^{1/2}\delta^2 - \delta^2}{q\delta}. \tag{10.2}$$

Si $q > 8n^2 d\delta^4$, de la estimación sobre la probabilidad (10.2) concluimos que, después de a lo sumo δ elecciones al azar, encontraremos con probabilidad al menos $1 - 2q^{-1/2}\delta^2 \geq 1 - 1/6$ un elemento $a \in \mathbb{F}_q$ para el cual existe $(a,b) \in W_\omega \setminus \widetilde{W}_\omega(\mathbb{F}_q)$. Este paso se reduce a calcular el máximo común divisor entre $h(a, Z_{r+1})$ y $Z_{r+1}^q - Z_{r+1}$ hasta que este sea un elemento no constante de $\mathbb{F}_q[Z_{r+1}]$. Una vez hallado $a \in \mathbb{F}_q$, aplicando [vzGG99, Corollary 14.16], el cálculo de $b \in \mathbb{F}_q$ se reduce al de un número de máximo común divisores y a factorización en $\mathbb{F}_q[Z_{r+1}]$. El resultado siguiente resume el algoritmo recién descrito:

Proposición 10.2.2. *Sea $q > 8n^2 d\delta^4$. A partir de la solución geométrica de la curva C_ω, provista por la Proposición 10.1.2, es posible calcular un punto q–racional de la curva C_ω con $O\big(n\delta M(\delta)\log q\big)$ operaciones en K. El algoritmo devuelve el resultado correcto con probabilidad al menos $1 - 25/144$.*

Demostración. Dado $a \in \mathbb{F}_q$, definimos el siguiente polinomio de $\mathbb{F}_q[Z_{r+1}]$:

$$h_a^*(Z_{r+1}) := \gcd\left(h(a, Z_{r+1}), Z_{r+1}^q - Z_{r+1}\right).$$

Aplicando [vzGG99, Corollary 11.16]) podemos calcular h_a^* con $O\big(M(\delta)\log q\big)$ operaciones en $\mathbb{F}_q$. Además, decidir si $h(a, Z_{r+1})$ es un polinomio libre de cuadrados requiere $O\big(M(\delta)\big)$ operaciones en $\mathbb{F}_q$. De la estimación sobre la probabilidad (10.2) vemos que después de a lo sumo δ elecciones al azar, encontramos, con probabilidad al menos $1-1/6$, un elemento $a \in \mathbb{F}_q$ tal que $h(a, Z_{r+1})$ es libre de cuadrados y h_a^* es un polinomio no constante de $\mathbb{F}_q[Z_{r+1}]$. Por lo tanto, encontrar tal $a \in \mathbb{F}_q$ y calcular el polinomio h_a^* requiere a lo sumo $O\big(\delta M(\delta)\log q\big)$ operaciones en $\mathbb{F}_q$.

Como h_a^* se factoriza en factores lineales simples en $\mathbb{F}_q[Z_{r+1}]$, la factorización de h_a^* en $\mathbb{F}_q[Z_{r+1}]$ puede llevarse a cabo con $O(M(\delta)\log q)$ operaciones en $\mathbb{F}_q$ y se obtiene el resultado correcto con probabilidad por lo menos $1-1/144$ (ver eg., [vzGG99, Theorem 14.9]). Cualquier raíz $b \in \mathbb{F}_q$ de h_a^* proporciona un punto q–racional $(a, b) \in \mathbb{F}_q^2$ de $W_\omega \setminus \widetilde{W}_\omega$.

Especializamos las parametrizaciones de Y_{r+k} $(2 \le k \le n-r)$ por los ceros de $m(\omega T + Q, Z_{r+1})$ en $T = a$ y $Z_{r+1} = b$ y obtenemos un punto racional de C_ω (observemos que la elección de a asegura que las especializaciones están bien definidas). Esto completa la prueba de la proposición. □

10.3. El algoritmo final

Finalmente, estamos en condiciones de describir el algoritmo completo:

1. Comenzamos ejecutando el algoritmo delineado en el Teorema 8.5.1 para obtener una solución geométrica de la fibra de levantamiento V_P.

2. Obtenemos una solución geométrica de la fibra de levantamiento V_Q y de la curva absolutamente irreducible C_ω aplicando los algoritmos de las Proposiciones 9.2.1 y 10.1.2.

3. Aplicamos el algoritmo de la Proposición 10.2.2 para conseguir un punto q–racional de la curva $C_\omega \subset V$.

Resumimos las consideraciones anteriores en el siguiente resultado:

Teorema 10.3.1. *Sea $q > 8n^2 d\delta^4$. A partir de un straight–line program que evalúa los polinomios de entrada $F_1, \ldots, F_{n-r}$ en tiempo $\mathcal{T}$ puede calcularse un punto q–racional de la variedad V con $O\big((n\mathcal{T} + n^5)M(\Delta)M(d\Delta)\log q\, M(\log(q\Delta))\big)$ operaciones bit y con probabilidad de éxito al menos $2/3 > 1/2$.*

Nuestro algoritmo puede ser extendido al caso de una $\mathbb{F}_q$–variedad equidimensional V (definida por una sucesión regular reducida), en tanto tenga una componente absolutamente irreducible definida sobre $\mathbb{F}_q$. De hecho, el algoritmo del Teorema 8.5.1 puede ser aplicado en este caso, porque solo requiere que la variedad V sea equidimensional y esté definida por una sucesión regular reducida. Con un argumento similar al del Teorema 7.3.1 y de la Proposición 10.1.2, obtenemos una solución geométrica de una curva $C \subset V$ definida sobre $\mathbb{F}_q$, con al menos una componente absolutamente irreducible definida sobre $\mathbb{F}_q$. Luego, usando algoritmos rápidos para factorización bivariada y tests de irreducibilidad absoluta (ver e.g., [Kal95]), calculamos tal componente absolutamente irreducible; a esta componente le aplicamos el algoritmo de la Proposición 10.2.2. Si $q > 8n^2d\delta^4$, nuestra estimación asintótica de complejidad y las estimaciones de probabilidad son las mismas que las del Corolario 10.3.1.

11 Una aplicación a la criptografía

Este capítulo constituye una aplicación, al ámbito criptográfico, de las herramientas algorítmicas desarrolladas a lo largo de esta tesis. Estudiamos el problema de invertir un morfismo polinomial biyectivo $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$. El interés por este tipo de problemas se origina en los casos en que dicho morfismo F codifica alguna permutación de un esquema criptográfico.

11.1. El contexto

Sean $F_1, \ldots, F_n$ polinomios en $\mathbb{F}_q[X] := \mathbb{F}_q[X_1, \ldots, X_n]$. Consideremos la aplicación polinomial $F : \mathbb{A}^n \to \mathbb{A}^n$ definida por $F_1, \ldots, F_n$, es decir $F(x) = (F_1(x), \ldots, F_n(x))$. Decimos que F es un automorfismo si existe una aplicación polinomial $G = (G_1, \ldots, G_n) : \mathbb{A}^n \to \mathbb{A}^n$ tal que $X_i = G_i(F_1, \ldots, F_n)$ para todo $1 \leq i \leq n$. Decidir si un conjunto de n polinomios define un automorfismo es un problema duradero y forma parte de lo que se conoce como la Conjetura del Jacobiano: F define un automorfismo si y solo si el determinante de la matriz jacobiana $(\partial F_i / \partial X_j)_{1 \leq i,j \leq n}$ es una unidad.

Desde el trabajo [IM88] se han construido esquemas de clave pública cuya seguridad se sostiene en la dificultad de resolver sistemas de ecuaciones polinomiales sobre cuerpos finitos; pero, en general, los esquemas que se proponen son vulnerados a través de «ataques» *ad hoc* (ver e.g., [WP05], [KS99]). Esta situación podría proporcionar indicios sobre el hecho de que invertir los morfismos polinomiales utilizados en criptografía de clave pública –típicamente definidos por polinomios cuadráticos– no constituye un problema difícil, y pone de manifiesto la necesidad de caracterizar parámetros que midan tal dificultad.

Carl Sturtivant y Zhi–Li Zhang [SZ90] presentan un algoritmo para invertir una aplicación polinomial del tipo descrito, asumiendo que F es un automorfismo de $\mathbb{F}_q[X]^n$ cuya inversa tiene grado $(dn)^{O(1)}$, con d el máximo de los grados de los polinomios $F_1, \ldots, F_n$. El algoritmo tiene una complejidad de $(\mathcal{T} n d)^{O(1)}$ operaciones aritméticas en $\mathbb{F}_q$, donde $\mathcal{T}$ es el número de operaciones aritméticas necesarias para evaluar F.

Desde el punto de vista de la criptografía, el problema crítico es el de calcular la imagen inversa de un punto $y^{(0)} \in \mathbb{F}_q^n$ bajo una aplicación F, más que el de invertir el morfismo F. En este sentido, resolvemos aquel bajo hipótesis más relajadas que las de [SZ90]. Más precisamente, mostramos un algoritmo probabilístico que, dado un punto

$y^{(0)} \in \mathbb{F}_q^n$ y un straight–line program que evalúa F en $\mathbb{F}_q[X_1,\ldots,X_n]$, calcula el punto $x^{(0)} \in \mathbb{F}_q^n$ para el cual $F(x^{(0)}) = y^{(0)}$.

La complejidad del algoritmo es *grosso modo* $O((\mathcal{T}n^4+\delta^2)n\delta^2)$, donde L es la complejidad de la evaluación de F y δ es el grado del gráfico de F. Creemos que el grado δ podría desempeñar un papel importante para medir la dificultad de invertir F; debería ser tenido en cuenta como un parámetro que estime la seguridad de los esquemas criptográficos subyacentes.

11.2. Preparación de los datos de entrada

Dados polinomios $F_1,\ldots,F_n \in \mathbb{F}_q[X_1,\ldots,X_n]$ de grado acotado por d, consideremos la aplicación polinomial $F\colon \mathbb{A}^n \to \mathbb{A}^n$ definida por $F(x) := (F_1(x),\ldots,F_n(x))$. En particular, la restricción de F, de $\mathbb{F}_q^n$ en $\mathbb{F}_q^n$, está bien definida y será denotada también por F.

Sea $V \subset \mathbb{A}^{2n}$ la $\mathbb{F}_q$–variedad dada por el gráfico del morfismo F:

$$V := \{(x,y) \in \mathbb{A}^{2n} :\ y_i = F_i(x), 1 \le i \le n\}.$$

Vamos a suponer que F satisface las siguientes condiciones (usuales en las situaciones criptográficas en que estamos interesados).

(i) $F\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ es biyectivo.

(ii) La proyección $\pi\colon V \to \mathbb{A}^n$ definida por $\pi(x,y) := y$ es un morfismo finito. En particular, para cada $y \in \mathbb{A}^n$ la fibra $V_y := \pi^{-1}(y)$ es una subvariedad de V de dimensión 0.

Bajo las condiciones anteriores, la variedad V (dado que es un gráfico) es una $\mathbb{F}_q$–variedad absolutamente irreducible de dimensión n y F es un morfismo dominante. En consecuencia, las indeterminadas $Y_1,\ldots,Y_n$ son algebraicamente independientes en $\overline{\mathbb{F}}_q[V]$. Sea δ el grado de V y D el grado del morfismo π.

Supongamos que disponemos de una solución geométrica de la $\mathbb{F}_q$–variedad V. En particular, disponemos de una forma lineal $\mathcal{L} \in \overline{\mathbb{F}}_q[Y_1,\ldots,Y_n]$ cuyo minimal $m_{\mathcal{L}}$ (un elemento de $\overline{\mathbb{F}}_q[Y_1,\ldots,Y_n,T]$) verifica $\deg_T m_{\mathcal{L}} = D$. Entonces V es birracionalmente equivalente a la hipersuperficie H definida por $m_{\mathcal{L}} \in \overline{\mathbb{F}}_q[Y_1,\ldots,Y_n,T]$. Como V es absolutamente irreducible, H y por lo tanto $m_{\mathcal{L}}$ lo son.

Dado $y^{(0)} \in \mathbb{F}_q^n$ denotamos por $V_{y^{(0)}}$ la fibra correspondiente. Para calcular la preimagen $x^{(0)} \in \mathbb{F}_q^n$ de $y^{(0)}$, o lo que es lo mismo, el punto $(x^{(0)},y^{(0)}) \in V_{y^{(0)}}$, vamos a deformar el sistema $F(X) = y^{(0)}$ en otro sistema $F(X) = F(x^{(1)})$, con $x^{(1)}$ un punto elegido en forma aleatoria en una extensión finita K de $\mathbb{F}_q$, extensión que será determinada oportunamente, como hicimos durante el desarrollo del algoritmo. Debemos señalar que esta deformación está influenciada por el trabajo [PS04].

En primer lugar, debemos entonces establecer cotas apropiadas sobre el grado de las condiciones genéricas que subyacen a la elección de $x^{(1)}$.

Lema 11.2.1. *Existe un polinomio* $A \in \overline{\mathbb{F}}_q[X_1,\ldots,X_n]$ *de grado a lo sumo* $3d\delta^4$ *tal que para cada* $x \in \mathbb{A}^n$ *con* $A(x) \neq 0$*, el punto* $y := F(x)$ *satisface las siguientes condiciones:*

(i) y *es un punto de levantamiento de* $\pi : V \to \mathbb{A}^n$*,*

(ii) *La curva* $\mathcal{C} \subset \mathbb{A}^{n+1}$ *definida por* $F(X) = y + (S-1)(y - y^{(0)})$ *es absolutamente irreducible.*

Demostración. Sea $\mathcal{L} \in \overline{\mathbb{F}}_q[X]$ una forma lineal que induce un elemento primitivo de la extensión de anillos $\overline{\mathbb{F}}_q[Y_1,\ldots,Y_n] \hookrightarrow \overline{\mathbb{F}}_q[V]$ y sea $m_{\mathcal{L}} \in \overline{\mathbb{F}}_q[Y_1,\ldots,Y_n][T]$ su polinomio minimal.

Si $\tilde{A}_1 \in \overline{\mathbb{F}}_q[Y_1,\ldots,Y_n]$ denota el discriminante de $m_{\mathcal{L}}$ con respecto a T, de la irreducibilidad absoluta de $m_{\mathcal{L}}$ concluimos que $\tilde{A}_1 \neq 0$. En realidad, podemos expresarlo como un polinomio en las indeterminadas $X_1,\ldots,X_n$ definiendo $A_1 := \tilde{A}_1(F(X_1,\ldots,X_n))$. De este modo, A_1 pertenece a $\overline{\mathbb{F}}_q[X_1,\ldots,X_n]$ y tiene grado acotado por $(2D-1)d\delta$; además, como el morfismo F es dominante, existe $x \in \mathbb{A}^n$ tal que $A_1(x) \neq 0$. En otras palabras, A_1 es un polinomio no nulo.

Definimos $\widetilde{m}_{\mathcal{L}}(X,S,T) := m_{\mathcal{L}}(F(X) + (S-1)(F(X) - y^{(0)}),T) \in \overline{\mathbb{F}}_q[X,S,T]$. Notemos que $\widetilde{m}_{\mathcal{L}}$ es un elemento mónico de $\overline{\mathbb{F}}_q[X,S][T]$ ya que $m_{\mathcal{L}} \in \overline{\mathbb{F}}_q[Y][T]$. Si y es un punto de levantamiento de π y x es cualquier punto de la fibra V_y, tenemos que $\widetilde{m}_{\mathcal{L}}(x,1,T) = m_{\mathcal{L}}(y,T)$ es un polinomio separable de $\overline{\mathbb{F}}_q[X][T]$.

Aplicando entonces el Teorema 7.3.1, existe un polinomio $A_2 \in \overline{\mathbb{F}}_q[X]$ de grado acotado por $2d\delta^4$ tal que para cada $x \in \overline{\mathbb{F}}_q^n$ con $A_2(x) \neq 0$ el polinomio $\widetilde{m}_{\mathcal{L}}(x,S,T)$ es absolutamente irreducible.

Definimos el polinomio del enunciado del lema como $A := A_1A_2$. Observemos que $A \in \overline{\mathbb{F}}_q[X]$ y que A tiene grado a lo sumo $3d\delta^4$. Ahora, si $x \in \mathbb{A}^n$ es tal que $A(x) \neq 0$ y si definimos $y := F(x)$, se verifican las condiciones (i) y (ii) del enunciado del lema. En efecto, de $A_1(x) \neq 0$ se sigue que $\tilde{A}_1(y) \neq 0$; es decir, el discriminante de $m_{\mathcal{L}}(y,T)$ con respecto a T es distinto de cero. Deducimos que $m_{\mathcal{L}}(y,T)$ tiene D raíces distintas y por lo tanto, y es un punto de levantamiento de π. Para terminar, dado que y es un punto de levantamiento de π y que $A_2(x) \neq 0$, el polinomio $\widetilde{m}_{\mathcal{L}}(x,S,T)$ es absolutamente irreducible y la curva $\mathcal{C}$ también. □

Supongamos que ya hemos elegido $x \in \mathbb{A}^n$ que verifica las condiciones del Lemma 11.2.1 y sea $y := F(x)$. Sean $\Lambda := (\Lambda_1,\ldots,\Lambda_n)$ nuevas indeterminadas.

Lema 11.2.2. *Existe un polinomio no nulo* $B \in \overline{\mathbb{F}}_q[\Lambda]$ *de grado a lo sumo* $2D^2$ *tal que para cada* $\lambda \in \mathbb{A}^n$ *con* $B(\lambda) \neq 0$*, la forma lineal* $\mathcal{L} = \lambda_1X_1 + \cdots + \lambda_nX_n$ *separa los puntos de las fibras* V_y *y* $V_{y^{(0)}}$*.*

Demostración. Sea $V_y \cup V_{y^{(0)}} := \{P_1, \ldots, P_{D'}\}$. Consideramos la forma lineal genérica $\mathcal{L}_\Lambda := \Lambda_1 X_1 + \cdots + \Lambda_n X_n$ y definimos el polinomio $B(\Lambda) := \Pi_{1 \le i < j \le D'}(\mathcal{L}_\Lambda(P_i) - \mathcal{L}_\Lambda(P_j))$. Como $D' \le 2D$, $B \in \overline{\mathbb{F}}_q[\Lambda]$ es un polinomio no nulo de grado a lo sumo $2D^2$. Cualquier $\lambda \in \mathbb{A}^n$ que no anule a B proporciona una forma lineal $\mathcal{L}$ que separa los puntos de V_y y de $V_{y^{(0)}}$. □

La cuestión radica en determinar una extensión finita K de $\mathbb{F}_q$ de modo de poder garantizar la existencia de $\lambda, x \in K^n$ que satisfagan los Lemas 11.2.1 y 11.2.2. El próximo resultado establece que podemos realizar esta elección en forma aleatoria en cualquier extensión de $\mathbb{F}_q$ de grado adecuado.

Corolario 11.2.3. *Con las mismas notaciones que en los Lemas 11.2.1 y 11.2.2, fijamos $\mu > 0$ y elegimos una extensión finita K de $\mathbb{F}_q$ tal que $|K| > 4\mu d\delta^4$. La probabilidad de elegir $(\lambda, x) \in K^{2n}$ que no anule al polinomio AB es al menos $1 - 1/\mu$.*

Demostración. La probabilidad de elegir aleatoriamente $x \in K^n$ que no anula al polinomio A es al menos $1 - 3d\delta^4/|K| \ge 1 - 3/4\mu$. Habiendo realizado esta elección, podemos elegir un elemento $\lambda \in K^n$ no anula a B con probabilidad al menos $1 - 2D^2/|K| \ge 1 - 1/4\mu$. Por lo tanto, la probabilidad de elegir al azar $(\lambda, x) \in K^{2n}$ tal que $(AB)(\lambda, x) \ne 0$ es al menos $(1 - 3/4\mu)(1 - 1/4\mu) \ge 1 - 1/\mu$. □

11.3. El algoritmo

Sea K un cuerpo de cardinal $O(d\delta^4)$ que extiende a $\mathbb{F}_q$. Corolario 11.2.3 mediante, asumimos haber elegido $(\lambda, x^{(1)}) \in K^{2n}$ que verifica las condiciones de los Lemas 11.2.1 y 11.2.2. Por lo tanto, $y^{(1)} := F(x^{(1)})$ es un punto de levantamiento de $\pi : V \to \mathbb{A}^n$, la curva $\mathcal{C} \subset \mathbb{A}^{n+1}$ definida por

$$F(X) = y^{(1)} + (S - 1)(y^{(1)} - y^{(0)}) \tag{11.1}$$

es absolutamente irreducible, y la forma lineal $\mathcal{L} := \lambda_1 X_1 + \cdots + \lambda_n X_n \in K[X]$ separa los puntos de las fibras $V_{y^{(1)}}$ y $V_{y^{(0)}}$. Consideremos la proyección $\pi_S : \mathcal{C} \to \mathbb{A}^1$ definida por $\pi_S(s, x) := s$. Observemos que π_S es un morfismo finito de grado D, que $S = 1$ es un punto de levantamiento de π_S y que $\pi_S^{-1}(1) = \{1\} \times \mathcal{C}_1$ y $\pi_S^{-1}(0) = \{0\} \times \mathcal{C}_0$, donde $\mathcal{C}_1 = F^{-1}(y^{(1)})$ y $\mathcal{C}_0 = F^{-1}(y^{(0)})$. Además, como $\mathcal{L}$ separa los puntos de $V_{y^{(1)}}$ se sigue que $\mathcal{L}$ es un elemento primitivo de $K[S] \hookrightarrow K[\mathcal{C}]$.

El algoritmo que finalmente calcula el punto $x^{(0)}$ consta de tres etapas principales. En primer lugar, calculamos el polinomio minimal $m_S(S, T)$ de $\mathcal{L}$ en la extensión de anillos $K[S] \hookrightarrow K[\mathcal{C}]$. Luego calculamos una solución geométrica de la curva $\mathcal{C}$. Por último, calculamos efectivamente el punto $x^{(0)}$.

11.3.1. Cálculo de un polinomio minimal

Consideremos la factorización de $m_S(S,T)$ en el anillo de series de potencias $K[\![S-1]\!][T]$. Como $m_S(1,T)$ es separable y de grado D existen D series de potencias distintas $\sigma^{(1)},\dots,\sigma^{(D)} \in K[\![S-1]\!]$ tales que el polinomio $m_S(S,T)$ se factoriza como $m_S = \prod_{i=1}^{D}(T-\sigma^{(i)})$. Más aún, $m_S(1,T)$ puede factorizarse en la forma $m_S(1,T) = \prod_{i=1}^{D}(T-\sigma^{(i)}(1))$, donde $\sigma^{(i)}(1)$ representa el término constante de $\sigma^{(i)}$ para $1 \le i \le D$. Como $m_S(1,T)$ es el polinomio minimal de la forma lineal $\mathcal{L}$ en $K[V_{y^{(1)}}]$ entonces, si $V_{y^{(1)}} = \{P_1,\dots,P_D\}$, tenemos que $m_S(1,T) = \prod_{i=1}^{D}(T-\mathcal{L}(P_i))$. Dado que $x^{(1)}$ pertenece a la fibra $V_{y^{(1)}}$ existe una serie $\sigma^{(i)}$ para el cual $\mathcal{L}(x^{(1)}) = \sigma^{(i)}(1)$. En aras de simplificar la notación, escribimos σ en lugar de $\sigma^{(i)}$.

En primer lugar, calculamos la serie de potencias σ truncada a orden $N := 2D\delta$; es decir, calculamos el polinomio $\sigma_N \in \overline{\mathbb{F}}_q[S]$, de grado a lo sumo N, congruente a σ módulo $(S-1)^{N+1}$. La idea es recuperar $m_S(S,T)$ a partir de una ecuación que anule a σ_N.

Lema 11.3.1. *Sea* $g \in K[S,T]$ *con* $\deg_S g \le \delta$ *y* $\deg_T g \le D$ *que, además, satisface la siguiente congruencia*

$$g(S,\sigma_N) \equiv 0 \bmod (S-1)^{N+1}. \tag{11.2}$$

Entonces m_S *divide a* g *en* $K[S,T]$.

Demostración. Sea $g \in K[S,T]$ una solución de (11.2) con las condiciones de grado señaladas. La resultante $h \in K[S]$ de g y m_S respecto de T tiene grado a lo sumo N y pertenece al ideal generado por m_S y g. Dado que $m_S(S,\sigma_N)$ y $g(S,\sigma_N)$ son congruentes a 0 módulo $(S-1)^{N+1}$, tenemos que $h(S) \equiv 0$ módulo $(S-1)^{N+1}$ y, por lo tanto, que $h = 0$. Derivamos la existencia de un factor común a m_S y g en $K(S)[T]$. Teniendo en cuenta la irreducibilidad de m_S en $K(S)[T]$ y el lema de Gauss, concluimos la demostración. □

El Lema 11.3.1 evidencia la caracterización de m_S como una solución no nula de (11.2): la solución de grado mínimo. Observemos entonces que nos encontramos en la misma situación que la de la Sección 4.1.1. El sistema (11.2) representa un sistema de ecuaciones lineales cuyas incógnitas son los coeficientes del polinomio g, y las ecuaciones de este sistema se obtienen calculando las potencias $\sigma_N,\dots,\sigma_N^D$ truncadas a orden $N+1$.

Procederemos como en el algoritmo de la sección 4.1.1 aunque, en este caso, trabajamos solamente con la raíz $x^{(1)}$. Comenzamos calculando σ_N, aplicando el operador de Newton, tal como fue aplicado en esa sección, sobre el anillo de series de potencias $K[\![S-1]\!]$. Evaluando (11.1) en $S=1$, obtenemos el sistema $y^{(1)} = F(X)$. Como $y^{(1)}$ es un punto de levantamiento de π, del Lema 2.1.9 se desprende que ninguna de las soluciones de $y^{(1)} = F(X)$ anulan el determinante de la matriz Jacobiana $J_F := (\partial F_i)/(\partial X_j)_{1\le i,j\le n}$. En particular, $\det J_F(x^{(1)}) \neq 0$. Por lo tanto, estamos en condiciones de llevar adelante la iteración de Newton. La diferencia, es que en aquella instancia, tratamos con un único

polinomio bivariado, mientras que en este caso lo aplicaremos a un sistema de ecuaciones polinomiales –en este sentido, se asemeja a la forma en que fue utilizado durante el desarrollo del algoritmo, con la salvedad de que en este caso, la iteración de Newton es local– dado por el sistema de ecuaciones

$$G(S,X) := F(X) - y^{(1)} - (S-1)(y^{(1)} - y^{(0)}).$$

Sea N_G el operador de Newton–Hensel $N_G(X) := X - J_F^{-1}(X)G(S,X)$ y denotemos por $N_G^{(k)}$ la k–ésima iteración de N_G. Si definimos $\Psi_k := N_G^{(k)}(x^{(1)}) \in K[\![S-1]\!]^n$ entonces

$$G(S,\Psi_k) \equiv 0 \bmod (S-1)^{2^k}. \tag{11.3}$$

El polinomio $m_S(S,\mathcal{L}(X))$ pertenece al ideal de $K[S,X]$ generado por G pues se anula sobre la curva $\mathcal{C}$, con lo cual (11.3) implica que $m_S(S,\mathcal{L}(\Psi_k)) \equiv 0$ módulo $(S-1)^{2^k}$. De la identidad $\mathcal{L}(\Psi_k)(1) = \mathcal{L}(x^{(1)})$ deducimos también que $\mathcal{L}(\Psi_k) \equiv \sigma \bmod (S-1)^{2^k}$. De este modo, aplicando $\kappa := \lceil \log_2(N+1) \rceil$ iteraciones del operador de Newton obtenemos σ_N truncando a orden $N+1$ la serie de potencias $\mathcal{L}(\Psi_\kappa)$. Luego, calculamos las potencias $\sigma_N^2, \ldots, \sigma_N^D$ multiplicando y truncando.

La multiplicación de dos matrices de tamaño $n \times n$ con coeficientes en K requiere $O(n^\omega)$ operaciones en K, donde $\omega < 2{,}376$ (teóricamente), pero en la práctica usualmente se considera $\omega = \log_2 7 \sim 2{,}81$ (cf. [BP94]). La siguiente proposición proporciona la estimación de complejidad del procedimiento descrito anteriormente:

Proposición 11.3.2. *Si los polinomios $F_1, \ldots, F_n$ se evalúan con $\mathcal{T}$ operaciones sobre K, entonces las potencias $\sigma_N, \ldots, \sigma_N^D$, truncadas a orden $N+1$, pueden calcularse con $O\big((\mathcal{T} + n^{1+\omega})M(D\delta)\big)$ operaciones en K.*

Demostración. En primer lugar, apelando al teorema de Baur–Strassen [BS83], dado que los polinomios $F_1, \ldots, F_n$ se evalúan con $\mathcal{T}$ operaciones en K, evaluamos las entradas de J_F con $O(\mathcal{T})$ operaciones aritméticas. Luego, el determinante y la matriz adjunta de J_F con $O(\mathcal{T} + n^{1+\omega})$ operaciones aritméticas [BP94].

Para calcular Ψ_{k+1} a partir de Ψ_k, calculamos la matriz inversa $J_F^{-1}(\Psi_k)$ como el producto $J_F^{-1}(\Psi_k) = \det J_F(\Psi_k)^{-1} \cdot \mathrm{Adj}\big(J_F(\Psi_k)\big)$

Utilizando inversión rápida de series de potencias podemos calcular $\det J_F(\Psi_k)^{-1}$ con $O\big((\mathcal{T} + n^{1+\omega})M(2^k)\big)$ operaciones aritméticas ([vzGG99], [BP94]). Con un costo similar, la adjunta $\mathrm{Adj}\big(J_F(\Psi_k)\big)$ y el producto $\det J_F(\Psi_k)^{-1} \cdot \mathrm{Adj}\big(J_F(\Psi_k)\big)$.

Por lo tanto, el cálculo de Ψ_k para $2 \le k \le \kappa$ requiere $O\big((\mathcal{T} + n^{1+\omega}) \sum_{k=0}^{\kappa-1} M(2^k)\big) = O\big((\mathcal{T} + n^{1+\omega})M(D\delta)\big)$ operaciones aritméticas.

Los pasos restantes no cambian la complejidad total. □

Discutimos ahora como resolver el sistema de ecuaciones que surge en (11.2). Se trata de un sistema lineal con $N+1$ ecuaciones y $D\delta$ incógnitas representadas por los coefi-

cientes de la solución $g \in K[S,T]$ de (11.2). Un sistema arbitrario de $O(D\delta \times D\delta)$ puede resolverse con $O((D\delta)^\omega)$ operaciones aritméticas ([BP94] presenta algoritmos rápidos para esta tarea); no obstante, en este caso, vamos a sacar provecho (en vistas de mejorar la estimación de la complejidad) del hecho siguiente: ordenando las incógnitas en forma adecuada, la matriz M del sistema (11.2) es una matriz Toeplitz en bloques.

Lema 11.3.3. *La matriz M del sistema (11.2) puede expresarse como una matriz Toeplitz en bloques con D bloques.*

Demostración. Para empezar, escribimos el polinomio

$$g(S,T) := \sum_{j=0}^{\delta} \sum_{k=0}^{D} A_{j,k}(S-1)^j T^k$$

cuyos coeficientes indeterminados $A_{j,k}$ representan las incógnitas del sistema. Además, las potencias de σ_N pueden expresarse como

$$\sigma_N^k \equiv \sum_{h=0}^{N} \alpha_{h,k}(S-1)^h \bmod (S-1)^{N+1} \quad (1 \le k \le D).$$

Por lo tanto, fijando i con $0 \le i \le N$, la i–ésima ecuación de (11.2) es una ecuación homogénea

$$\sum_{j=0}^{\delta} \sum_{k=0}^{D} \alpha_{i-j,k} A_{j,k} = 0, \tag{11.4}$$

(con $\alpha_{i-j,k} = 0$ para $i-j < 0$) que expresa que el coeficiente de $(S-1)^i$ en $g(S,\sigma_N)$ es cero.

Fijemos k_0 y llamemos $M^{(k_0)}$ a la submatriz de M de tamaño $(N+1) \times \delta$ formada por las columnas de M correspondientes a las incógnitas A_{j,k_0} para $0 \le j \le \delta$. Como consecuencia de (11.4) la matriz $M^{(k_0)}$ resulta ser una matriz Toeplitz y, ordenando las incógnitas $A_{j,k}$ según el orden lexicográfico inverso aplicado al conjunto de pares (k,j), concluimos que M es una matriz Toeplitz en bloques, con D bloques. □

El Lema 11.3.3 nos permite resolver (11.2) usando la teoría de matrices de rango de desplazamiento fijo (cf. [BP94], [Pan01]). De [Pan01, Chapter 5] se sigue que una base del espacio nulo de una matriz Toeplitz en bloques de tamaño $2D\delta \times D\delta$ con D bloques puede calcularse en forma probabilística con $O\big(D^2 M(D\delta)\big)$ operaciones en K. De esa base obtenemos m_S dentro de la misma estimación de complejidad. Para concluir, la siguiente proposición resume el costo de calcular el polinomio minimal m_S:

Proposición 11.3.4. *El polinomio $m_S \in K[S,T]$ puede calcularse con $O\big((\mathcal{T} + n^{1+\omega} + D^2)M(D\delta)\big)$ operaciones en K con probabilidad de éxito $1 - 1/\mu$.*

11.3.2. Una solución geométrica de una sección plana

La tarea en ciernes consiste en extender el algoritmo de la sección previa a un algoritmo que calcula una solución geométrica de la curva $\mathcal{C}$ definida en (11.1). Sea $\Lambda := (\Lambda_1, \ldots, \Lambda_n)$ un vector de nuevas indeterminadas y consideremos la proyección $\pi_\Lambda : \mathbb{A}^n \times \mathcal{C} \to \mathbb{A}^n \times \mathbb{A}^1$ definida como $\pi_\Lambda(\lambda, s, x) := (\lambda, s)$. Como π_S es un morfismo finito, el morfismo π_Λ es finito y, por lo tanto, la extensión de anillos $K[\Lambda, S] \hookrightarrow K[\Lambda] \otimes_K K[\mathcal{C}]$ es entera. El polinomio minimal $m_\Lambda \in K[\Lambda, S, T]$ de la forma lineal $\mathcal{L}_\Lambda := \Lambda_1 X_1 + \cdots + \Lambda_n X_n$ en $K[\Lambda, S] \hookrightarrow K[\mathbb{A}^n] \otimes_K K[\mathcal{C}]$ es un elemento separable de $K[\Lambda, S][T]$, tal que $\partial m_\Lambda / \partial T$ no es divisor de cero de $K[\mathbb{A}^n] \otimes_K K[\mathcal{C}]$, que satisface las cotas de grado $\deg_T m_\Lambda \leq D$, $\deg_S m_\Lambda \leq \delta$ y $\deg_\Lambda m_\Lambda \leq \delta$. Recordemos que si reemplazamos Λ en λ tenemos que $m_\Lambda(\lambda, S, T) = m_S(S, T)$ y, posteriormente, las n parametrizaciones requeridas:

$$\frac{\partial m_S}{\partial T}(S, T) X_k - \nu_k(S, T) = 0 \quad (1 \leq k \leq n), \tag{11.5}$$

donde $\nu_k := \frac{\partial m_\Lambda}{\partial \Lambda_k}(\lambda, S, T)$. Conociendo el polinomio minimal m_s, resta calcular las parametrizaciones $\nu_1, \ldots, \nu_n$. Para ese fin, consideramos el desarrollo de Taylor de orden uno de $m_\Lambda(\Lambda, S, T)$ en potencias de $\Lambda - \lambda := (\Lambda_1 - \lambda_1, \ldots, \Lambda_n - \lambda_n)$:

$$m_\Lambda = m_S + \sum_{k=1}^{n} \frac{\partial m_\Lambda(\lambda, S, T)}{\partial \Lambda_k} (\Lambda_k - \lambda_k) \bmod (\Lambda - \lambda)^2.$$

Calcularemos este desarrollo de Taylor aplicando el algoritmo que subyace a la Proposición 11.3.4 a la forma lineal genérica $\mathcal{L}_\Lambda$. Cada operación aritmética en este algoritmo es una operación aritmética entre dos polinomios de $K[\Lambda]$, truncados a orden $(\Lambda - \lambda)^2$. Dado que sumar o multiplicar dos polinomios de $K[\Lambda]$ truncados a orden $(\Lambda - \lambda)^2$ requiere $O(n)$ operaciones aritméticas en K obtenemos:

Proposición 11.3.5. *Una solución geométrica de $\mathcal{C}$ puede calcularse con $O\big((\mathcal{T} + n^{1+\omega} + D^2) n M(D\delta)\big)$ operaciones en K.*

11.3.3. Cálculo de un punto racional

En esta sección mostramos finalmente como hallar la única solución en $\mathbb{F}_q^n$ del sistema $F(X) = y^{(0)}$.

Consideremos una solución geométrica K–definible de la curva $\mathcal{C}$ definida en (11.1). Esta solución geométrica viene dada por una forma lineal $\mathcal{L} \in K[X]$, el polinomio minimal $m_S \in K[S, T]$ de $\mathcal{L}$ en la extensión de anillos $K[S] \hookrightarrow K[\mathcal{C}]$ y las parametrizaciones $(\partial m_S / \partial T) X_k - \nu_k(S, T)$ de las variables $X_1, \ldots, X_n$ por los ceros de m_S, para $k = 1, \ldots, n$.

Sea $\pi_S^{-1}(0) =: \{0\} \times \mathcal{C}_0$ donde $\mathcal{C}_0 = F^{-1}(y^{(0)})$. Nuestras hipótesis sobre F implican que $x^{(0)}$ es el único punto q–racional de $\mathcal{C}_0$. Como $\mathcal{L}$ separa los puntos de $\pi_S^{-1}(0)$, de una solu-

ción geométrica de $\mathcal{C}$ podemos obtener una solución geométrica de $\mathcal{C}_0$. De hecho, reemplazando S por 0 en $m_S, v_1, \ldots, v_n$ obtenemos polinomios $m_S(0,T), v_1(0,T), \ldots, v_n(0,T) \in K[T]$ que representan una descripción de la fibra $\mathcal{C}_0$. El inconveniente de esta representación es la posible presencia de multiplicidades, representadas por factores múltiples de $m_S(0,T)$, que son también factores de $v_1(0,T), \ldots, v_n(0,T)$. Para eliminarlas, procedemos del siguiente modo: en primer lugar, calculamos

$$a(T) := \gcd\big(m_S(0,T), \frac{\partial m_S}{\partial T}(0,T)\big),$$

y limpiamos de cuadrados $m_S(0,T)$ calculando $m_0(T) := m_S(0,T)/a(T)$. A continuación, dado que $a(T)$ divide a $v_k(0,T)$, obtenemos

$$\frac{\partial m_S}{\partial T}(0,T)/a(T)X_k - v_k(0,T)/a(T), \quad (1 \le k \le n).$$

Para terminar, como m_0 y $(\partial m_S/\partial T)(0,T)/a(T)$ son elementos coprimos de $K[T]$, invertimos $(\partial m_S/\partial T)(0,T)/a(T)$ módulo m_0 y llegamos a las parametrizaciones $X_k - w_k(T)$.

Proposición 11.3.6. *Dada una solución geométrica de $\mathcal{C}$, provista por el algoritmo de la Proposición 11.3.5, podemos calcular una solución geométrica $m_0(T), X_1 - w_1(T), \ldots, X_n - w_n(T)$ de la variedad de dimensión cero $\mathcal{C}_0$ con $O(n\delta M(D))$ operaciones en K.*

Demostración. La representación densa de los polinomios $m_S(0,T), v_1(0,T), \ldots, v_n(0,T)$ puede calcularse con $O(nD\delta)$ operaciones aritméticas en K. El resto de las operaciones consiste en multiplicaciones, máximo común divisores e inversiones modulares de polinomios univariados, cuyos grados son menores o iguales que D; esto adiciona $O\big(nM(D)\big)$ operaciones en K.

□

Buscamos los puntos K–racionales de $\mathcal{C}_0$ remedando la demostración de la Proposición 10.2.2. Con $O\big(M(D)\log|K|\big)$ operaciones en K calculamos $h := \gcd(m_0, T^{|K|} - T) \in K[T]$ [vzGG99, Corollary 11.16]. La factorización de h en $K[T]$ se lleva a cabo probabilísticamente con $O\big(M(D)\log|K|\big)$ operaciones en K [vzGG99, Theorem 14.9]. Las raíces de h son los valores $\mathcal{L}(P)$ que se obtienen al evaluar la forma lineal $\mathcal{L}$ en los puntos $P \in \mathcal{C}_0(K)$. En particular, $\mathcal{L}(x^{(0)}) \in K$ es una raíz de h.

Evaluamos los polinomios w_k en las raíces α de h y obtenemos $x^{(0)}$ como el único punto q–racional que se expresa como $\big(w_1(\alpha), \ldots, w_n(\alpha)\big)$.

Reuniendo los resultados de las Proposiciones 11.3.5 y 11.3.6 obtenemos el principal resultado de este capítulo:

Teorema 11.3.7. *El único punto q–racional solución del sistema $F(X) = y^{(0)}$ puede calcularse con $O\big((\mathcal{T} + n^{1+\omega} + D^2)nM(D\delta)M(\log q\delta) + M(D)M^2(\log q\delta)\big)$ operaciones*

bit.

Dado que $D \leq \delta$, la estimación de complejidad que hemos logrado puede ser descrita como polinomial en $\mathcal{T}$ (el costo de evaluar $F_1, \ldots, F_n$), las cantidades n y $\log q$, y δ el grado del gráfico de F. Por lo tanto, el interés de nuestro algoritmo, y la consecuente (in)seguridad de los criptosistemas basados en aplicaiones polinomiales sobre cuerpos finitos, descansa en el parámetro δ. Recordemos que en el peor caso $\delta = \deg F_1 \cdots \deg F_n$. Adaptando los argumentos de [CGH$^+$03] es posible probar que cualquier algoritmo *universal* que resuelva $F(X) = y^{(0)}$ tiene necesariamente complejidad $(\deg F_1 \cdots \deg F_n)^{\Omega(1)}$, mostrando de esta manera la seguridad del correspondiente criptosistema con respecto a algoritmos universales de decodificación. Un algoritmo universal es un algoritmo que no distingue los sistemas de entrada de acuerdo a invariantes geométricos y representa un modelo para los algoritmos estandar basados en técnicas de reescritura, tales como los algoritmos de bases de Gröbner.

Como colofón, algunas observaciones acerca del comportamiento de nuestro algoritmo bajo las hipótesis de [SZ90]. Recordemos que [SZ90] requiere que la aplicación polinomial $F : \mathbb{A}^n \to \mathbb{A}^n$ sea polinomialmente inversible, con inversa $G := (G_1, \ldots, G_n)$ de grado $(nd)^{O(1)}$. Entonces muestran que G puede calcularse con $(\mathcal{T} nd)^{O(1)}$ operaciones. Bajo estas condiciones, tenemos que la proyección $\pi : V \to \mathbb{A}^n$ tiene grado 1, es decir, $D = 1$. Más aún, es fácil mostrar que el polinomio minimal $m_S(S, T)$ tiene grado acotado por $e := \max_{1 \leq k \leq n} \deg G_k$, y los algoritmos presentados en las Proposiciones 11.3.5 y 11.3.6 tienen en realidad complejidad $\mathcal{T}(nd)^{O(1)}$. Esto muestra que nuestro resultado de complejidad es polinomial con las hipótesis más fuertes de [SZ90].

12 Conclusiones

Para concluir este trabajo, planteamos algunas reflexiones sobre la tarea llevada a cabo, sobre los resultados obtenidos. A la vez, planteamos algunas inquietudes, algunos interrogantes, y posibles líneas de investigación que se despliegan a lo largo de la tesis.

- En términos de estimaciones generalistas, las estimaciones obtenidas en los Capítulos 4 y 5 están cerca de ser óptimas. Es decir, aun en el caso de que se mejoren las cotas de grado de las versiones efectivas del primer teorema de Bertini (recientemente Gregoire Lecerf [Lec06] ha obtenido una de orden $O(\delta^2)$ para cuerpos de característica mayor que $2\delta^2$), lo que llevaría a mejorar el segundo término de error de dichas estimaciones, los métodos que hemos empleado no permiten mejorar el término canónico del error de las mismas: $(\delta-1)(\delta-2)q^{r-1/2}$. Este término es el que impone condiciones de regularidad de orden por lo menos $O(\delta^4)$ al momento de deducir, a partir de las estimaciones, resultados de existencia y cotas inferiores no triviales sobre el número de puntos q–racionales. Sin embargo, obtuvimos resultados de existencia con la misma condición de regularidad (Teorema 4.3.5 y Corolario 5.2.4) aplicando directamente una versión efectiva del primer teorema de Bertini.

- La optimalidad antes señalada nos permite entrever que es necesario considerar familias particulares de variedades (distinguidas por alguna condición geométrica tal como no singularidad, intersección completa, etc) y beneficiarse de estas condiciones para obtener resultados de existencia, cotas superiores e inferiores o estimaciones. Nuestra estimación para una variedad intersección completa normal del Capítulo 6 es un primer paso en este sentido. Naturalmente, esperamos que nuestros métodos puedan ser extendidos a fin de obtener una versión efectiva de las estimaciones de Hooley (1.10). Creemos que es posible obtener mejores estimaciones que las de Ghorpade y Lachaud (1.11).

- No conocemos ejemplos de $\mathbb{F}_q$–variedades absolutamente irreducibles que no tengan puntos q–racionales, que nos permitan justificar que la imposición de condiciones de regularidad no es un hecho arbitrario.

- Como una doble evidencia, por un lado de la ausencia de resultados en casos específicos y, por otro, de que en casos específicos podemos obtener mejores resultados, tenemos la siguiente conjetura debida a Lachaud [GL02a, Conjecture 12.2]:

Conjetura: *Si* $V \subset \mathbb{P}^n$ *es una* $\mathbb{F}_q$*–variedad intersección completa de dimensión* $r \geq n/2$ *y de grado* $\delta \leq q+1$ *entonces*

$$|V(\mathbb{F}_q)| \leq \delta p_r - (\delta - 1)p_{2r-n}.$$

Es sabido que la conjetura es válida cuando V tiene codimensión 1 (en este caso, la conjetura no es más que la cota de Serre presentada en la Proposición 3.1.2) y cuando V es unión de variedades lineales de la misma dimensión.

- ¿Qué podemos decir respecto de la determinación del número exacto de puntos q–racionales de una $\mathbb{F}_q$–variedad? No es demasiado lo que se conoce. En el caso de $\mathbb{F}_q$–hipersuperficies, los ejemplos en los cuales se ha determinado de manera exacta la cantidad de puntos q–racionales son sumamente particulares (por ejemplo, ecuaciones diagonales); en el caso de $\mathbb{F}_q$–variedades es más notoria la ausencia de resultados.

- En términos de estimaciones, podríamos considerar que un *gran* problema por resolver es el de obtener –como hicieran Stepanov y Schmidt con los resultados de Weil– demostraciones elementales de los resultados de Deligne (1.9).

- En cuanto al aspecto algorítmico del trabajo, ya hemos señalado que nuestro algoritmo puede ser extendido al caso de una $\mathbb{F}_q$–variedad equidimensional V, en tanto tenga una componente absolutamente irreducible definida sobre $\mathbb{F}_q$. Sin embargo, no puede ser extendido a situaciones más generales dado que carecemos de herramientas para tratar el caso de una $\mathbb{F}_q$–variedad relativamente irreducible. Es este el caso que permanece inexplorado, ya sea por su dificultad intrínseca, por la imposibilidad de aplicar nuestras herramientas o por la casi inexistente bibliografía. Una dificultad clave es que los puntos q–racionales de una variedad relativamente irreducible anulan el discriminante de la misma (el discriminante de la forma de Chow de V) y, por lo tanto, no es posible aplicar nuestras técnicas para calcular puntos q–racionales. Por ejemplo, una $\mathbb{F}_q$–variedad proyectiva normal relativamente irreducible no tiene puntos q–racionales [FHJ94]. Sin embargo, creemos que el caso relativamente irreducible ocurre con una probabilidad muy baja (las únicas referencias, a la vez que evidencias, sobre este hecho se encuentran en unos trabajos de los años '60 de Leonard Carlitz [Car63, Car65]). Esto sugiere una posible línea de trabajo: estudiar con que frecuencia aparece este caso, o en otras palabras, caracterizar el caso promedio y, en consecuencia, desarrollar algoritmos que funcionen adecuadamente en el caso promedio.

- Queda pendiente la cuestión de considerar criptosistemas concretos y analizar cómo se pueden aplicar nuestras herramientas algorítmicas a fines de criptoanalizar-

los. Consideramos que algoritmos que funcionan en el caso promedio podrían ser importantes en el ámbito criptográfico.

Las observaciones precedentes pretenden poner de manifiesto la necesidad de desarrollar nuevos métodos, nuevos enfoques, para dar cuenta de las tareas no contempladas en nuestro trabajo y en la literatura matemática, en general.

Bibliografía

[ABRW96] M.E. Alonso, E. Becker, M.-F. Roy y T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. En *Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94*, volumen 143 de *Progr. Math.*, páginas 1–15, Boston, 1996. Birkhäuser Boston.

[Bal03] E. Ballico. An effective Bertini theorem over finite fields. *Advances in Geometry*, 3:361–363, 2003.

[BCS97] P. Bürgisser, M. Clausen y M.A. Shokrollahi. *Algebraic Complexity Theory*, volumen 315 de *Grundlehren Math. Wiss.* Springer, Berlin, 1997.

[BFS03] M. Bardet, J.-C. Faugère y B. Salvy. Complexity of Gröbner basis computation for semi–regular overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$. Rapport de Recherche INRIA RR–5049, `www.inria.fr/rrrt/rr-5049.html`, 2003.

[BG04] J. Brawley y S. Gao. On density of primitive elements for field extensions. Manuscrito, disponible en `www.math.clemson.edu/~sgao/`, 2004.

[BGHM97] B. Bank, M. Giusti, J. Heintz y G.M. Mbakop. Polar varieties and efficient real equation solving: The hypersurface case. *J. Complexity*, 13(1):5–27, 1997.

[BGHM01] B. Bank, M. Giusti, J. Heintz y G.M. Mbakop. Polar varieties and efficient real elimination. *Math. Z.*, 238(1):115–144, 2001.

[BGHP04] B. Bank, M. Giusti, J. Heintz y L.M. Pardo. A first approach to generalized polar varieties. *Kybernetika (Prague)*, 40(5):519–550, 2004.

[BGHP05] B. Bank, M. Giusti, J. Heintz y L.M. Pardo. Generalized polar varieties: Geometry and algorithms. *J. Complexity*, 21(4):377–412, 2005.

[Bog05] A. Bogdanov. Pseudorandom generators for low degree polynomials. En H.N. Gabow y R. Fagin, editores, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, páginas 21–30, New York, 2005. ACM.

[BP94] D. Bini y V. Pan. *Polynomial and matrix computations.* Progress in Theoretical Computer Science. Birkhäuser, Boston, 1994.

[BS83] W. Baur y V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Sci.*, 22:317–330, 1983.

[Car63] L. Carlitz. The distribution of irreducible polynomials in several indeterminates. *Ill. J. Math.*, 7:371–375, 1963.

[Car65] L. Carlitz. The distribution of irreducible polynomials in several indeterminates II. *Can. J. Math.*, 17:261–266, 1965.

[CG83] A.L. Chistov y D.Y. Grigoriev. Subexponential time solving systems of algebraic equations. I, II. LOMI preprints E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.

[CGH91] L. Caniglia, A. Galligo y J. Heintz. Equations for the projective closure and effective Nullstellensatz. *Discrete Appl. Math.*, 33:11–23, 1991.

[CGH+03] D. Castro, M. Giusti, J. Heintz, G. Matera y L.M. Pardo. The hardness of polynomial equation solving. *Found. Comput. Math.*, 3(4):347–420, 2003.

[CKPS00] N. Courtois, A. Klimov, J. Patarin y A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. En B. Preneel, editor, *EUROCRYPT 2000*, volumen 1807 de *Lecture Notes in Comput. Sci.*, páginas 71–79, Berlin, 2000. Springer.

[CLO92] D. Cox, J. Little y D. O'Shea. *Ideals, Varieties, and Algorithms: an introduction to computational algebraic geometry and commutative algebra.* Undergrad. Texts Math. Springer, New York, 1992.

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

[CM06a] A. Cafure y G. Matera. Fast computation of a rational point of a variety over a finite field. Aceptado para su publicación en Mathematics of Computation, disponible en `www.arxiv.org/pdf/math.AG/0406085`, 2006.

[CM06b] A. Cafure y G. Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields Appl.*, 12(2):155–185, 2006.

[CMW06] A. Cafure, G. Matera y A. Waissbein. Inverting bijective polynomial maps over finite fields. En G. Seroussi y A. Viola, editores, *Proceedings of the 2006 Information Theory Workshop, ITW2006 (Punta del Este,*

Uruguay, March 13–17, 2006), páginas 27–31. IEEE Information Theory Society, 2006.

[CR96] J.P. Cherdieu y R. Rolland. On the number of points of some hypersurfaces in $\mathbb{F}_q^n$. *Finite Fields Appl.*, 2(2):214–224, 1996.

[Dan94] V. Danilov. Algebraic varieties and schemes. En I.R. Shafarevich, editor, *Algebraic Geometry I*, volumen 23 de *Encyclopaedia of Mathematical Sciences*, páginas 167–307. Springer, Berlin Heidelberg New York, 1994.

[Del74] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, 43:273–307, 1974.

[Dwo60] B. Dwork. On the rationality of the zeta function of an algebraic variety. *Am. J. Math.*, 82:631–648, 1960.

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volumen 150 de *Grad. Texts in Math.* Springer, New York, 1995.

[Fau02] J.-C. Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (F5). En T. Mora, editor, *ISSAC'02: Proceedings of the International Symposium on Symbolic and Algebraic Computation, Lille, France, July 7–10, 2002*, páginas 75–83, New York, 2002. ACM Press.

[FHJ94] M. Fried, D. Haran y M. Jarden. Effective counting of the points of definable sets over finite fields. *Israel J. Math.*, 85(1-3):103–133, 1994.

[Ful84] W. Fulton. *Intersection Theory*. Springer, Berlin Heidelberg New York, 1984.

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

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

[GHH+97] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña y L.M. Pardo. Lower bounds for Diophantine approximation. *J. Pure Appl. Algebra*, 117,118:277–317, 1997.

[GHM+98] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern y L.M. Pardo. Straight–line programs in geometric elimination theory. *J. Pure Appl. Algebra*, 124:101–146, 1998.

[GHMP95] M. Giusti, J. Heintz, J.E. Morais y L.M. Pardo. When polynomial equation systems can be solved fast? En G. Cohen, M. Giusti y T. Mora, editores, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings AAECC-11*, volumen 948 de *Lecture Notes in Comput. Sci.*, páginas 205–231, Berlin, 1995. Springer.

[GHMP97] M. Giusti, J. Heintz, J.E. Morais y L.M. Pardo. Le rôle des structures de données dans les problèmes d'élimination. *C. R. Math. Acad. Sci. Paris*, 325:1223–1228, 1997.

[GJ79] M. Garey y D. Johnson. *Computers and Intractability: A Guide to the Theory of NP–Completeness*. Freeman, San Francisco, 1979.

[GKL04] S. Gao, E. Kaltofen y A. Lauder. Deterministic distinct-degree factorization of polynomials over finite fields. *J. Symbolic Comput.*, 38(6):1461–1470, 2004.

[GL02a] S. Ghorpade y G. Lachaud. Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Mosc. Math. J.*, 2(3):589–631, 2002.

[GL02b] S. Ghorpade y G. Lachaud. Number of solutions of equations over finite fields and a conjecture of Lang and Weil. En A.K. Agarwal et al., editores, *Number Theory and Discrete Mathematics (Chandigarh, 2000)*, páginas 269–291, New Delhi, 2002. Hindustan Book Agency.

[GLS01] M. Giusti, G. Lecerf y B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

[GM89] P. Gianni y T. Mora. Algebraic solution of systems of polynomial equations using Gröbner bases. En L. Huguet y A. Poli, editores, *Proceedings 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, AAECC–5, Menorca, Spain, June 15–19, 1987*, volumen 356 de *Lecture Notes in Comput. Sci.*, páginas 247–257, Berlin, 1989. Springer.

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

[Hei89] J. Heintz. On the computational complexity of polynomials and bilinear mappings. A survey. En L. Huguet y A. Poli, editores, *Proceedings 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, AAECC–5, Menorca, Spain, June 15–19,*

1987, volumen 356 de *Lecture Notes in Comput. Sci.*, páginas 269–300, Berlin, 1989. Springer.

[HMPW98] J. Heintz, G. Matera, L.M. Pardo y R. Wachenchauzer. The intrinsic complexity of parametric elimination methods. *Electron. J. SADIO*, 1(1):37–51, 1998.

[HMW01] J. Heintz, G. Matera y A. Waissbein. On the time–space complexity of geometric elimination procedures. *Appl. Algebra Engrg. Comm. Comput.*, 11(4):239–296, 2001.

[Hoo91] C. Hooley. On the number of points on a complete intersection over a finite field. *Journal of Number Theory*, 38(3):338–358, 1991.

[HP68] W. Hodge y D. Pedoe. *Methods of algebraic geometry. Vol. II*. Cambridge Math. Lib., Cambridge Univ. Press, Cambridge, 1968.

[HS82] J. Heintz y C. P. Schnorr. Testing polynomials which are easy to compute. En *International Symposium on Logic and Algorithmic, Zurich 1980*, volumen 30 de *Monogr. Enseig. Math.*, páginas 237–254, 1982.

[HW98] M.-D. Huang y Y.-C. Wong. An algorithm for approximate counting of points on algebraic sets over finite fields. En J. Buhler, editor, *Third International Symposium on Algorithmic Number Theory, ANTS-III, Portland, Oregon, USA, June 21-25, 1998*, volumen 1423 de *Lecture Notes in Comput. Sci.*, páginas 514–527, Berlin, 1998. Springer.

[HW99] M.-D. Huang y Y.-C. Wong. Solvability of systems of polynomial congruences modulo a large prime. *Comput. Complexity*, 8(3):227–257, 1999.

[HW00] M.-D. Huang y Y.-C. Wong. Extended Hilbert irreducibility and its applications. *J. Algorithms*, 37(1):121–145, 2000.

[IM88] H. Imai y T. Matsumoto. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. En C.G. Günther, editor, *Advances in Cryptology - EUROCRYPT '88, Workshop on the Theory and Application of Cryptographic Techniques, Davos, Switzerland, May 25-27, 1988*, volumen 330 de *Lecture Notes in Computer Science*, páginas 419–453, Berlin, 1988. Springer.

[Jol73] J.-R. Joly. Equations et variétés algébriques sur un corps fini. *Enseign. Math.*, 19:1–117, 1973.

[Kal95] E. Kaltofen. Effective Noether irreducibility forms and applications. *J. Comput. System Sci.*, 50(2):274–295, 1995.

[Kna01] M. Knapp. Artin's conjecture for forms of degree 7 and 11. *J. London Math. Soc. (2)*, 63:268–274, 2001.

[Kro82] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. Reine Angew. Math.*, 92:1–122, 1882.

[KS99] A. Kipnis y A. Shamir. Cryptanalysis of the HFE Public Key Cryptosystem by relinearization. En M.J. Wiener, editor, *Proceedings of Advances in Cryptology – CRYPTO'99, Santa Barbara, California, USA, August 15–19, 1999*, volumen 1666 de *Lecture Notes in Comput. Sci.*, páginas 19–30, Berlin, 1999. Springer.

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

[Lec03] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *J. Complexity*, 19(4):564–596, 2003.

[Lec06] G. Lecerf. Sharp precision in Hensel lifting for bivariate polynomial factorization. *Math. Comp.*, 75(254):921–933, 2006.

[LN83] R. Lidl y H. Niederreiter. *Finite fields.* Addison–Wesley, Reading, Massachusetts, 1983.

[Luo99] W. Luo. Rational points on complete intersections over F_{p}. *Int. Math. Res. Not.*, 16:901–907, 1999.

[LW54] S. Lang y A. Weil. The number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

[Mac16] F. S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge Univ. Press, Cambridge, 1916.

[Mat80] H. Matsumura. *Commutative Algebra.* Benjamin, 1980.

[Mum95] D. Mumford. *Algebraic Geometry I. Complex Projective Varieties.* Classics Math., Springer, Berlin, 2nd edition, 1995.

[Pan01] V. Pan. *Structured matrices and polynomials. Unified superfast algorithms.* Birkhäuser, Boston, 2001.

[Par95] L.M. Pardo. How lower and upper complexity bounds meet in elimination theory. En G. Cohen, M. Giusti y T. Mora, editores, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC–11*, volumen 948 de *Lecture Notes in Comput. Sci.*, páginas 33–69, Berlin, 1995. Springer.

[PS04] L.M. Pardo y J. San Martín. Deformation techniques to solve generalized Pham systems. *Theoret. Comput. Sci.*, 315(2–3):593–625, 2004.

[Rag02] J.-F. Ragot. Probabilistic absolute irreducibility test for polynomials. *J. Pure Appl. Algebra*, 172(1):87–107, 2002.

[Rou99] F. Rouillier. Solving zero–dimensional systems through the rational univariate representation. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):433–461, 1999.

[Sam67] P. Samuel. *Méthodes d'algèbre abstraite en géométrie algébrique.* Springer, Berlin Heidelberg New York, 1967.

[Sav98] J.E. Savage. *Models of Computation. Exploring the Power of Computing.* Addison Wesley, Reading, Massachussets, 1998.

[Sch74] W. Schmidt. A lower bound for the number of solutions of equations over finite fields. *J. Number Theory*, 6(6):448–480, 1974.

[Sch76] W. Schmidt. *Equations over Finite Fields. An Elementary Approach.* Volumen 536 en Lectures Notes in Math., Springer, New York, 1976.

[Sch80] J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[Sch03] E. Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13:349–393, 2003.

[Ser91] J-P. Serre. Lettre à M. Tsfasman. *Astérisque*, 198-200:351–353, 1991.

[Sha84] I.R. Shafarevich. *Basic algebraic geometry.* Grad. Texts in Math., Springer, New York, 1984.

[Sha94] I.R. Shafarevich. *Basic Algebraic Geometry: Varieties in Projective Space.* Springer, Berlin Heidelberg New York, 1994.

[Sko92] A. Skorobogatov. Exponential sums, the geometry of hyperplane sections, and some diophantine problems. *Israel J. Math.*, 80:359–379, 1992.

[SS90] I. Shparlinski y A. Skorobogatov. Exponential sums and rational points on complete intersections. *Mathematika*, 37:201–208, 1990.

[Str90] V. Strassen. Algebraic complexity theory. En J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, capítulo 11, páginas 634–671. Elsevier, Amsterdam, 1990.

[SZ90] C. Sturtivant y Z.-L. Zhang. Efficiently inverting bijections given by straight line programs. En *Proceedings of the 31st Annual Symposium on Foundations of Computer Science, FOCS'90 (St. Louis, Missouri, October 22–24, 1990)*, volumen 1, páginas 327–334. IEEE Computer Society Press, 1990.

[Vog84] W. Vogel. *Results on Bézout's theorem*, volumen 74 de *Tata Inst. Fundam. Res. Lect. Math.* Tata Inst. Fund. Res., Bombay, 1984.

[vzG86] J. von zur Gathen. Parallel arithmetic computations: a survey. En J. Gruska, B. Rovan y J. Wiedermann, editores, *Proceedings of the 12th International Symposium on Mathematical Foundations of Computer Science, Bratislava, Czechoslovakia, August 25–29, 1996*, volumen 233 de *Lecture Notes in Comput. Sci.*, páginas 93–112, Berlin, August 1986. Springer.

[vzGG99] J. von zur Gathen y J. Gerhard. *Modern computer algebra.* Cambridge Univ. Press, Cambridge, 1999.

[vzGKS97] J. von zur Gathen, M. Karpinski y I. Shparlinski. Counting curves and their projections. *Comput. Complexity*, 6(3):64–99, 1997.

[vzGSS03] J. von zur Gathen, I. Shparlinski y A. Sinclair. Finding points on curves over finite fields. *SIAM J. Comput.*, 32(6):1436–1448, 2003.

[Wei48] A. Weil. *Sur les courbes algébriques et les varietés qui s'en déduisent.* Hermann, Paris, 1948.

[Wei49] A. Weil. Number of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

[WP05] C. Wolf y B. Preneel. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report 2005/077, 2005. `http://eprint.iacr.org/`.

[Zar95] O. Zariski. *Algebraic surfaces.* Classics Math., Springer, Berlin, 1995.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. En *EUROSAM '79: Proceedings of International Symposium on Symbolic and Algebraic Computation, Marseille 1979*, volumen 72 de *Lecture Notes in Comput. Sci.*, páginas 216–226, Berlin, 1979. Springer.