Construcción y decodificación de códigos álgebro-geométricos a partir de curvas planas: algoritmos y aplicaciones

José Ignacio Farrán Martín

Valladolid – 1997

Impreso por: E.T.D., S.A.
Tamarit 104
08015 BARCELONA
ESPAÑA

Depósito legal: B-40483/96
ISBN: 84-7762-622-7

Para solicitar ejemplares de esta tesis doctoral dirigirse a:
Secretariado de Publicaciones e Intercambio Científico
UNIVERSIDAD DE VALLADOLID
Avda. Ramón y Cajal 7
47005 VALLADOLID
Tfno.: (983) 264000 - 250458 - Ext. 2247
Telex 26357
FAX (983) 302095

UNIVERSIDAD DE VALLADOLID
Departamento de Algebra, Geometría y Topología

Construcción y decodificación de códigos álgebro-geométricos a partir de curvas planas: algoritmos y aplicaciones

José Ignacio Farrán Martín

Memoria presentada bajo la dirección de
Antonio Campillo López
para la obtención del título de
Doctor en Ciencias Matemáticas

La tesis doctoral titulada *Construcción y decodificación de códigos álgebro-geométricos a partir de curvas planas: algoritmos y aplicaciones*, dirigida por el Dr. D. Antonio Campillo López, fue presentada por **D. José Ignacio Farrán Martín** el día 7 de Noviembre de 1997 en el Departamento de Algebra, Geometría y Topología de la Universidad de Valladolid ante el tribunal compuesto de la siguiente forma:

PRESIDENTE:
Dr. D. Juan Gabriel Tena Ayuso

VOCALES:
Dr. D. Ignacio Luengo Velasco
Dr. D. Tom Høholdt
Dr. D. Santos González Jiménez

SECRETARIO:
Dra. Dña. Sylvia Novo Martín

La Tesis obtuvo la calificación de Apto *cum Laude*

ANTONIO CAMPILLO LOPEZ, CATEDRATICO DE ALGEBRA DE LA UNIVERSIDAD DE VALLADOLID

CERTIFICA :

Que la presente Memoria titulada "Construcción y decodificación de códigos álgebro-geométricos a partir de curvas planas: algoritmos y aplicaciones" ha sido realizada bajo mi dirección en el Departamento de Algebra, Geometría y Topología de la Universidad de Valladolid por D. José Ignacio Farrán Martín para optar al grado de Doctor en Ciencias Matemáticas, y para que así conste en cumplimiento de la presente legislación, autoriza su presentación ante la Facultad de Ciencias de dicha Universidad.

En Valladolid a 24 de Septiembre de 1997 .

Fdo: Antonio Campillo López

José Ignacio Farrán Martín
Dpto. Matemática Aplicada a la Ingeniería
E. T. S. de Ingenieros Industriales
Universidad de Valladolid
Paseo del Cauce s/n
47011 Valladolid - SPAIN

$Tfno.$: 34 83 42 33 95
Fax : 34 83 42 34 06
$e-mail$: ignfar@eis.uva.es

Introducción

El origen de la teoría de códigos correctores de errores se encuentra en los trabajos de Golay, Hamming y Shannon hacia mediados del presente siglo, tanto en su vertiente probabilista como en la algebraica, y desde su inicio el tema ha sido siempre un problema de ingeniería, con aplicación tanto en la transmisión de información (ingeniería de telecomunicaciones) como en el almacenamiento de la misma en soporte digital (ingeniería informática), siendo su finalidad el preservar la calidad de la información y las comunicaciones contra la amenaza del ruido, la distorsión o el deterioro del medio. No obstante, el desarrollo de dicha teoría se ha realizado gracias a la utilización de técnicas matemáticas cada vez más sofisticadas; estas técnicas recorren múltiples campos de la matemática, que van desde la teoría de probabilidades, el cálculo combinatorio o el álgebra lineal hasta la aritmética, la teoría de cuerpos o la geometría algebraica.

Por otro lado, el estudio de la *teoría de códigos* está íntimamente ligado a una serie de tópicos propios de la matemática discreta tales como retículos, formas cuadráticas, empaquetamientos de esferas, sumas exponenciales, la teoría de grafos o la geometría aritmética, así como otra serie de temas de procedencia variada tales como la teoría de la información, la criptografía, el álgebra computacional o la teoría de la señal, entre otros.

La introducción en los años 70 por Goppa de una nueva construcción de códigos lineales a partir de curvas algebraicas lisas (llamados *códigos geométricos de Goppa* o códigos álgebro-geométricos) cambió por completo el panorama de investigación en el terreno de la teoría de códigos correctores de errores; por un lado, la codificación de dichos códigos no parecía ofrecer excesivos problemas (aunque no era tan clara y tan sencilla como en el caso de

los códigos lineales clásicos), y por otro sus parámetros podían ser fácilmente controlables a partir de fórmulas clásicas de la geometría algebraica (tales como el teorema de Riemann-Roch). Además, la introducción de dicha teoría permitió en los años 80 la construcción explícita de familias de códigos cuyos parámetros sobrepasan asintóticamente la cota de Varshamov-Gilbert, y en consecuencia dar una solución efectiva (y con complejidad polinomial) al problema principal de la teoría de códigos, que fue considerado por Shannon en términos probabilísticos pero sin dar ninguna idea constructiva sobre la existencia de tales familias.

A pesar del interés que suscitó el estudio de los códigos geométricos de Goppa desde su origen, no pudieron encontrarse algoritmos eficientes para su *decodificación* hasta finales de los años 80, gracias a sucesivos trabajos de Justesen, Larsen, Jensen, Havemose y Høholdt [62], Skorobogatov y Vlăduţ [102], y Porter, Shen y Pellikaan [88]. Estos métodos están lejos de la capacidad correctora de los códigos a los que se aplican, y algunos de ellos requieren condiciones restrictivas respecto al tipo de códigos que pueden utilizarse, pero algunos años más tarde surgieron nuevos métodos que resolvieron este problema de una forma efectiva, como es el caso de los algoritmos de Ehrhard [38] o Duursma [32]. En la actualidad se desarrollan algoritmos más rápidos y eficientes (a costa de perder algo de generalidad), basados en el esquema de decodificación mayoritaria de Feng y Rao [42], que utilizan o bien relaciones de recurrencia lineal (como Sakata [95]) o bien bases de Gröbner (como Saints y Heegard [93]).

No obstante, los códigos AG (álgebro-geométricos) apenas han sido implementados en la práctica por los ingenieros debido entre otras a las siguientes razones:

- En primer lugar, las ideas que hay detrás de este tipo de códigos son consideradas como demasiado abstractas en el campo de la ingeniería, y no se ha considerado práctico hacer el esfuerzo de comprender una teoría tan profunda como es el caso de la *geometría algebraica* si hay otras alternativas. En este sentido, los matemáticos están haciendo actualmente una descripción de este tipo de códigos y de su tratamiento práctico mediante una aproximación más elemental, sin hacer uso más que de nociones básicas de álgebra abstracta (ver [43], [44], [58] o [103]).

- Por otra parte, aunque los *parámetros* de los códigos álgebro-geométricos son mucho mejores que los clásicos en sentido asintótico (es decir, para

códigos de longitud arbitrariamente grande), las aplicaciones técnicas no se han visto aún en la necesidad práctica de sustituir los códigos que actualmente se utilizan por otros de mayor longitud sin que se dispare simultáneamente el coste y la tasa de error de los mismos. Como contrapartida, los códigos clásicos que actualmente se utilizan tienen una decodificación bastante más rápida y efectiva que cualquiera de los métodos que han sido desarrollados hasta la fecha para los códigos geométricos de Goppa, habiendo frenado esta circunstancia una apuesta definitiva por los códigos AG.

- Además, el proceso de *codificación* en el caso de los códigos estándar es muy claro, pudiéndose distinguir con precisión los símbolos de información de los símbolos de control; este fenómeno no se reproduce con tanta nitidez en los códigos álgebro-geométricos y sería una propiedad deseable con vistas a la implementación práctica.

- Por último, aunque algunos de los métodos de decodificación para códigos geométricos de Goppa son efectivos, su *preprocesamiento* es de una elevada dificultad e involucra una serie de algoritmos que resultan complejos al estar basados en métodos de la geometría algebraica computacional, incluso a nivel de software; por tanto, mientras éstos no se describan de forma totalmente eficiente en términos de operaciones elementales no podrán implementarse en hardware, que es la situación que se requiere en la práctica para las aplicaciones técnicas.

El *objetivo principal* de nuestro trabajo consiste precisamente en examinar con detalle los dos últimos puntos que acabamos de exponer, es decir, el problema de la *construcción efectiva y decodificación de los códigos geométricos de Goppa* y los algoritmos de geometría algebraica que están involucrados en dicho proceso. De forma más precisa, el problema más difícil en la construcción de tales códigos es el cálculo de una base del espacio vectorial $\mathcal{L}(G)$ asociado a un divisor racional G sobre una curva algebraica χ definida sobre un cuerpo finito $\mathbb{F}_q$. Para realizar este cálculo existen dos métodos generales basados en principios completamente diferentes: la vía algebraica dada por el algoritmo de Coates, basada en el cálculo del cierre íntegro de cierto anillo de funciones racionales (ver [35]), o la vía geométrica del algoritmo de Brill-Noether, basada en el proceso de resolución de singularidades y la teoría

de adjunción (ver [50]). Ambos métodos suponen que ya se dispone de un modelo plano singular para la curva.

Por otra parte, en los algoritmos de decodificación que hoy en día se consideran más eficientes el divisor considerado es de la forma $G = mP$, donde P es un punto racional de la curva; en este caso, el cálculo de una base de $\mathcal{L}(mP)$ es equivalente a calcular el *semigrupo de Weierstrass* Γ_P de la curva en P y construir explícitamente funciones racionales con un único polo en P cuyo orden sea un elemento arbitrario de dicho semigrupo. Este proceso puede realizarse como mostramos al final del capítulo 2 con ayuda de la teoría de adjuntas para el caso de curvas proyectivas planas. El algoritmo resultante se puede sustituir por otro que presenta una forma más sencilla y efectiva y que se basa en un resultado de Abhyankar y Moh, suponiendo que el modelo plano tenga una sola rama racional en el infinito y ésta esté definida sobre el cuerpo de definición de la curva, tomándose entonces como P el único punto en el infinito; esta vía alternativa de describir semigrupos de Weierstrass nunca había sido considerada anteriormente en el contexto de la teoría de códigos álgebro-geométricos, y constituye la parte más original del presente trabajo. El método da además una estimación del número de errores corregibles (la llamada distancia de Feng-Rao), que depende únicamente del citado semigrupo de Weierstrass.

El trabajo expuesto en la presente memoria está organizado de la siguiente manera:

- En el **capítulo 1** se presenta una breve exposición de los conceptos fundamentales de la teoría de códigos incluyendo el estudio de sus parámetros y su comportamiento asintótico, y tras ello se pasa a una rápida revisión de la geometría de curvas algebraicas con el fin de introducir los llamados códigos álgebro-geométricos con sus parámetros y su relación con el llamado problema principal de la teoría de códigos. El capítulo termina con una exhaustiva introducción al problema general de la decodificación y a los principales algoritmos que actualmente se conocen o se están desarrollando para decodificar los códigos geométricos de Goppa, incluyendo al final una aportación original (algoritmo 1.3 del apartado 1.3.4) que sintetiza dos de los algoritmos generales ya conocidos, como son los de Ehrhard y Duursma.

- El **capítulo 2** comienza por la introducción de los conceptos de parametrizaciones y ramas racionales de curvas planas, con el fin de presen-

tar de forma intrínseca el proceso de *desingularización* de un modelo plano singular y ciertos objetos combinatorios y geométricos racionales (es decir, definidos sobre el cuerpo base) asociados a dicho proceso, tras lo cual se describe la teoría clásica de adjunción y la llamada resolución sumergida, estudiando su relación con el proceso intrínseco. A continuación se introduce la *teoría de Brill-Noether*, que nos permite elaborar un algoritmo general para calcular una base del espacio $\mathcal{L}(G)$ para cualquier divisor G sobre la curva plana; este algoritmo (llamado de Brill-Noether) se presenta en su versión racional, en la cual el cuerpo base es un cuerpo perfecto arbitrario, G es un divisor racional y la base obtenida está definida sobre el cuerpo base, que es la versión que tiene utilidad práctica en la teoría de códigos álgebro-geométricos. Posteriormente, se muestra un algoritmo que calcula las llamadas *expresiones simbólicas de Hamburger-Noether*, de las cuales se deducen la resolución, la resolución sumergida y los objetos anteriormente aludidos, que no son otros que los bosques y configuraciones de resolución y resolución sumergida de la curva plana. Utilizando el algoritmo de cálculo de las expresiones simbólicas de Hamburger-Noether se encuentra en el teorema 2.4 un algoritmo que calcula bases para los espacios $\mathcal{L}(G)$ a partir del dato G y un modelo plano para la curva. Se termina el capítulo dando, en términos similares, un algoritmo dado por el teorema 2.5 que calcula el semigrupo de Weierstrass en una rama racional de una curva plana a partir de la ecuación de dicha curva. Los dos últimos resultados son conocidos desarrollos de la teoría clásica de curvas algebraicas, pero son originales en el contexto de su aplicación a la teoría de códigos álgebro-geométricos.

- El **capítulo 3** es el de mayor relevancia en la configuración total de la memoria. Comienza por estudiar dos semigrupos S_P y Γ_P en un punto racional P, siendo Γ_P el semigrupo de Weierstrass y S_P un subsemigrupo suyo auxiliar, suponiendo que éste sea el único punto del infinito de un modelo plano singular en donde sólo existe una rama, también racional. La descripción clásica de S_P a través del *teorema de Abhyankar-Moh* y el algoritmo de raíces aproximadas, es completada mediante un algoritmo original (lema 3.1) que calcula la diferencia entre ambos semigrupos. Ambos procesos proporcionan además funciones explícitas que alcanzan un único polo en P de orden arbitrario

dentro del semigrupo de Weierstrass Γ_P, lo cual se aplica fácilmente en el cálculo de una base de $\mathcal{L}(mP)$, y por tanto en la construcción efectiva y decodificación de los llamados códigos geométricos sobre un punto. En el resto del capítulo se expone brevemente cómo encontrar explícitamente modelos planos singulares con una sola rama en el infinito, cómo calcular una base entera para el anillo afín de coordenadas de la curva plana (necesario para poder computar la diferencia $\Gamma_P \setminus S_P$), y cómo puede calcularse la *distancia de Feng-Rao* del semigrupo de Weierstrass utilizando las propiedades dadas por el teorema de Abhyankar-Moh, la teoría de generadores de Apéry y las sucesivas modificaciones de éstos cuando añadimos los elementos de Γ_P que no están en S_P. Como resultado y resumen del capítulo, el teorema 3.4 muestra cómo el semigrupo de Weierstrass, funciones con polos únicamente en P de orden dado y la distancia de Feng-Rao de los sucesivos códigos sobre el punto P se pueden calcular todos ellos simultáneamente por medio de un mismo algoritmo.

Contents

Chapter 1

Decodificación de códigos geométricos de Goppa

El presente capítulo tratará de exponer brevemente los conceptos, resultados y problemas fundamentales de la *teoría de códigos*, así como una breve introducción a la teoría de curvas algebraicas, con el fin de poder explicar con más detalle la teoría de códigos álgebro-geométricos y su importancia en el panorama actual de investigación sobre la materia. El objetivo final del capítulo es exponer los principales métodos de decodificación desarrollados en los últimos años para dichos códigos, incluyendo entre ellos una aportación original en el método basado en la resolución de una *ecuación clave*.

1.1 Códigos correctores de errores

El modelo general de un sistema de protección contra los errores producidos en el almacenamiento o la transmisión de información a través de un canal discreto sin memoria sometido a ruido comprende los siguientes elementos:

1. Una **fuente de información** que genera una cadena o palabra de longitud k con símbolos o letras en un alfabeto Λ.

2. Un proceso de **codificación** que transforma unívocamente el mensaje anterior en otro de longitud $n \geq k$, sobre el mismo alfabeto u otro diferente, y al que se ha añadido información redundante suficiente

como para poder detectar y corregir un número razonable de errores que puedan producirse en el proceso de almacenamiento o de transmisión.

3. Un **canal** a través del cual se transmite el mensaje anteriormente codificado o en el cual se almacena dicha información, la cual puede sufrir algunos errores debidos al ruido existente en dicho canal, o al deterioro del mismo en el caso de almacenamiento en un soporte digital.

4. Un proceso de **decodificación** que asigna al mensaje distorsionado por el canal otro mensaje que, en caso de haberse producido pocos errores, es el mensaje introducido inicialmente en el canal, permitiéndonos así recuperar la información transmitida o almacenada, según el caso.

Con más precisión, la *codificación* es una aplicación inyectiva

$$\mathcal{C} \ : \ S \subseteq \Lambda^k \to \Gamma^n$$

y se llama **código** a la imagen C de dicha aplicación. En el conjunto Γ^n se define la **distancia de Hamming** entre dos palabras $\mathbf{x}, \mathbf{y} \in \Gamma^n$ como

$$d(\mathbf{x}, \mathbf{y}) \doteq \sharp\{x_i \neq y_i \mid i = 1, \ldots, n\}$$

y mide el número de errores cometidos en la transmisión cuando se recibe $\mathbf{x}$ en lugar de $\mathbf{y}$, dando lugar a una estructura de espacio métrico sobre Γ^n. Podemos definir entonces la cantidad

$$d \doteq d(C) \doteq \mathit{mín}\,\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \ \ \mathbf{x} \neq \mathbf{y}\ \}$$

llamada **distancia minimal** o **distancia mínima** del código C, y que representa el mínimo número de coordenadas diferentes entre dos palabras distintas cualesquiera de C.

La distancia minimal d está ligada a la *capacidad correctora* del código C. Más precisamente, la propiedad triangular de la distancia de Hamming permite mostrar que el código C detecta cualquier configuración de hasta $d-1$ errores cometidos en la transmisión de una palabra, siendo capaz de corregir (teóricamente) cualquier configuración de hasta $\left\lfloor \dfrac{d-1}{2} \right\rfloor$ errores.

El caso que consideraremos en adelante es aquél en que $\Lambda = \Gamma = \mathbb{F}_q$ es un cuerpo finito de cardinal q, $S = \mathbb{F}_q^k$ y $\mathcal{C}$ es una aplicación $\mathbb{F}_q$-lineal, en

cuyo caso diremos que $C \doteq Im(\mathcal{C})$ es un **código lineal** de **longitud** n y **dimensión** k, y llamaremos **redundancia** a la diferencia $n-k$.

Si C es un código lineal, se dice que G es una **matriz generatriz** del código C si es de tipo $n \times k$ y sus filas forman una base de C como subespacio de $\mathbb{F}_q^n$; si fijamos una matriz generatriz G, la operación de codificación puede describirse en forma matricial como $\mathbf{c} = \mathbf{m} \cdot G$, donde $\mathbf{m} \in \mathbb{F}_q^k$ es la información que queremos codificar. Si la matriz G es de la forma $G = (I_k|M)$, donde I_k es la matriz identidad de dimensión k, se dice que C es un *código en forma estándar*; en este caso, los k primeros símbolos de una palabra código se denominan *símbolos de información*, y los $n-k$ últimos se denominan *símbolos de control*. La codificación de un código estándar es muy sencilla, puesto que consiste en añadir al mensaje $\mathbf{m}$ los símbolos de control $\mathbf{m} \cdot M$, y un ejemplo típico es el llamado código de Hamming (ver MacWilliams-Sloane [72]).

Se dice que una matriz H de tipo $(n-k) \times n$ de rango máximo es una **matriz de control** del código C si la aplicación lineal dada por $S_H(\mathbf{x}) \doteq \mathbf{x} \cdot H^t$ tiene a C como núcleo; en este caso, podemos describir C como

$$C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x} \cdot H^t = \underline{0}\}$$

El *código dual* $C^\perp$ de un código lineal C se define como el subespacio ortogonal de C relativo a la forma bilineal simétrica no degenerada

$$\mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$$

dada por

$$\langle \mathbf{x}, \mathbf{y} \rangle \doteq \mathbf{x} \cdot \mathbf{y}^t$$

Se comprueba fácilmente que una matriz generatriz de $C^\perp$ es una matriz de control para C, y viceversa.

Para cada elemento $\mathbf{x} \in \mathbb{F}_q^n$ se define su **peso de Hamming** por $w(\mathbf{x}) \doteq \sharp\{x_i \neq 0 \mid i = 1, \ldots, n\}$, relacionado con la distancia de Hamming a través de la fórmula

$$d(\mathbf{x}, \mathbf{y}) \doteq w(\mathbf{x} - \mathbf{y})$$

De esta manera, la distancia minimal de C puede calcularse como

$$d(C) \doteq mín\,\{w(\mathbf{c}) \mid \mathbf{c} \in C, \;\; \mathbf{c} \neq 0\}$$

Finalmente, se llaman **parámetros fundamentales** de un código lineal C a la longitud n, la dimensión k y la distancia minimal d, en cuyo caso se dice que C es un código de *tipo* $[n, k, d]$. Asimismo, se llaman **parámetros asintóticos** de C al par $[R, \delta]$, donde $R \doteq k/n$ se llama **tasa de transmisión** del código y representa simultáneamente el coste y la velocidad de transmisión, y donde $\delta \doteq d/n$ se llama **distancia relativa** del código y mide la capacidad correctora de C en relación a su longitud.

Sea $\mathcal{C}_q$ el conjunto de todos los códigos sobre $\mathbb{F}_q$ (es decir, $\Lambda = \Gamma = \mathbb{F}_q$), lineales o no; se puede considerar la aplicación

$$\Psi \ : \ \mathcal{C}_q \to [0,1] \times [0,1]$$

$$C \mapsto (R(C), \delta(C))$$

donde la dimensión de C se define por $k(C) \doteq \log_q \sharp C$ en caso de que el código no sea lineal. Llamando $V_q \doteq Im\, \Psi$, se denomina **dominio de códigos** (sobre $\mathbb{F}_q$) al conjunto de puntos de acumulación U_q de V_q. Un resultado de *Manin* dice que existe una función continua

$$\alpha_q \ : \ [0,1] \to [0,1]$$

tal que $\alpha_q(\delta) = \sup\{R \mid (R, \delta) \in V_q\}$ para $\delta \in [0,1] \cap \mathbb{Q}$, y que además $U_q = \{(R, \delta) \mid 0 \leq R \leq \alpha_q(\delta)\}$ (ver Tsfasman-Vlăduţ [106]).

La función $\alpha_q(\delta)$ no se conoce explícitamente, pero se conocen algunas cotas para ella. En primer lugar, la **cota de Singleton**

$$\alpha_q(\delta) \leq 1 - \delta$$

establece una cota superior para el dominio de códigos, y se deduce de la desigualdad $d + k \leq n + 1$, válida para todo código de tipo $[n, k, d]$.

De hecho, esta cota puede refinarse fácilmente obteniendo la llamada **cota de Plotkin**

$$\alpha_q(\delta) \leq máx\, \{1 - \frac{q\delta}{q-1}, 0\}$$

Por otro lado, la cota inferior más relevante es la llamada **cota de Varshamov-Gilbert**, que establece

$$\alpha_q(\delta) \geq 1 - H_q(\delta)\ ,$$

donde

$$H_q(\delta) \doteq \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\, log_q(1-\delta)$$

es la función *entropía* para un canal simétrico q-ario, según el modelo probabilístico de Shannon para un sistema de transmisión de información.

El dominio de códigos está relacionado con el llamado *problema principal de la teoría de códigos*, que trata sobre el comportamiento asintótico de los parámetros de familias de códigos. Más precisamente, sea $W_n \subseteq \mathbb{F}_q^n$ el conjunto de todas las posibles configuraciones de errores que (por hipótesis) se pueden cometer al utilizar un código de longitud n en el sistema de transmisión (según el modelo algebraico de Hamming). Si $W'(C) \subseteq W_n$ es el conjunto de aquellas configuraciones que el código C de longitud n puede corregir, se denomina **tasa de error** del código C a la cantidad $e(C) \doteq 1 - \dfrac{\sharp W'(C)}{\sharp W_n}$, y mide la probabilidad de que el código C fracase al decodificar una palabra emitida.

Por otro lado, se llama **entropía de Hartley del sistema** al límite

$$\mu \doteq \lim_{n\to\infty} \frac{\log_q \sharp W_n}{n}$$

llamándose **capacidad del canal** al número $\beta \doteq 1 - \mu$. Lo que se pretende es tener familias de códigos de longitud arbitrariamente grande en las cuales la tasa de transmisión de los códigos se aproxime cuanto uno quiera a la capacidad del sistema a la vez que la tasa de error sea todo lo pequeña que se quiera. El siguiente resultado, debido a Shannon, garantiza la existencia de dichas familias (llamadas **familias de Shannon**) utilizando la *ley de los grandes números*, pero sin dar ninguna idea sobre su construcción (ver Shannon [99]).

Teorema 1.1 (Shannon) *Dado un modelo algebraico de sistema de transmisión con capacidad β, existen familias de códigos $\mathcal{C}$ tales que, para cualesquiera $\varepsilon_1 > 0$ y $\varepsilon_2 > 0$ prefijados, existe un código $C \in \mathcal{C}$ con $R(C) > \beta - \varepsilon_1$ y $e(C) < \varepsilon_2$.*

El **problema principal de la teoría de códigos** consiste en construir explícitamente familias de Shannon sobre cualquier cuerpo finito. En la práctica, la tasa de error de un código es difícil de calcular de forma explícita, con lo que suele tomar la distancia relativa $\delta(C)$ como medida de la calidad del código; de esta manera, la primera aproximación a la resolución del *problema principal* consiste en encontrar familias de códigos para las cuales R y δ son grandes cuando la longitud n tiende a infinito.

De forma más precisa, se pretende en una primera etapa encontrar familias de códigos cuyos parámetros asintóticos tengan un punto de acumulación en el interior del dominio de códigos (llamadas **buenas familias de códigos**), o mejor aún, familias de códigos cuyos parámetros asintóticos tengan un punto de acumulación que sobrepase la cota de Varshamov-Gilbert (llamadas **familias excelentes de códigos**), puesto que esta cota es una buena estimación de la capacidad del sistema, suponiendo que éste fuese simétrico y sin memoria. La solución explícita a este problema, conocido como *problema asintótico principal*, se ha obtenido exclusivamente mediante los llamados *códigos álgebro-geométricos*, y ésta es una de las razones por las cuales centraremos en ellos nuestro trabajo.

Por último, nos referiremos brevemente a otra posible aplicación de los códigos correctores de errores aparte de la usual, ya explicada al principio del capítulo, como es su utilización en el *sistema criptográfico de McEliece*; en este sistema, se encripta un mensaje $\mathbf{m}$ de longitud k sobre $\mathbb{F}_q$ utilizando como clave pública una matriz H inversible de tipo $k \times n$, mediante la fórmula

$$\mathbf{c} = \mathbf{m} \cdot H + \mathbf{e}$$

donde $\mathbf{e}$ es un vector de errores aleatorio de peso a lo más una cantidad prefijada t. El descifre se efectúa utilizando como clave privada un par de matrices (S, P), donde S es una matriz inversible de tipo $k \times k$ y P es una matriz $n \times n$ de permutaciones aleatorias, ambas prefijadas, que dan lugar a una descomposición $H = SGP$ de H, donde G, de tipo $k \times n$, es la matriz generatriz de un código corrector de errores capaz de corregir cualquier configuración de a lo más t errores. Un cálculo sencillo muestra que

$$\mathbf{c}P^{-1} = \mathbf{m}SG + \mathbf{e}P^{-1}$$

y como G es capaz de corregir hasta t errores, la clave privada nos permite obtener $\mathbf{m}S$ y en consecuencia $\mathbf{m}$. Este ingenioso procedimiento es aplicable en la práctica siempre que el código utilizado cuente con un algoritmo de decodificación eficiente, lo cual será estudiado con más detalle en la parte final del presente capítulo, al menos para el tipo de códigos que nos interesan.

1.2 Códigos álgebro-geométricos

A continuación estudiaremos un tipo especial de códigos lineales, construidos a partir de **curvas algebraicas**, y cuyos parámetros tienen un excelente

comportamiento asintótico, según se ha hecho referencia en el apartado anterior; para ello, recordaremos brevemente algunos resultados fundamentales de *geometría algebraica*.

Sea χ una curva algebraica proyectiva definida sobre un cuerpo perfecto $\mathbb{F}$, y supongamos que χ es *lisa* y *absolutamente irreducible* (es decir, irreducible sobre la clausura algebraica $\overline{\mathbb{F}}$ de $\mathbb{F}$). Para dicha curva, denotaremos por $\mathbb{F}(\chi)$ su cuerpo de **funciones racionales** sobre $\mathbb{F}$ y por $\Omega(\chi)$ el $\mathbb{F}(\chi)$-espacio vectorial de las **formas diferenciales racionales** sobre χ; nótese que, al ser $\mathbb{F}$ perfecto y $gr\ tr_{\mathbb{F}}\mathbb{F}(\chi) = 1$, toda forma diferencial sobre χ puede escribirse como $f \cdot d\phi$, donde $f, \phi \in \mathbb{F}(\chi)$ y ϕ es un *parámetro separable* de la extensión $\mathbb{F}(\chi)|\mathbb{F}$, es decir, un elemento tal que $\mathbb{F}(\chi)$ es una extensión separable de $\mathbb{F}(\phi)$.

Sobre la curva χ pueden considerarse diferentes tipos de **puntos**: los puntos **geométricos**, con coordenadas en la clausura algebraica $\overline{\mathbb{F}}$ de $\mathbb{F}$, los puntos **racionales** sobre $\mathbb{F}$, con coordenadas en el cuerpo de definición $\mathbb{F}$, y los puntos **cerrados** del esquema (que en adelante llamaremos abreviadamente *puntos cerrados*), que pueden verse también como clases de puntos geométricos conjugados por la acción del grupo de Galois de la extensión $\overline{\mathbb{F}}|\mathbb{F}$. Se define el *grado* de un punto cerrado P como el cardinal de la clase de conjugación que representa, y éste coincide con el grado de la extensión $\mathbb{F}'$ de $\mathbb{F}$, donde $\mathbb{F}'$ es el cuerpo residual de P. En consecuencia, P es racional si y sólo si tiene grado 1. El conjunto de todos los puntos racionales de χ sobre $\mathbb{F}$ se denota por $\chi(\mathbb{F})$.

Un **divisor racional** sobre $\mathbb{F}$ es una combinación lineal formal finita de puntos cerrados de χ con coeficientes enteros; si $D = \sum_P n_P \cdot P$ es un divisor racional, se define su **grado** como $deg\, D \doteq \sum_P n_P \cdot deg\, P$, donde $deg\, P$ denota el grado del punto P, y se llama **soporte** de D al conjunto $sop\,(D)$ de los puntos cerrados de χ para los cuales $n_P \neq 0$.

Asociados a un divisor racional D, pueden definirse los siguientes *espacios*:

$$\mathcal{L}(D) \doteq \{\varphi \in \mathbb{F}(\chi) \mid (\varphi) + D \geq 0\} \cup \{0\}$$

$$\Omega(D) \doteq \{\omega \in \Omega(\chi) \mid (\omega) \geq D\} \cup \{0\}$$

donde (φ) es el divisor asociado a una función racional no nula φ o **divisor principal**, y (ω) es el divisor asociado a una forma diferencial no nula ω o **divisor canónico**; nótese que $deg\,(\varphi) = 0$ debido al *teorema de Bezout*, y que $deg\,(\omega) = 2g - 2$, donde g es el **género** (geométrico) de la curva χ.

Ambos son $\mathbb{F}$-espacios vectoriales de dimensión finita, y denotamos sus dimensiones por $\ell(D)$ e $i(D)$ respectivamente; para todo divisor racional D, se verifica la igualdad dada por el **teorema de Riemann-Roch**

$$\ell(D) - i(D) = deg\ D + 1 - g$$

que es la herramienta fundamental para el estudio de los códigos con los que trabajaremos.

Por otro lado, el **teorema de los residuos** establece que, para toda forma diferencial ω sobre χ, se verifica

$$\sum_{P \in sop\,((\omega)_\infty)} res_P(\omega) = 0$$

donde el residuo $res_P(\omega)$ se calcula a partir de una expresión local de ω en términos de un parámetro separable (ver Fulton [45]).

Los divisores principales y los divisores canónicos forman sendas clases de equivalencia, en relación a la llamada **equivalencia lineal** en el grupo $Div_{\mathbb{F}}(\chi)$ de divisores racionales sobre χ dada por

$$D \equiv D' \iff D = D' + (\varphi),\ \ \exists \varphi \in \mathbb{F}(\chi) \setminus \{0\}$$

En consecuencia, si en los espacios $\mathcal{L}(D)$ y $\Omega(D)$ se cambia D por otro divisor en la misma clase de equivalencia lineal, los $\mathbb{F}$-espacios vectoriales obtenidos son isomorfos a los anteriores.

Además, para cualquier divisor racional D y para cualquier divisor canónico K, se tiene el siguiente **principio de dualidad**:

$$(a) \quad \mathcal{L}(D) \cong \Omega(K - D)$$

$$(b) \quad \mathcal{L}(K - D) \cong \Omega(D)$$

Aplicando el teorema de Riemann-Roch, es inmediato comprobar que $\mathcal{L}(D) = 0$ si $deg(D) < 0$ y, por dualidad, $\Omega(D) = 0$ si $deg(D) > 2g - 2$. Por último, es fácil ver que $\ell(0) = 1$, y por lo tanto $i(0) = g$, donde $\Omega(0)$ es el espacio de las llamadas *formas diferenciales de primera especie*.

Para construir los llamados **códigos álgebro-geométricos**, nos reduciremos al caso en que $\mathbb{F} = \mathbb{F}_q$ es un cuerpo finito (en particular perfecto). En este caso, sobre la curva χ se considera un divisor racional de la forma

$D = P_1 + \ldots + P_n$, donde $P_i \in \chi(\mathbb{F}_q)$, y otro divisor racional G con soporte disjunto al de D; entonces, tenemos bien definidas las dos aplicaciones $\mathbb{F}_q$-lineales siguientes:

$$\begin{array}{rcl} ev_D \ : \ \mathcal{L}(G) & \rightarrow & \mathbb{F}_q^n \\ \varphi & \mapsto & (\varphi(P_1), \ldots, \varphi(P_n)) \end{array}$$

$$\begin{array}{rcl} res_D \ : \ \Omega(G-D) & \rightarrow & \mathbb{F}_q^n \\ \omega & \mapsto & (res_{P_1}(\omega), \ldots, res_{P_n}(\omega)) \end{array}$$

En consecuencia, podemos definir los códigos siguientes:

$$C_L \doteq C_L(D,G) \doteq Im\,(ev_D)$$
$$C_\Omega \doteq C_\Omega(D,G) \doteq Im\,(res_D)$$

Usando el citado *teorema de los residuos* es fácil comprobar que, si $2g-2 < deg\,G < n$, ambos códigos son *duales* uno del otro, es decir

$$C_L = C_\Omega^\perp$$

Por otro lado, dados D y G en las condiciones anteriores, existe una forma diferencial ω tal que

$$C_L(D,G) = C_\Omega(D, D-G+(\omega))$$

con lo que, a efectos teóricos, basta considerar los códigos de uno de los dos tipos.

Por otra parte, es inmediato ver que

$$ker(ev_D) = \mathcal{L}(G-D)$$

$$ker(res_D) = \Omega(G)$$

y por tanto

$$dim\ C_L = \ell(G) - \ell(G-D)$$
$$dim\ C_\Omega = i(G-D) - i(G)$$

(ver detalles en Stichtenoth [103]).

Esto nos permite enunciar el siguiente resultado, debido a Goppa, que da una estimación de los parámetros fundamentales de los códigos que acabamos

de definir (también llamados *códigos geométricos de Goppa*), y en cuya demostración juega un papel esencial la *fórmula de Riemann-Roch* anteriormente citada; por supuesto, la longitud de ambos códigos es obviamente n, es decir, el número de puntos racionales usados en el divisor D.

Teorema 1.2 (Goppa) *Supongamos que* $2g-2 < deg\, G < n$*; entonces las aplicaciones* ev_D *y* res_D *son inyectivas, y se tiene*

$$(1) \quad \left[\begin{array}{lcl} k(C_L) & = & deg\, G + 1 - g \\ d(C_L) & \geq & n - deg\, G \doteq d^*(C_L) \end{array} \right.$$

$$(2) \quad \left[\begin{array}{lcl} k(C_\Omega) & = & n - deg\, G + g - 1 \\ d(C_\Omega) & \geq & deg\, G + 2 - 2g \doteq d^*(C_\Omega) \end{array} \right.$$

En las expresiones anteriores, la cota inferior para la distancia minimal en cada caso se denomina **distancia de Goppa** del correspondiente código álgebro-geométrico, y será denotada simplemente por d^* una vez fijado el código con el que estemos trabajando. Nótese que estas estimaciones dependen únicamente del grado del divisor G (fijados n y g) con lo que, con vistas a conseguir códigos con parámetros prefijados, podríamos suponer que $G = mP$, donde $m > 0$ y P es un punto racional que no esté en el soporte de D (siempre que tal punto exista, es decir, siempre que no utilicemos todos los puntos racionales de la curva en el divisor D), con la ventaja adicional de que este tipo de códigos (llamados *códigos sobre un punto*) pueden decodificarse de una manera bastante eficiente y la capacidad correctora del código puede incrementarse con respecto a la distancia de Goppa, como veremos en el siguiente apartado. Además, aunque no aprovechemos todos los puntos racionales de la curva en la construcción del divisor D, esto no va a influir en la obtención de códigos con longitud arbitrariamente grande, hecho de gran interés en la práctica. Por todas estas razones, son éstos los códigos álgebro-geométricos más ampliamente estudiados en la actualidad, y es por ello que la parte más importante de nuestro trabajo está dedicada a la construcción efectiva de este tipo de códigos.

En cuanto a la *descripción* de estos códigos en la práctica, se puede dar una matriz generatriz del código $C_L(D, G)$ en la forma

$$\begin{pmatrix} \varphi_1(P_1) & \dots & \varphi_1(P_n) \\ \dots & \dots & \dots \\ \varphi_k(P_1) & \dots & \varphi_k(P_n) \end{pmatrix}$$

donde $\{\varphi_1, \ldots, \varphi_k\}$ es una base del espacio vectorial $\mathcal{L}(G)$ sobre $\mathbb{F}_q$ y $k = \ell(G)$, asumiendo la hipótesis $2g - 2 < deg\, G < n$ del *teorema de Goppa*. En consecuencia, teniendo en cuenta la dualidad $C_\Omega = C_L^\perp$, la matriz anterior es también una matriz de control para el código $C_\Omega(D, G)$, con lo que éste último puede describirse como

$$C_\Omega(D, G) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \varphi_i(P_1)\, x_1 + \ldots + \varphi_i(P_n)\, x_n = 0, \;\; i = 1, \ldots, k\}$$

lo cual pone de relevancia la necesidad de calcular de forma efectiva una base del espacio $\mathcal{L}(G)$ para un divisor racional G dado, problema que será abordado de forma exhaustiva en los siguientes capítulos y que constituye uno de los objetivos fundamentales del presente trabajo. Por otro lado se necesita además saber evaluar una función racional en un punto racional cualquiera de la curva, cosa que se puede hacer en términos de un modelo plano para la curva mediante explosiones sucesivas en dicho punto (ver [51] para más detalles). Se podría describir análogamente este tipo de códigos en su versión dual, es decir, en términos de diferenciales y residuos, pero esta vía alternativa no es tan utilizada como la anteriormente descrita.

Para finalizar esta sección, volvemos sobre el *problema asintótico principal de la teoría de códigos*, para dar una indicación de su resolución efectiva utilizando los códigos álgebro-geométricos. En primer lugar, si queremos conseguir códigos geométricos de Goppa de longitud arbitrariamente grande, necesitamos encontrar curvas con una cantidad arbitrariamente grande de *puntos racionales* sobre $\mathbb{F}_q$; en relación a este problema, conviene recordar las **fórmulas de Weil**, según las cuales el número de puntos racionales de χ sobre el cuerpo $\mathbb{F}_{q^m}$ viene dado por

$$N_m = q^m + 1 - \sum_{i=1}^{g} (\alpha_i^m + \overline{\alpha_i}^m), \quad \forall m \geq 1$$

donde $|\alpha_i| = |\overline{\alpha_i}| = \sqrt{q}$ ($\alpha_i \in \mathbb{C}$) satisfacen

$$Z(\chi, t) = \frac{\prod_{i=1}^{g} (1 - \alpha_i t)(1 - \overline{\alpha_i} t)}{(1 - t)(1 - qt)}$$

y $Z(\chi, t) \doteq \sum_{k=0}^{\infty} a_k t^k$ es la *función zeta* de la curva χ, es decir, a_k es el número de divisores racionales efectivos de grado k sobre χ (ver Weil [110]). Estas

fórmulas permiten acotar superiormente el número de puntos racionales sobre $\mathbb{F}_q^m$ mediante las llamadas **cotas de Hasse-Weil**

$$|N_m - (q^m + 1)| \leq 2g\sqrt{q^m}$$

En particular, si $m = 1$ se obtiene la cota

$$|\sharp\chi(\mathbb{F}_q) - (q + 1)| \leq 2g\sqrt{q}$$

diciéndose que la curva χ es *maximal* si alcanza el máximo número posible de puntos en la desigualdad anterior, es decir, si q es un cuadrado y $\sharp\chi(\mathbb{F}_q) = (q + 1) + 2g\sqrt{q}$. No obstante, las cotas de Hasse-Weil no son una estimación muy fina si el género g es muy grande, como se podrá deducir fácilmente de los resultados que expondremos más adelante.

Por otra parte, conseguir $\chi_i(\mathbb{F}_q) \geq n$ arbitrariamente grande no es suficiente para obtener una buena familia de códigos si no conseguimos controlar el *crecimiento del género* de las curvas χ_i. De forma un poco más precisa, diremos qué condiciones deben cumplir dichas familias de curvas para poder obtener familias de códigos que sobrepasen la cota de Varshamov-Gilbert.

Como la gráfica determinada por la cota de Varshamov-Gilbert es diferenciable y convexa, es fácil comprobar que existe un punto en el que la tangente tiene pendiente -1 y en el que dicha recta deja a la gráfica siempre por encima de la misma; dicha tangente es la recta $R + \delta = 1 - S_0$, donde $S_0 = S_0(q) = \log_q \dfrac{2q-1}{q}$. En consecuencia, si tomamos un número $1 < S < S_0$, la recta $R + \delta = 1 - S$ (llamada *recta de Tsfasman*) tiene un segmento propio contenido en el dominio de códigos sobre $\mathbb{F}_q$ que situado por encima de la cota de Varshamov-Gilbert (ver [105]).

Por otro lado, se define el número

$$A(q) \doteq \sup_{\chi} \left\{ \limsup_{g \to \infty} \frac{N_q(\chi)}{g(\chi)} \right\}$$

donde $N_q(\chi) \doteq \sharp\chi(\mathbb{F}_q)$, y el extremo superior se extiende a todas las curvas χ definidas sobre $\mathbb{F}_q$ lisas y absolutamente irreducibles, si bien los resultados pueden generalizarse (con ciertas hipótesis) a curvas reducidas (ver [40]). Este número es finito, pues aplicando las fórmulas de Hasse-Weil se tiene que $A(q) \leq 2\sqrt{q}$, y además es estrictamente positivo para todo posible q, gracias a un resultado de *Serre* que utiliza una construcción con torres de cuerpos

de clases (ver [98]). Pues bien, si se consigue una familia de curvas tal que el límite superior del cociente entre el número de puntos racionales y el género supere $1/S_0$, Tsfasman demostró que ciertos códigos definidos sobre dichas curvas sobrepasan la cota de Varshamov-Gilbert. De forma más precisa, si $1 < A(q) < \infty$ (en particular, $q \geq 5$), fijamos un número $b \in \mathbb{R}$ tal que $2\,S(q) < b < 1 + S(q)$, donde $S(q) \doteq 1/A(q)$, y tomamos una sucesión de curvas $(\chi_i)_{i=1}^{\infty}$ tal que

$$\lim_{i\to\infty} \frac{N_q(\chi_i)}{g(\chi_i)} = A(q)$$

Llamemos $n_i \doteq N_q(\chi_i)$, $D_i \doteq P_1^i + \ldots + P_{n_i-1}^i$ y $G_i \doteq b_i\, P_{n_i}^i$, donde $P_1^i, \ldots, P_{n_i}^i$ son los puntos racionales de la curva χ_i, y donde $b_i \in \mathbb{R}$ verifican que $\lim_{i\to\infty} \dfrac{b_i}{n_i - 1} = b$. Entonces la sucesión de códigos $C_i \doteq C_\Omega(D_i, G_i)$ tiene parámetros asintóticos tales que

$$\begin{array}{rcccl} \lim\limits_{i\to\infty} R(C_i) & = & 1 + S(q) - b & > & S(q) \\ \lim\limits_{i\to\infty} \delta(C_i) & = & b - 2\,S(q) & > & 0 \end{array}$$

y en particular superan asintóticamente la cota de Varshamov-Gilbert siempre que $S(q) \geq S_0$. Este resultado implica, en particular, la llamada *desigualdad AG* (de *Algebraic Geometry bound*), que establece

$$R + \delta \geq 1 - S(q)$$

Ahora bien, gracias a un resultado de Drinfeld y Vlăduţ, se sabe que $A(q) \leq \sqrt{q} - 1$ para todo q (ver [30]), y de hecho se da la igualdad si q es un cuadrado; este último resultado fue probado por Ihara e, independientemente, por Tsfasman, Vlăduţ y Zink. En consecuencia, el problema asintótico tiene una posible solución efectiva para los cuadrados $q \geq 49$ (debido a la desigualdad $A(q) \geq 1/S_0$). Para los restantes q habría que dar cotas inferiores suficientemente grandes para $A(q)$ cuando q no es cuadrado, pues en este caso su valor exacto es aún un problema abierto, así como buscar una solución alternativa cuando $A(q) < 1/S_0$.

En cuanto a la efectividad de la construcción, ha habido hasta ahora dos vías alternativas para construir familias de curvas alcanzando la *cota de Drinfeld-Vlăduţ*. La vía clásica, debida a Katsman, Manin, Tsfasman y Vlăduţ, consiste en utilizar las *curvas modulares de Drinfeld* (ver [64] y [74]),

cuya construcción tiene una complejidad polinomial si bien las ideas son muy sofisticadas y el problema de la decodificación efectiva está aún abierto. Una vía más moderna, debida a García y Stichtenoth (ver [46]), utiliza *torres de cuerpos de funciones racionales*; esta alternativa es más simple desde el punto de vista conceptual, pero mantiene la dificultad de la decodificación efectiva debido al problema ya mencionado de la construcción explícita de bases para los espacios $\mathcal{L}(G)$.

1.3 El problema de la decodificación

A continuación expondremos las generalidades de la teoría de decodificación de códigos correctores de errores, para pasar en seguida a la descripción de las principales líneas en las que se trabaja hoy en día para decodificar los códigos geométricos de Goppa, haciendo referencia a la generalidad de los algoritmos, así como a su efectividad y a su complejidad.

1.3.1 Planteamiento del problema

Dado un código C, nos planteamos la existencia de un *algoritmo efectivo* de decodificación para C que sea *eficiente* y, a ser posible *rápido* , puesto que no basta con saber que el código es capaz de corregir teóricamente cierto número de errores si no somos capaces, mediante un algoritmo, de decodificar una palabra recibida en un tiempo razonablemente corto en relación a la longitud n del mensaje (concretamente, con una *complejidad polinomial en* n). Además, la mayor o menor rapidez del mismo puede condicionar fuertemente su utilización en ciertas aplicaciones que, en la práctica real, requieren una decodificación rápida de los datos.

Para ello, fijamos un código arbitrario $C \subseteq \Gamma^n$ de dimensión k; si $\mathbf{c}$ es la palabra transmitida e $\mathbf{y}$ la palabra recibida, denotamos $\mathbf{e} \doteq \mathbf{y} - \mathbf{c}$ al *vector error*, con lo que $\{i \,|\, e_i \neq 0\}$ es el conjunto de *posiciones de error*, los e_i son los *valores del error* y $wt(\mathbf{e})$ es el *número de errores* cometidos. Si garantizamos técnicamente que el número de errores es a lo sumo $(d-1)/2$, donde d es la distancia minimal de C, estamos seguros de que $\mathbf{c}$ es la palabra del código más próxima a la palabra recibida, en relación a la distancia de Hamming. El inconveniente de este método es que el cálculo de la palabra código más próxima a una dada no es eficiente desde el punto de

vista algorítmico, al ser un problema de tipo NP-completo (ver Welsh [111]).

En términos generales, se llama **decodificador** para el código C a toda aplicación

$$\mathcal{D} \ : \ \Gamma^n \to C^* \doteq C \cup \{?\}$$

tal que $\mathcal{D}(\mathbf{c}) = \mathbf{c}$, para todo $\mathbf{c} \in C$, permitiendo como salida el símbolo ? en caso de que $\mathcal{D}$ fracase al intentar decodificar una cierta palabra potencialmente recibida. Si además $\mathcal{D}(\mathbf{y})$ es, para todo $\mathbf{y}$, la palabra código más próxima a $\mathbf{y}$, se dice que $\mathcal{D}$ es un *decodificador de mínima distancia*, y es el que minimiza la probabilidad de error en la decodificación para el caso de un canal q-ario simétrico.

Si $0 \leq t \leq (d-1)/2$, el decodificador $\mathcal{D}$ se llama *t-corrector* (o *de distancia acotada por t*) si $\mathcal{D}(\mathbf{y})$ es la palabra código más próxima a $\mathbf{y}$ siempre que $d(\mathbf{y}, C) \leq t$. En particular, si $t = \lfloor (d-1)/2 \rfloor$ se dice que $\mathcal{D}$ *decodifica hasta la mitad de la distancia minimal*.

Un **algoritmo de decodificación** para una clase de códigos, es una aplicación $\mathcal{A}$ que asigna a cada código C de la clase un decodificador $\mathcal{D}_C$ para el código C junto con un algoritmo $\mathcal{A}_C$ para calcular la imagen por $\mathcal{D}_C$ de cualquier palabra que pueda recibirse en la transmisión, y será de diferente naturaleza según el tipo de decodificador que sea $\mathcal{D}_C$. En general, lo que nos interesa es un *algoritmo de decodificación de mínima distancia*, es decir, tal que $\mathcal{D}_C$ decodifique hasta la mitad de la distancia minimal para todo código C de la familia. La construcción de tales algoritmos para clases arbitrarias de códigos es un problema de tipo NP-completo, y éste es precisamente el fundamento principal del *criptosistema de McEliece* al que nos referimos anteriormente.

El cálculo de $\mathcal{D}_C(\mathbf{y})$ para C e $\mathbf{y}$ dados (donde $\mathbf{y}$ tiene la misma longitud que C y está escrito en el mismo alfabeto) puede descomponerse en dos partes: el **preprocesamiento**, donde agrupamos el conjunto de operaciones que son comunes a toda palabra $\mathbf{y}$ recibida y que sólo dependen por tanto del código C, las cuales sólo se efectúan una vez y en las que podemos permitir un mayor consumo de tiempo (dentro de la eficiencia), y la **decodificación** propiamente dicha, en donde englobamos el resto de las operaciones, a las cuales exigiremos la mayor rapidez posible, puesto que se repetirán cada vez que se reciba un mensaje diferente; el problema así planteado se denomina *decodificación de distancia mínima con preprocesamiento*. Los algoritmos de decodificación conocidos con complejidad polinomial son válidos únicamente

para determinadas clases de códigos lineales y son de distancia acotada; el mismo resultado para la totalidad de los códigos lineales y decodificando hasta la mitad de la distancia minimal es aún un problema abierto.

A partir de ahora nos ocuparemos únicamente de la decodificación de códigos geométricos de Goppa, y más concretamente de los *códigos residuales* C_Ω . Fijemos pues un código $C = C_\Omega(D, G)$, donde $D = P_1 + \ldots + P_n$ con P_i puntos racionales de la curva χ considerada. Como la distancia minimal exacta no es conocida en general, no podremos pensar (en principio) en un algoritmo que decodifique hasta la mitad de la distancia minimal, si no que tendremos que contentarnos con la mitad de alguna cota inferior de la misma, que en la mayoría de los casos es la distancia de Goppa.

En primer lugar, es fácil darse cuenta que si sabemos que las posiciones de error en el caso de un código lineal cualquiera se encuentran en un conjunto de índices J de cardinal estrictamente menor que la distancia minimal, los valores del error pueden hallarse resolviendo el sistema lineal

$$\begin{cases} \mathbf{x}H = \mathbf{y}H \\ x_j = 0 \ \text{ si } \ j \notin J \end{cases}$$

donde H es una matriz de control del código e $\mathbf{y}$ es la palabra recibida; nótese que el vector error es una solución del sistema y además es única, puesto que si $\mathbf{x}$ fuese otra distinta entonces la palabra $\mathbf{x} - \mathbf{e}$ estaría en el código y tendría peso menor estrictamente que la distancia minimal.

En consecuencia, nos basta en nuestro caso con determinar un conjunto $I \subseteq \{1, \ldots, n\}$ de cardinal suficientemente pequeño que contenga las posiciones de error. De hecho, la mayor parte de los algoritmos conocidos están planteados de la siguiente manera: "hallar una función racional f (dentro de un espacio de funciones relativamente pequeño) que se anule en todo punto P_i tal que $e_i \neq 0$". Tales funciones se denominan **funciones localizadoras de errores**, y nos permiten decodificar correctamente siempre que el número de ceros que tienen dentro del soporte de D sea menor que $d - 1$; esto se puede garantizar en general imponiendo condiciones sobre los divisores D y G, así como acotando superiormente el número de errores que pueden cometerse y dando una buena estimación de la distancia minimal.

1.3.2 Decodificación lineal

Sea el código $C = C_\Omega(D, G)$ y $\mathbf{e} = \mathbf{y} - \mathbf{c}$ como en el párrafo anterior; sea F un divisor arbitrario (usualmente se toma F con soporte disjunto al de D, pero en lo que sigue se verá que no es necesario). Llamaremos *divisor de error*, y será denotado por $D_\mathbf{e}$, al único divisor $0 \leq D_\mathbf{e} \leq D$ tal que $\upsilon_{P_i}(D_\mathbf{e}) > 0$ si y sólo si $e_i \neq 0$, donde $\upsilon_{P_i}(D)$ denota el coeficiente de P_i en D. El conjunto de todas las funciones de $\mathcal{L}(F)$ cuyos ceros contienen las posiciones de error es el espacio $\mathcal{L}(F - D_\mathbf{e})$, y se obtiene a partir de $\mathcal{L}(F)$ imponiendo t condiciones lineales, donde t es el número de errores cometidos. Si suponemos que $deg\, F \geq t + g$, entonces $\ell(F) \geq t + 1$ y, en consecuencia, existe al menos una función localizadora de errores no nula sea quien sea $\mathbf{e}$ de peso a lo más t.

Por otro lado, si $f \in \mathcal{L}(F)$ y $g \in \mathcal{L}(G - F)$, entonces $fg \in \mathcal{L}(G)$; por lo tanto, puesto que $C_L(D, G) \perp C_\Omega(D, G)$, se tiene

$$\sum y_i((fg)(P_i)) = \sum e_i((fg)(P_i))$$

Análogamente, si $f \in \mathcal{L}(F - D_\mathbf{e})$ y $g \in \mathcal{L}(G - F)$, entonces $fg \in \mathcal{L}(G - D_\mathbf{e})$; en consecuencia, se tiene

$$K(\mathbf{y}, F) \doteq \{f \in \mathcal{L}(F) \mid \sum y_i((fg)(P_i)) = 0, \ \ \forall g \in \mathcal{L}(G - F)\} \supseteq \mathcal{L}(F - D_\mathbf{e})$$

puesto que, al tener D y G soportes disjuntos, fg se anula en las posiciones de error si $fg \in \mathcal{L}(G - D_\mathbf{e})$. Nótese que el objeto de la izquierda (que llamaremos *núcleo asociado a* F *e* $\mathbf{y}$) es computable a partir de la palabra recibida $\mathbf{y}$, mientras que el de la derecha es el que queremos conocer; para ello daremos una condición suficiente que implique la igualdad entre ambos.

Supongamos además que $deg\,(G - F) > 2g - 2 + t$; en este caso, se tiene que $C_\Omega(D_\mathbf{e}, G - F) = 0$ al ser $\Omega(G - F - D_\mathbf{e}) = 0$. Por lo tanto, si $f \in K(\mathbf{y}, F)$ se verifica que

$$\sum y_i((fg)(P_i)) = \sum e_i((fg)(P_i)) = 0$$

para toda función $g \in \mathcal{L}(G - F)$; pero esto significa que $(e_1 f(P_1), \ldots, e_n f(P_n))$ es una palabra que está en el código dual de $C_L(D_\mathbf{e}, G - F)$, que acabamos de ver que era cero. En consecuencia, f se anula en las posiciones de error, y se tiene la igualdad $\mathcal{L}(F - D_\mathbf{e}) = K(\mathbf{y}, F)$.

Para que las dos hipótesis hechas sobre el grado de F sean compatibles, es necesario que el número de errores sea a lo más $\lfloor (d^* - g - 1)/2 \rfloor$. Sea

pues $t = \lfloor (d^* - g - 1)/2 \rfloor$ y sea F un divisor de grado $t + g$; suponiendo calculadas bases para los espacios $\mathcal{L}(F)$ y $\mathcal{L}(G)$, así como una matriz de control H para el código, estamos en condiciones de describir el siguiente algoritmo de decodificación, debido a *Skorobogatov y Vlăduţ*, y que se conoce como *algoritmo básico*.

Algoritmo 1.1 (Algoritmo $\mathcal{A}(F)$)

1. *Calcular el núcleo* $K(\mathbf{y}, F)$.

2. *Si* $K(\mathbf{y}, F) = 0$ *se cometieron demasiados errores; se devuelve el símbolo* ? *y se termina.*

3. *En caso contrario, elegir* $f \in K(\mathbf{y}, F)$ *no nula y calcular el conjunto* $J = \{i \mid f(P_i) = 0\}$.

4. *Resolver el sistema lineal*

$$\begin{cases} \mathbf{x}H = \mathbf{y}H \\ x_j = 0 \text{ si } j \notin J \end{cases}$$

5. *Si la solución del sistema anterior no es única, se cometieron demasiados errores y se procede como en el paso* **2.**

6. *En caso contrario, dicha solución es el vector error, siempre que* $wt(\mathbf{e}) \leq \lfloor (d^* - 1)/2 \rfloor$ *y que* $\mathbf{y} - \mathbf{e} \in C$.

Las hipótesis sobre el grado de F implican también que toda función no nula de $K(\mathbf{y}, F)$ tiene a lo más $d^* - 1 \leq d - 1$ ceros. En consecuencia, el *algoritmo básico* corrige hasta $\left\lfloor \dfrac{d^* - 1 - g}{2} \right\rfloor$ errores con un orden de complejidad $\mathcal{O}(n^3)$.

Existen varios métodos para mejorar el número de errores que se pueden corregir con el algoritmo anterior:

a) Pueden elegirse convenientemente sucesiones de divisores $(F_1, \ldots, F_s)$ de forma que, al ir aplicando sucesivamente el algoritmo básico con cada uno de estos divisores, se consigue finalmente que uno de ellos decodifique correctamente; el número de errores corregibles aumenta ligeramente (entorno a $g/4$) mientras que el orden de complejidad no varía (ver [102] y [31]).

b) Pellikaan demostró la existencia de s-uplas de divisores $(F_1, \ldots, F_s)$ tales que, al aplicar en paralelo el algoritmo básico con todos ellos a la vez, al menos uno de ellos decodifica correctamente (ver [83]); este método decodifica hasta la mitad de la distancia de Goppa pero la existencia y construcción de tales s-uplas es un difícil problema de geometría algebraica sobre *jacobianas* de curvas, y además la complejidad es del orden de $\mathcal{O}(n^4)$.

1.3.3 Ecuación clave y decodificación

A continuación expondremos un método de decodificación alternativo que, en cierto sentido, es equivalente al algoritmo básico estudiado en el apartado anterior; este método se basa en la idea de resolver una *ecuación clave* análoga al caso de códigos clásicos de Goppa, la cual se resolvía mediante el algoritmo de Euclides en el anillo de polinomios en una variable. Para ello, supondremos en adelante que existe un punto racional P en la curva además de los utilizados en el divisor D para definir el correspondiente código geométrico.

En primer lugar, se considera el **anillo afín** de la curva χ con respecto al punto P como el conjunto $K_\infty(P)$ de funciones racionales sobre χ que pueden tener polos únicamente en el punto P. En este anillo, puede definirse una función *grado*

$$\rho(f) \doteq -\upsilon_P(f)$$

que representa el orden del polo de f en P, y que tiene las propiedades de una *función peso*, es decir:

(0) $\rho(f) = -\infty$ si y sólo si $f = 0$.

(1) $\rho(\lambda f) = \rho(f)$ para todo $\lambda \in \mathbb{F}_q \setminus \{0\}$.

(2) $\rho(f+g) \leq máx\,\{\rho(f), \rho(g)\}$, y se da la igualdad si $\rho(f) < \rho(g)$.

(3) Si $h \neq 0$ y $\rho(f) < \rho(g)$, entonces $\rho(fh) < \rho(gh)$ [1].

(4) Si $\rho(f) = \rho(g)$, entonces existe $\lambda \in \mathbb{F}_q \setminus \{0\}$ tal que $\rho(f - \lambda g) < \rho(f)$.

[1] En realidad, esta propiedad es consecuencia de la propiedad (5), y se incluye en la definición únicamente para establecer la diferencia entre una *función peso* y una *función orden*, que sólo verifica las propiedades (0) a (4).

(5) $\rho(fg) = \rho(f) + \rho(g)$.

En este método de decodificación, nos restringiremos al caso en que $G = (h)_0 - \mu P$, donde $h \in K_\infty(P)$ y $(h)_0$ denota el divisor de ceros de h [2]; para mayor simplicidad, supondremos además que existe una forma diferencial η tal que $(\eta) = (2g-2)P$ (aunque basta con imponer condiciones sobre los ceros y polos de dicha diferencial). En todo caso, se puede demostrar la existencia de diferenciales $\varepsilon_1, \ldots, \varepsilon_n \in \Omega(-D - \mu P)$ tales que $res_D(\varepsilon_1), \ldots, res_D(\varepsilon_n)$ es la base canónica de $\mathbb{F}_q^n$; en consecuencia, toda diferencial $\omega \in \Omega(G - D)$ se escribe en la forma

$$\omega = \sum_{i=1}^{n} res_{P_i}(\omega)\, \varepsilon_i$$

Para cada palabra recibida $\mathbf{y}$, se define la **función síndrome** $S(\mathbf{y})$ como aquel elemento de $K_\infty(P)$ que satisface

$$S(\mathbf{y})\eta = \sum_{i=1}^{n} y_i \frac{h(P_i) - h}{h(P_i)} \varepsilon_i$$

Esta función tiene la propiedad de que $\mathbf{y} \in C_\Omega(D, G)$ si y sólo si $S(\mathbf{y}) \equiv 0 \ (mod \ \ h)$. Se dice que un par (f, r) de funciones en el anillo afín $K_\infty(P)$ es una solución de la **ecuación clave**, si existe $q \in K_\infty(P)$ tal que

$$f\, S(\mathbf{y}) = r + qh$$

La solución se dice que es *válida* si además

$$\rho(r) - \rho(f) \leq 2g - 2 + \mu$$

Por último, una solución válida se dice *minimal* si $\rho(f)$ es minimal en el conjunto de soluciones válidas de la ecuación clave. Pues bien, si $t \doteq \dfrac{d^* - 1}{2} - s(P)$, donde $s(P)$ denota el *índice de Clifford* de P [3], y el número de errores

[2] Todo código $C_\Omega(D, mP)$ es isométrico a uno de este tipo, con lo que el método es aplicable a los códigos sobre un punto. Isométrico quiere decir que se corresponde por una isometría del espacio métrico $\mathbb{F}_q^n$. Nótese que códigos isométricos tienen iguales parámetros, y que de un algoritmo de decodificación para uno de ellos se puede deducir uno para el otro código a través de la isometría.

[3] El *índice de Clifford* de un punto racional P de la curva χ se define mediante la expresión $s(P) \doteq máx \left\{ \dfrac{k}{2} - \ell(kP) + 1 \mid 0 \leq k \leq 2g - 1 \right\}$.

cometidos es a lo más t, un resultado de *Porter, Shen y Pellikaan* (ver [88]) demuestra que existe al menos una solución válida de la ecuación clave, y cualquier solución válida minimal verifica

$$\frac{r}{f}\eta \in \Omega(-D-\mu P) \quad \text{y} \quad res_D\left(\frac{r}{f}\eta\right) = \mathbf{e}$$

En consecuencia, la decodificación queda reducida al cálculo de una solución válida minimal de la ecuación clave, lo cual puede realizarse mediante la llamada *sucesión subresultante*, que generaliza el algoritmo de Euclides en el caso de los códigos clásicos de Goppa (ver [100]).

Existe una *formulación más general* de la ecuación clave, debida a *Ehrhard*; esta generalización es equivalente al algoritmo básico de Skorobogatov y Vlăduţ, y será expuesta brevemente a continuación (ver [36]).

Elegimos un divisor G^* tal que $\ell(G^*) = 0$ y $G \geq G^*$; puesto que $\Omega(G-D) \subseteq \Omega(G^*-D)$, y puesto que res_D es inyectiva en $\Omega(G-D)$ y suprayectiva en $\Omega(G^*-D)$, existe un espacio vectorial de formas diferenciales $\Omega(G-D) \subseteq V \subseteq \Omega(G^*-D)$ tal que $res_D : V \to \mathbb{F}_q^n$ es un isomorfismo. Este espacio tiene dimensión n, y juega el mismo papel que el espacio generado por las diferenciales ε_i en el algoritmo de Porter.

Por otro lado, fijada una forma diferencial no nula arbitraria η y escribiendo $K = (\eta)$, podemos considerar el isomorfismo

$$\mathcal{L}(K-H) \to \Omega(H)$$

$$f \mapsto f\eta$$

para cualquier divisor racional H; la aplicación anterior es compatible con inclusiones y restricciones, con lo que las contenciones $\Omega(G-D) \subseteq V \subseteq \Omega(G^*-D)$ inducen las correspondientes $\mathcal{L}(K+D-G) \subseteq U \subseteq \mathcal{L}(K+D-G^*)$, donde la aplicación $f \mapsto res_D(f\eta)$ es un isomorfismo de U sobre $\mathbb{F}_q^n$. Denotemos por $\mathbf{y} \mapsto h_{\mathbf{y}}$ a la aplicación inversa, es decir, $h_{\mathbf{y}}$ es el único elemento de U tal que $res_D(h_{\mathbf{y}}\eta) = \mathbf{y}$.

Para un divisor arbitrario F, se llama ahora solución de la *ecuación clave* para la palabra recibida $\mathbf{y}$ (relativa a F), a toda terna $(f,q,r) \in (\mathcal{L}(F) \setminus \{0\}) \times \mathcal{L}(K+F+D-G) \times \mathcal{L}(K+F-G^*)$ tal que $f\,h_{\mathbf{y}} = q + r$.

Si $deg\,F = \left\lfloor \dfrac{d^*+g-1}{2} \right\rfloor$ y $wt(\mathbf{e}) \leq t \doteq \left\lfloor \dfrac{d^*-g-1}{2} \right\rfloor$, entonces existe al

menos una solución (f, q, r) de la ecuación clave, y cualquiera de ellas verifica que $\mathbf{e} = res_D\left(\frac{r}{f}\eta\right)$.

Por otro lado, para la palabra $\mathbf{y} \in \mathbb{F}_q^n$ se define la aplicación lineal

$$\begin{array}{rccc} \delta_{\mathbf{y}} & : & \mathcal{L}(F) & \rightarrow & \mathcal{L}(K+F+D-G^*) \\ & & f & \mapsto & f\, h_{\mathbf{y}} \end{array}$$

Es fácil ver que $\mathcal{L}(K+F+D-G) \cap \mathcal{L}(K+F-G^*) = \mathcal{L}(K+F-G) = 0$, y en consecuencia existe un espacio vectorial W tal que

$$\mathcal{L}(K+F+D-G^*) = \mathcal{L}(K+F+D-G) \oplus \mathcal{L}(K+F-G^*) \oplus W$$

Si denotamos por π_W y π^* las proyecciones naturales sobre W y $\Omega(H-F)$ respectivamente, observamos que hallar una solución de la ecuación clave equivale a buscar una función f tal que $\delta_{\mathbf{y}}(f)$ tiene una proyección nula sobre W. Por lo tanto, calculadas bases para los espacios de diferenciales anteriores, decodificar $\mathbf{y}$ mediante este método consiste simplemente en efectuar operaciones de álgebra lineal, y su complejidad es de orden $\mathcal{O}(n^3)$. Exponemos a continuación con más detalle el algoritmo que calcula el vector error.

Algoritmo 1.2 (Algoritmo $\mathcal{K}_G(F)$)

1. *Calcular una matriz de la aplicación lineal* $\delta_{\mathbf{y}}$.

2. *Si* $\ker(\pi_W \circ \delta_{\mathbf{y}}) = 0$ *se cometieron demasiados errores; se devuelve el símbolo ? y se termina.*

3. *En caso contrario, se toma una función no nula* f *en dicho núcleo.*

4. *Calcular* $\omega = \pi^*(\delta_{\mathbf{y}}(f))$.

5. *Se devuelve el valor* $\mathbf{e} = res_D\frac{\omega}{f}$ *como vector error, siempre que* $\mathbf{y}-\mathbf{e} \in C$ *y* $wt(\mathbf{e}) \leq \lfloor (d^* - g - 1)/2 \rfloor$.

Nótese que en la versión original, la idea esencial es encontrar funciones (f, r) tales que r/f tenga el mínimo número posible de polos en el soporte de D y calcular el vector error como $res_D(r\eta/f)$. La idea fundamental de

Ehrhard es completamente similar, pero con la ventaja adicional de que no se necesitan hipótesis restrictivas sobre el tipo de códigos, ni tampoco hace falta considerar ninguna diferencial η ni ninguna función h especiales para poder definir una ecuación clave.

Ehrhard modificó este algoritmo para poder corregir hasta la mitad de la distancia de Goppa; dicha modificación consiste en, a partir de una palabra recibida, construir una sucesión F_i de divisores de forma que, aplicando el algoritmo $\mathcal{K}_G(F)$ con el último de ellos, se decodifica correctamente si no se cometen demasiados errores (ver [38]). La única objeción es que se necesita una hipótesis restrictiva sobre el grado del divisor G ($deg\, G \geq 4g - 2\tau$, donde τ es la *gonalidad* de la curva [4]).

1.3.4 Decodificación por mayoría

En este apartado, estudiaremos uno de los métodos más actuales y más eficientes para decodificar hasta la mitad de la distancia de Goppa, y que incluso supera esta cota en determinados casos. Tanto este método, debido a *Feng y Rao*, como sus generalizaciones, se basan en un *test de mayoría* similar al que se efectuaba en códigos lineales en el método de mayoría lógica o reducción secuencial de códigos. Para ello, supondremos que existe en la curva un punto racional P_∞ distinto de $P_1, \ldots, P_n$ y denotaremos por $\{\rho_i \mid i \in \mathbb{N}\}$ el conjunto ordenado de sus *no-lagunas* [5]. Los códigos que queremos decodificar serán denotados o bien por $C(m) \doteq C_\Omega(D, mP_\infty)$ o bien por $C_r \doteq C(\rho_r)$, según se quiera.

Si fijamos un función racional g_i con un único polo en P_∞ de orden ρ_i, se tiene que $g_1, \ldots, g_r$ es una base de $\mathcal{L}(\rho_r P_\infty)$, y en consecuencia la matriz H_r de tamaño $r \times n$ cuyas filas son $\mathbf{h}_i \doteq ev_D(g_i)$ es una matriz de control del código C_r. Para un posible vector error $\mathbf{e}$, definimos los **síndromes unidimensionales** como $s_i(\mathbf{e}) \doteq \mathbf{h}\mathbf{e}^t$, y los **síndromes bidimensionales**

[4] Se define la *gonalidad* de la curva χ como el mínimo grado posible de un morfismo no constante de χ en la recta proyectiva $\mathbb{P}^1$, y se puede probar que coincide con el valor $\tau = mín\,\{deg\, A \mid A \text{ divisor}, \ \ell(A) \geq 2\}$.

[5] Se dice que un entero no negativo m es una *no-laguna de Weierstrass* en el punto P si o bien $m = 0$, o bien $m > 0$ y $\mathcal{L}(mP) \setminus \mathcal{L}((m-1)P) \neq \emptyset$, siendo una *laguna de Weierstrass* en P en caso contrario.

como

$$s_{ij}(\mathbf{e}) \doteq \sum_{k=1}^{n} e_k \, g_i(P_k) g_j(P_k)$$

Si $\mathbf{y}$ es una palabra recibida y el error respecto del código C_r es $\mathbf{e}$, se tiene que $g_i g_j \in \mathcal{L}(\rho_r P_\infty)$ siempre que $\rho_i + \rho_j \leq \rho_r$, y en consecuencia el síndrome $s_{ij} \equiv s_{ij}(\mathbf{e})$ es conocido a partir de $\mathbf{y}$, siendo desconocido en caso contrario.

Sea $\mathcal{N}_r \doteq \{(i,j) \in \mathbb{N}^2 \mid \rho_i + \rho_j = \rho_{r+1}\}$ y sea $n_r \doteq \sharp\mathcal{N}_r$; se define la *distancia de Feng y Rao* δ_r del código C_r como el entero

$$\delta_r \doteq \delta_{FR}(\rho_{r+1}) \doteq mín\,\{n_s \mid s \geq r\}$$

Se tiene que $\delta_r \geq d^* = \rho_r + 2 - 2g$, dándose la igualdad si $r > 3g - 2$ (ver [65] o [95]).

Las entradas de la matriz $S = (s_{ij})_{1 \leq i,j \leq r}$ con índices $(i,j) \in \mathcal{N}_r$ son los primeros síndromes desconocidos que nos encontramos. Una vez que hubiésemos calculado uno de ellos conoceríamos todos los demás $s_{i'j'}$ con $(i',j') \in \mathcal{N}_r$, puesto que las funciones que nos dan estos síndromes se encuentran en el espacio vectorial $\mathcal{L}(\rho_{r+1}P_\infty)/\mathcal{L}(\rho_r P_\infty)$, que tiene dimensión uno, con lo que dichas funciones se encuentran ligadas por combinaciones lineales conocidas de antemano y que son heredadas por los correspondientes síndromes.

Se considera la matriz

$$\mathcal{S}(i,j) \doteq (s_{i'j'})_{1 \leq i' \leq i, 1 \leq j' \leq j}$$

Si $(i,j) \in \mathcal{N}_r$, todas sus entradas son conocidas excepto s_{ij}; en este caso, se dice que (i,j) es un *candidato* respecto de C_r si las matrices $\mathcal{S}(i-1,j-1)$, $\mathcal{S}(i-1,j)$ y $\mathcal{S}(i,j-1)$ tienen igual rango, en cuyo caso sólo hay un posible valor $\overline{s_{ij}}$ (llamado *valor candidato*) para asignar a la posición (i,j) de manera que $\mathcal{S}(i-1,j-1)$ y $\mathcal{S}(i,j)$ tengan el mismo rango. Si dicho valor coincide con s_{ij} se dice que el candidato es *verdadero*, llamándose *falso* en caso contrario. Denotaremos por T el número de candidatos verdaderos y por F el de falsos.

Por otro lado, una entrada cualquiera (i,j) de S se dice que es una *discrepancia* si las matrices $\mathcal{S}(i-1,j-1)$, $\mathcal{S}(i-1,j)$ y $\mathcal{S}(i,j-1)$ tienen el mismo rango pero no así $\mathcal{S}(i-1,j-1)$ y $\mathcal{S}(i,j)$; es obvio que el número D de discrepancias es exactamente igual al rango de S. Más aún, es fácil ver que S puede escribirse como producto de tres matrices en la forma $S = H_r \cdot E \cdot H_r^t$, donde E es una matriz diagonal $n \times n$ con los valores del error como entradas

y H_r es la matriz de control de C_r descrita anteriormente, con lo que D es a lo más el número de errores cometidos.

Supongamos que el número de errores es como mucho $(n_r-1)/2$, y denotemos por K el número de discrepancias en la parte conocida de S (llamadas *discrepancias conocidas*). Puesto que un candidato es falso si y sólo si es una discrepancia, se tiene

$$K + F \leq D \leq wt(\mathbf{e})$$

Por otro lado, si (i, j) es una discrepancia conocida, entonces no hay ningún candidato en las posiciones (i, j') para $j' > j$ ni en las posiciones (i', j) para $i' > i$. De la misma manera, si $(i, j) \in \mathcal{N}_r$ no es un candidato, entonces hay al menos una discrepancia conocida en la misma fila o en la misma columna, con lo que el número NC de elementos en $\mathcal{N}_r$ que no son candidatos es a lo más $2K$. En consecuencia, se tiene

$$n_r = (T + F) + NC \leq (T + F) + 2K$$

y puesto que suponemos que $wt(\mathbf{e}) \leq (n_r - 1)/2$, combinando las anteriores desigualdades se concluye que

$$F < T$$

lo que da un *criterio mayoritario* para obtener los síndromes desconocidos en las posiciones de $\mathcal{N}_r$. De forma más precisa, para cada predicción $\overline{s_{ij}}$ realizada en cada candidato, podemos asignar valores a las demás posiciones de $\mathcal{N}_r$ a través de las relaciones lineales entre los síndromes, y $\overline{s_{ij}}$ es un candidato verdadero si produce una mayoría de coincidencias en el resto de las posiciones. Para poder continuar el razonamiento con $\mathcal{N}_{r+1}$ y así sucesivamente, necesitamos mantener la cota del número de errores para los sucesivos n_s con $s \geq r$, es decir, necesitamos que $wt(\mathbf{e}) \leq (\delta_r - 1)/2$. Esto basta para *decodificar hasta la mitad de la distancia de Feng y Rao*, pues calculando una cantidad suficiente de síndromes desconocidos se obtiene el vector error (en el caso más desfavorable, tras haber calculado los síndromes hasta el paso $r+g$ se obtiene una relación lineal de una columna de S en función de las anteriores, y esto nos proporciona una función localizadora de errores reescribiendo esta combinación lineal entre las correspondientes funciones g_i). En particular, se deduce que $d(C_r) \geq \delta_r$, si bien esta desigualdad puede demostrarse directamente por métodos elementales (ver [65]).

El cálculo de los síndromes desconocidos puede realizarse mediante generalizaciones del método de *eliminación Gaussiana* que se aplican a matrices

con entradas desconocidas que tengan una estructura semejante a la matriz de síndromes bidimensionales, lo que da al algoritmo que acabamos de describir una complejidad de orden $\mathcal{O}(n^3)$. Ahora bien, aprovechando que la matriz S tiene una estructura en bloques de Hankel, se puede sustituir la eliminación Gaussiana por el cálculo de relaciones de *recurrencia lineal* en varias variables, generalizando el algoritmo de Berlekamp-Massey, con lo cual se gana en rapidez; esta modificación del algoritmo se debe a ideas de *Sakata* (ver [94] y [95]) y tiene una complejidad de orden $\mathcal{O}(n^{3-\frac{2}{r+1}})$, donde r es aquí el número de variables utilizadas, es decir, la dimensión del espacio afín en donde, en la práctica, tenemos inmersa la curva. De hecho, el algoritmo de Sakata calcula no sólo una función localizadora de errores, sino una *base de Gröbner* del ideal de dichas funciones, lo cual abre una nueva vía teórica para abordar el problema de la decodificación (ver [92] o [93]).

El algoritmo de Feng y Rao puede generalizarse a códigos geométricos de Goppa arbitrarios mediante el test de mayoría de *Duursma*, que expondremos a continuación; el método corrige hasta la mitad de la distancia de Goppa y sólo exige como condición adicional que exista un punto racional P_∞ en la curva que no esté en el soporte de D (ver detalles en [32]).

Sea G_1 un divisor racional con soporte disjunto a $sop\,(D)$; sean $G_0 = G_1 - P_\infty$ y $G_2 = G_1 + P_\infty$. Para $i = 0, 1, 2$, sea $C_i = C_\Omega(D, G_i)$ y $d_i^* = deg\,(G_i) + 2 - 2g$; es obvio que $C_0 \supseteq C_1 \supseteq C_2$. Para la palabra recibida $\mathbf{y} \in \mathbb{F}_q^n$, se define el *síndrome unidimensional* $S_i(\mathbf{y})$, para $i = 0, 1, 2$, como la aplicación lineal

$$S_i(\mathbf{y}) \ : \ \mathcal{L}(G_i) \to \mathbb{F}_q$$

$$h \mapsto \sum_{j=1}^{n} y_j h(P_j)$$

Análogamente, fijado un divisor racional arbitrario F, se definen para $i = 0, 1, 2$ los *síndromes bidimensionales* $S_i(F)$ asociados al vector error $\mathbf{e}$ como la aplicación bilineal

$$S_i(F) \ : \ \mathcal{L}(F) \times \mathcal{L}(G_i - F) \to \mathbb{F}_q$$

$$(f, g) \mapsto S_i(\mathbf{e})(f \cdot g)$$

Definimos también los núcleos $K_i(F)$ como

$$K_i(F) \doteq \{f \in \mathcal{L}(F) \mid S_i(F)(f, g) = 0, \ \ \forall g \in \mathcal{L}(G_i - F)\}$$

Los espacios vectoriales $K_0(F)/K_1(F)$, $K_1(F+P_\infty)/K_2(F+P_\infty)$, $K_1(F+P_\infty)/K_0(F)$ y $K_2(F+P_\infty)/K_1(F)$ tienen a lo más dimensión uno sobre $\mathbb{F}_q$, lo cual nos lleva a considerar las siguientes condiciones:

(A1) $K_1(F+P_\infty) \neq K_0(F)$

(A2) $K_0(F) = K_1(F)$

(A3) $\mathcal{L}(G_1 - F) \neq \mathcal{L}(G_1 - F - P_\infty)$

(B1) $K_1(F+P_\infty) = K_2(F+P_\infty)$

(B2) $K_2(F+P_\infty) \neq K_1(F)$

Definimos $(A) \Leftrightarrow (A1) \wedge (A2) \wedge (A3)$ y $(B) \Leftrightarrow (B1) \wedge (B2)$. Suponiendo que (A) y (B) se verifican, tomando $f \in K_1(F+P_\infty)\backslash K_0(F)$ y $g \in \mathcal{L}(G_1-F)\backslash \mathcal{L}(G_1-F-P_\infty)$, se tiene $fg \in \mathcal{L}(G_2)\setminus\mathcal{L}(G_1)$, y como además $K_1(F+P_\infty) = K_2(F+P_\infty)$, entonces $S_2(\mathbf{e})(fg) = 0$.

Por otro lado, si $\mathbf{y} \in C_1 \setminus C_2$ e $\mathbf{y}_1 \in \mathbf{e} + C_1$, existe una única constante $\lambda \in \mathbb{F}_q$ tal que $\mathbf{y}_1 - \lambda\mathbf{y} \in \mathbf{e}+C_2$. Por lo tanto, si tomamos $h \in \mathcal{L}(G_2)$ se tiene que $\lambda S_2(\mathbf{y})(h) = S_2(\mathbf{y}_1)(h) - S_2(\mathbf{e})(h)$, donde $S_2(\mathbf{y})(h) \neq 0$ si $h \notin \mathcal{L}(G_1)$.

Uniendo ambas cosas, la función $h = fg$ nos permite cambiar una palabra $\mathbf{y}_1$ recibida tal que $S_1(\mathbf{y}_1) = S_1(\mathbf{e})$ por otra $\mathbf{y}_2$ tal que $S_2(\mathbf{y}_2) = S_2(\mathbf{e})$; si este procedimiento se itera, como en cada paso cambiamos un código por otro cada vez más pequeño, tras un número finito de pasos conseguimos determinar el vector error. El único problema es que la condición (B) no puede comprobarse a partir de la palabra recibida, pero esta condición se verifica la mayoría de las veces, según establece el siguiente resultado (ver [32]).

Teorema 1.3 (Teorema de decodificación) *Sea $C_0 \supseteq C_1 \supseteq C_2$ la extensión de códigos anterior; supongamos que el género de la curva es $g \geq 1$ y tomemos $t, r \geq 0$ tales que $2t + r + 1 \leq d_1^*$. Sea F_0 un divisor arbitrario de grado t, y definimos $F_i \doteq F_0 + iP_\infty$ para $i = 1, \ldots, 2g-1$. Para un vector error $\mathbf{e}$ con peso $wt(\mathbf{e}) \leq t$, se define*

$$I \doteq \{r, r+1, \ldots, 2g-2\}$$

$$T \doteq \{i \in I \mid F = F_i \ \ verifica \ \ (A) \wedge (B)\}$$
$$F \doteq \{i \in I \mid F = F_i \ \ verifica \ \ (A) \wedge \neg(B)\}$$

Entonces se verifica al menos una de las tres condiciones siguientes:

$$\mathcal{L}(G_1 - F_{2g-1} - D_{\mathbf{e}} - rP_\infty) \neq 0$$

$$\mathcal{L}(F_r - D_{\mathbf{e}}) \neq 0$$

$$\sharp T > \sharp F$$

Nótese que si $g = 0$ el algoritmo básico corrige hasta la mitad de la distancia de Goppa y no necesitamos ningún test de mayoría, y si $g > 0$ podemos aplicar de forma algorítmica el resultado anterior: dado el código $C = C_\Omega(D, G)$, consideraremos sucesivamente los divisores $G_1 = G + rP_\infty$, para $r = 0, 1, \ldots, g$. Tomando $t \doteq \left\lfloor \frac{d^* - 1}{2} \right\rfloor$, se verifica la condición $2t + r + 1 \leq d_1^*$ para todo divisor G_1 desde $r = 0$ hasta $r = g$. Sea F_0 un divisor de grado t y definimos $F_i \doteq F_0 + iP_\infty$ para $i = 1, \ldots, 2g - 1$.

La condición $\mathcal{L}(G_1 - F_{2g-1} - D_{\mathbf{e}} - rP_\infty) \neq 0$ junto con la cota del número de errores garantizan el poder aplicar el algoritmo básico, o equivalentemente el algoritmo de la *ecuación clave generalizada*, utilizando como divisores $G = G_1 - rP_\infty$ y $F = G_1 - F_{2g-1} - rP_\infty$; de la misma manera, la condición $\mathcal{L}(F_r - D_{\mathbf{e}}) \neq 0$ y la cota del número de errores dan el mismo resultado para $G = G_1$ y $F = F_r$. Por lo tanto, las dos primeras condiciones del teorema anterior nos permiten obtener directamente el vector error mediante algoritmos conocidos y, si éstas no se verifican, un test de mayoría nos permite *reducir el tamaño del código* y continuar el proceso. Además este proceso termina como mucho en $r = g$, pues la condición $\mathcal{L}(F_r - D_{\mathbf{e}}) \neq 0$ siempre se verifica en este caso. En consecuencia, el siguiente algoritmo decodifica C hasta la mitad de la distancia de Goppa, como se muestra en nuestro trabajo [41], y supone una *aportación original* al introducir el esquema de votación mayoritaria de Duursma en la ecuación clave de Ehrhard.

Algoritmo 1.3 (Algoritmo $\mathcal{D}_G(F_0)$)

Input: $\mathbf{y} \in \mathbb{F}_q^n$.

Se asigna $\mathbf{y}_1 = \mathbf{y}$.

Para r desde $r = 0$ hasta $r = g$:

$$G_0 = G + (r-1)P_\infty, \;\; G_1 = G + rP_\infty, \;\; G_2 = G + (r+1)P_\infty$$

- *Si $\mathcal{K}_{G_1 - rP_\infty}(G_1 - F_{2g-1} - rP_\infty)$ decodifica correctamente, se devuelve el valor $\mathbf{e}$ y se termina.*
- *En caso contrario, si $\mathcal{K}_{G_1}(F_r)$ decodifica correctamente, se devuelve el valor $\mathbf{e}$ y se termina.*
- *En caso contrario, se calcula $I_A \doteq \{i = r, r+1, \ldots, 2g-2 \mid F = F_i \;\; verifica \;\; (A)\}$, para $F = F_i$ con $i \in I_A$ se calcula el vector $\mathbf{y}_2$ de la manera anteriormente descrita, es decir:*
  - *Hallar $f \in K_1(F + P_\infty) \setminus K_0(F)$.*
  - *Hallar $g \in \mathcal{L}(G_1 - F) \setminus \mathcal{L}(G_1 - F - P_\infty)$.*
  - *Hallar $\mathbf{c} \in C_1 \setminus C_2$.*
  - *Sea $\lambda = S_2(\mathbf{y}_1)(fg)/S_2(\mathbf{c})(fg)$ y tomamos como resultado $\mathbf{y}_2 = \mathbf{y}_1 - \lambda\mathbf{c}$.*

  Finalizados estos cálculos (cada uno de los cuales se denomina "coset decoding" en el trabajo original de Duursma), nos quedamos con aquel valor de $\mathbf{y}_2$ que se repita más veces.

  Se asigna $\mathbf{y}_1 = \mathbf{y}_2$ y se pasa al siguiente r.

Output: ?

Nótese que, en caso de haberse cometido demasiados errores, podemos llegar al final sin haber obtenido el vector error, e incluso podemos no llegar hasta el final por falta de mayoría en alguno de los pasos. Además, la complejidad de este algoritmo es de orden $\mathcal{O}(n^3)$, puesto que la mayoría de las operaciones vienen de aplicar el algoritmo $\mathcal{K}_G(F)$ o de hallar una función en $K_1(F + P_\infty) \setminus K_0(F)$ resolviendo un sistema lineal (ver [32]). En consecuencia, como los códigos de tipo C_L y los de tipo C_Ω son esencialmente la misma cosa se tiene, a modo de conclusión del capítulo, el siguiente resultado (ver [41] para más detalles).

Teorema 1.4 *Si χ es una curva algebraica proyectiva lisa y absolutamente irreducible definida sobre el cuerpo finito $\mathbb{F}_q$ con al menos $n+1$ puntos racionales, entonces todo código álgebro-geométrico de longitud n sobre χ puede decodificarse de forma efectiva mediante una ecuación clave generalizada con la ayuda de un criterio mayoritario, siempre que el divisor G que define el código verifique la desigualdad $2g-2 < deg\, G < n$, donde g es el género de χ, y el algoritmo de decodificación tiene una complejidad de orden $\mathcal{O}(n^3)$.*

□

Ejemplo 1.1 *Sea χ la curva de Hermite sobre $\mathbb{F}_{16}$ dada por la ecuación $\mathrm{Y}^4\mathrm{Z} + \mathrm{YZ}^4 + \mathrm{X}^5 = 0$, la cual tiene 64 puntos racionales en la parte afín y sólo un punto en el infinito P_∞, también racional. Sea $D = P_1 + \ldots + P_{64}$, $G_1 = 23P_\infty$ y se define el código $C = C_\Omega(D, G_1)$, de tipo $[64, 46, \geq 13]$. Se considera la palabra recibida $\mathbf{y}_1 = (\alpha^{12}, \alpha^4, \alpha^7, \alpha^8, \alpha^9, \alpha^9, 0, \ldots, 0))$, donde $\alpha \in \mathbb{F}_{16}$ verifica $\alpha^4 + \alpha + 1 = 0$, y se toma el divisor $F_0 = 6P_\infty$ (más detalles [33] y [101]).*

Con las mismas notaciones que en el algoritmo 1.3 , para $r = 0$ se puede comprobar que las dos primeras condiciones del teorema de decodificación 1.3 no se satisfacen; por tanto la ecuación clave no decodifica esta configuración de 6 errores y es necesario efectuar un test mayoritario para disminuir el tamaño del código. En dicho test, se obtiene el conjunto $I_A = \{1, 2, 3, 5, 7, 8, 9\}$ y se aplica el método de "coset decoding" a los divisores $F = F_i$ para $i \in I_A$, es decir, elegida una palabra $\mathbf{c} \in C \setminus C_\Omega(D, G_1 + P_\infty)$ entonces:

- *Se halla $f \in K_1(F + P_\infty) \setminus K_0(F)$.*
- *Se halla $g \in \mathcal{L}(G_1 - F) \setminus \mathcal{L}(G_1 - F - P_\infty)$.*
- *Se halla $\mathbf{c} \in C_1 \setminus C_2$.*
- *Sea $\lambda = S_2(\mathbf{y}_1)(fg)/S_2(\mathbf{c})(fg)$ y se toma $\mathbf{y} = \mathbf{y}_1 - \lambda\mathbf{c}$ como resultado.*

Una vez hecho esto, se toma el resultado más repetido $\mathbf{y}$ obtenido entre los divisores correspondientes a I_A como solución del test mayoritario y se

repite el proceso hasta que la ecuación clave encuentre el vector error. Todos estos cálculos son elementales una vez que se hayan calculado bases para los espacios de funciones involucrados en el proceso.

Nota 1.1 *Las ideas existentes en el algoritmo básico pueden generalizarse a los* códigos lineales *mediante el concepto de* pares correctores*, y también pueden generalizarse las ideas de la decodificación por mayoría mediante el concepto de* matrices correctoras*, si bien el problema de la construcción efectiva de tales objetos no ha sido aún resuelto más que en casos muy particulares, como es el caso de ciertos códigos cíclicos (ver [34] y [82]).*

Por otra parte, señalemos que si bien es cierto que, en teoría, todo código lineal puede ser considerado, en cierto sentido, como un código álgebro-geométrico, la demostración de este hecho no se basa en una construcción efectiva (ver [85]), y no puede por tanto aplicarse en la decodificación de códigos lineales arbitrarios, que se mantiene aún como un problema abierto.

Chapter 2

Expresiones simbólicas de Hamburger-Noether y algoritmo de Brill-Noether

El objetivo principal de este capítulo es la revisión de las técnicas básicas que nos permiten trabajar con modelos planos singulares de curvas algebraicas. De forma más precisa, nos proponemos estudiar con detalle el proceso de desingularización de una curva plana y, a partir de ello, dar una solución efectiva al cálculo de bases para los espacios $\mathcal{L}(G)$ y $\Omega(G)$, mediante el algoritmo de Brill-Noether; de paso, analizaremos también el problema de dar parametrizaciones racionales para dichas curvas mediante el método de Hamburger-Noether. Todo ello es de enorme utilidad en la construcción efectiva y decodificación de códigos geométricos de Goppa arbitrarios. Aunque en el capítulo se revisan nociones y resultados clásicos, nuestra discusión presenta un punto de vista propio adaptado a nuestras necesidades, es decir, a su utilización en la teoría de códigos. En este sentido, aunque nuestro interés se centra en el estudio del caso de un cuerpo finito, todos los resultados de este capítulo son válidos para un cuerpo perfecto arbitrario, que denotaremos por $\mathbb{F}$.

2.1 Ramas racionales

En primer lugar, introduciremos de forma intrínseca el concepto de ramas racionales en un punto de una curva (singular) arbitraria, lo que nos permitirá simplificar conceptualmente la resolución de singularidades de una curva singular.

Sea χ una curva algebraica proyectiva definida sobre un cuerpo perfecto $\mathbb{F}$, y sea P un punto cerrado de χ. Consideremos una carta afín de dicha curva que contenga al punto P, y sea A el anillo afín de coordenadas de dicha carta. Por el *teorema de los ceros de Hilbert*, P puede ser considerado como un ideal primo no nulo del anillo A. Sea $\overline{A}$ la *normalización* de A; $\overline{A}$ es el anillo afín de coordenadas de la normalización $\tilde{\chi}$ de la curva χ, y $\tilde{\chi}$ es una curva algebraica proyectiva y lisa definida sobre $\mathbb{F}$, denotándose por $\mathbf{n} : \tilde{\chi} \to \chi$ el morfismo de normalización. Los elementos de $\mathbf{n}^{-1}(P) = \{\overline{P}_1, \ldots, \overline{P}_r\}$ se llaman *ramas racionales* de la curva en el punto P. Estos elementos $\overline{P}_i$ pueden verse también como los ideales primos (de hecho maximales) de $\overline{A}$ tales que $\overline{P}_i \cap A = P$. El concepto de rama racional puede darse también en términos del anillo local de la curva χ en el punto P, es decir, $R \doteq \mathcal{O}_{\chi,P} = A_P$; sea $k(P) \supseteq \mathbb{F}$ el cuerpo residual en P ($k(P) \doteq R/\mathfrak{m}$ donde $\mathfrak{m}$ es el único ideal maximal del anillo local R), y sea $\overline{R}$ la normalización de R. El anillo $\overline{R}$ es semilocal, luego tendrá un número finito de ideales maximales; sean $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ dichos maximales. Las extensiones de cuerpos $\overline{R}/\mathfrak{m}_j \supseteq k(P)$ son finitas, y las ramas racionales en P están en biyección con el conjunto de ideales maximales del anillo $\overline{R}$.

Existe una tercera interpretación intrínseca de las ramas racionales, basada en el isomorfismo $\overline{\widehat{R}} \cong \widehat{\overline{R}}$, donde la *complección* se realiza respecto del *radical de Jacobson*. Por un lado, existe una biyección entre los maximales de $\overline{R}$ y los maximales de $\widehat{\overline{R}}$, y por otro existe una biyección entre los primos minimales de $\widehat{R}$ y los primos minimales de $\overline{\widehat{R}}$; ahora bien, el anillo $\widehat{\overline{R}}$ tiene el mismo número de primos minimales que de maximales, luego lo mismo ocurrirá con $\overline{\widehat{R}}$ en virtud del isomorfismo citado. En conclusión, existe una biyección entre los ideales maximales de $\overline{R}$ y los ideales primos minimales de $\widehat{R}$, con lo que podemos reformular la noción de rama racional en los siguientes términos.

Definición 2.1 *Dado un punto cerrado P de la curva χ con anillo local R, se llama rama racional (de χ en P) sobre $\mathbb{F}$ a cualquiera de los dos objetos equivalentes siguientes:*

a) *Un ideal maximal de $\overline{R}$ (es decir, un punto cerrado de Spec($\overline{R}$)).*

b) *Un ideal primo minimal de $\widehat{R}$ (es decir, una componente irreducible de Spec($\widehat{R}$)).*

Sea $\mathfrak{p}$ un primo minimal de $\widehat{R}$, sea y $\mathfrak{m}$ su correspondiente maximal en $\overline{R}$; el cuerpo $\mathbb{F} \subseteq A \subseteq A_P = R$ es un cuerpo contenido en el anillo local R. Puesto que el cuerpo $\mathbb{F}$ es perfecto, aplicando el *lema de Hensel* existe una extensión finita K de $\mathbb{F}$ tal que $K \subseteq \widehat{A_P} = \widehat{R}$ es un cuerpo de coeficientes para la complección $\widehat{R}$. K está unívocamente determinado, ya que no es otra cosa que la clausura entera de $\mathbb{F}$ en $\widehat{R}$. Como $\widehat{R} \subseteq \overline{\widehat{R}} \cong \overline{\widehat{R}}$ y se tiene, por consiguiente, que $K \subseteq \widehat{R}/\mathfrak{p} \subseteq (\widehat{R/\mathfrak{p}}) = (\widehat{\overline{R}_{\mathfrak{m}}})$, nuevamente por el lema de Hensel se tiene una extensión finita K' de K que es un cuerpo de coeficientes para el anillo local $(\widehat{\overline{R}_{\mathfrak{m}}})$. También K' está unívocamente determinado como cuerpo contenido en $(\widehat{\overline{R}_{\mathfrak{m}}})$.

En consecuencia, para cualquier *parámetro uniformizante* $t \in \mathfrak{m} \setminus \mathfrak{m}^2$ se tienen morfismos naturales

$$\widehat{R} \to \widehat{R}/\mathfrak{p} \to K'[[t]] \cong (\widehat{\overline{R}_{\mathfrak{m}}})$$

Si consideramos ahora una inmersión de la curva χ en un espacio proyectivo de la dimensión apropiada, los morfismos anteriores nos permiten definir el concepto de parametrización racional, cosa que haremos con más detalle a continuación en el caso de curvas planas.

2.2 Resolución de singularidades de curvas

En este apartado nos dedicaremos al estudio de la desingularización de una curva singular para poder ver más adelante sus aplicaciones en los cálculos efectivos que se necesitan para manejar en forma práctica los códigos álgebro-geométricos. La idea esencial que se considera a continuación es que no hace falta tomar la clausura algebraica del cuerpo base para convertir todos los puntos cerrados singulares asociados al proceso de resolución en un conjunto de puntos racionales sobre cierta subextensión finita, explotar por separado cada uno de ellos y reagruparlos al final nuevamente en clases de conjugación, sino que puede explotarse de una sola vez cada punto cerrado del esquema

$Spec(A)$ (es decir, explotar uno de sus representantes de la clase de conjugación y guardar como dato el grado del punto cerrado), consiguiendo el mismo resultado pero con un proceso conceptualmente más simple.

2.2.1 Bosque y árboles de equisingularidad

Sea χ una curva algebraica proyectiva absolutamente irreducible definida sobre un cuerpo perfecto $\mathbb{F}$. La curva χ es posiblemente singular, pero en principio no ha de tener necesariamente una inmersión en el plano. Sea $\mathbb{F}(\chi)$ su cuerpo de funciones, que es además un álgebra sobre $\mathbb{F}$, y que coincide con el cuerpo de fracciones del anillo de coordenadas de cualquiera de sus cartas afines. Recordaremos en primer lugar el concepto de *morfismo birracional propio*, que será fundamental en lo que sigue.

Definición 2.2 *Un morfismo $\varphi : \chi \to \Upsilon$ entre dos curvas algebraicas se dice que es birracional si el morfismo natural inducido $\mathbb{F}(\Upsilon) \to \mathbb{F}(\chi)$ es un isomorfismo de $\mathbb{F}$-álgebras. Si además toda valoración con centro en Υ tiene un centro en χ, es decir, la aplicación natural inducida*

$$\{ramas\ racionales\ de\ \chi\} \to \{ramas\ racionales\ de\ \Upsilon\}$$

es suprayectiva, se dice que el morfismo birracional es propio.

Por otro lado, dada la curva χ, su normalización $\tilde{\chi}$ es la curva obtenida al normalizar las $\mathbb{F}$-álgebras afines A_U para todo abierto afín U de χ. Todo morfismo no constante de curvas $\varphi : \chi \to \Upsilon$ se extiende de forma natural a las normalizaciones $\tilde{\chi} \to \tilde{\Upsilon}$, y se tiene que φ es propio si y sólo si el morfismo inducido en las normalizaciones es suprayectivo. De hecho, φ es birracional y propio si y sólo si dicho morfismo es un isomorfismo entre las normalizaciones.

El morfismo de normalización $\mathbf{n} : \tilde{\chi} \to \chi$ es birracional y propio, con lo que $\tilde{\chi}$ es un modelo liso para la curva χ, es decir, una curva lisa birracionalmente equivalente a la dada; de hecho el único modelo liso salvo morfismo birregular. Se tiene así una biyección entre clases de curvas proyectivas salvo equivalencia birracional y clases de curvas lisas salvo equivalencia birregular. Nótese que la equivalencia birracional es equivalente a que las normalizaciones sean isomorfas, o bien que los cuerpos de funciones racionales sean isomorfos como $\mathbb{F}$-álgebras.

Otro punto de vista teórico de ver el modelo liso o desingularización de una curva dada χ es mediante la *superficie abstracta de Riemann-Zariski*. Para ello, dado un cuerpo de funciones racionales $\mathbb{F}(\chi)$ definido sobre un cuerpo perfecto $\mathbb{F}$ con grado de trascendencia sobre $\mathbb{F}$ igual a uno, se considera el conjunto $\mathbf{S}$ de subanillos de valoración de $\mathbb{F}(\chi)$ que contienen a $\mathbb{F}$; por ser uno el grado de trascendencia sobre $\mathbb{F}$ y estar $\mathbf{S}$ en biyección con los puntos del modelo liso $\tilde{\chi}$ cuyos anillos locales son dominios de Dedekind, los anillos de valoración considerados en $\mathbf{S}$ son de hecho anillos de valoración discreta. $\mathbf{S}$ es la llamada superficie abstracta de Riemann-Zariski a la que se puede dar una estructura de variedad algebraica mediante la topología cofinita, que la hace ser isomorfa a la normalización $\tilde{\chi}$. La biyección que da lugar a este isomorfismo consiste en asociar a cada rama racional de χ dada por el ideal maximal $\overline{\mathfrak{m}}$ de $\overline{R}$ el anillo de valoración $\overline{R}_{\overline{\mathfrak{m}}}$. Vemos a continuación cómo obtener explícitamente un modelo liso para χ de forma constructiva.

Definición 2.3 *Sea I_0 un haz de ideales sobre la curva χ_0; se llama explosión de I_0 a todo par (χ_1, π_1), donde χ_1 es una curva y $\pi_1 : \chi_1 \to \chi_0$ es un morfismo birracional propio tal que:*

(i) *$I_0\mathcal{O}_{\chi_1}$ es un haz de ideales localmente principal (es decir, inversible).*

(ii) *Si $\sigma : \Upsilon \to \chi_0$ es otro morfismo birracional propio cualquiera tal que $I_0\mathcal{O}_\Upsilon$ es localmente principal, entonces existe un único morfismo birracional propio $\psi : \Upsilon \to \chi_1$ tal que $\sigma = \pi_1 \circ \psi$.*

La explosión de un haz de ideales existe y está definida de forma única salvo χ_0-isomorfismo; además, conmuta con la localización y con la restricción a abiertos de $U \subseteq \chi_0$. Este concepto nos permite obtener de una manera alternativa la normalización de una curva χ (salvo χ-isomorfismo), mediante la explosión del ideal llamado *conductor de* χ, definido por:

$$\mathcal{C}_\chi(U) \doteq \{f \in \overline{\mathcal{O}_\chi(U)} \mid f\,\overline{\mathcal{O}_\chi(U)} \subseteq \mathcal{O}_\chi(U)\}$$

No obstante, es preferible en la práctica ir explotando paso por paso los ideales asociados a los puntos singulares de la curva χ hasta conseguir una curva no singular, pues estas explosiones son más manejables en cuanto a que pueden darse de forma explícita las ecuaciones locales de la curva obtenida en cada paso.

Con más precisión, sea $\chi_0 = \chi$ y sea S_0 el conjunto de todos los puntos cerrados de χ_0 que son singulares, es decir, aquellos puntos cerrados P tales que el anillo local $\mathcal{O}_{\chi,P}$ no sea regular; sea $I_0 = I(S_0)$, es decir, el haz de ideales que define S_0 como subvariedad cerrada de χ_0, esto es $I_0(U) = \{f \in \mathcal{O}_{\chi_0}(U) \mid f(P) = 0 \ \ \forall P \in S_0 \cap U\}$. Se considera entonces la explosión $\pi_1 : \chi_1 \to \chi_0$ de I_0 que, al ser S_0 un conjunto finito, se podría ver alternativamente como una sucesión de sucesivas explosiones de cada uno de los puntos de S_0, cada una de las cuales puede darse explícitamente mediante ecuaciones locales en caso de tener una inmersión de la curva en una variedad apropiada. En todo caso, esta explosión es un isomorfismo fuera del conjunto S_0 de puntos singulares.

Podemos ahora iterar el proceso, es decir, explotar en la curva χ_i el ideal $I_i = I(S_i)$ del conjunto finito S_i de puntos singulares de χ_i mediante un nuevo morfismo $\pi_{i+1} : \chi_{i+1} \to \chi_i$ y obtener así una nueva curva χ_{i+1}. Como en cada paso disminuye el *género aritmético* de la curva explotada y el *género geométrico* es un invariante birracional, resulta que tras un número finito de pasos se consigue la igualdad entre ambos géneros, con lo que la curva obtenida χ_N no tiene puntos singulares y el proceso termina. De hecho, el morfismo $\pi = \pi_1 \circ \ldots \circ \pi_N$ es la normalización de la curva plana χ de partida, salvo χ-isomorfismo.

En este proceso constructivo, se obtiene un objeto combinatorio que se denomina *bosque de equisingularidad*, también llamado *bosque de desingularización* o de *resolución*. Dicho bosque está compuesto por árboles, cada uno de los cuales está asociado a cada uno de los puntos singulares de la curva χ y se denomina *árbol de equisingularidad* del punto correspondiente. La descripción de dicho bosque, que denotaremos por $\mathcal{T}_\chi$, se realiza de la manera siguiente:

1) Los vértices del bosque se disponen en niveles, desde el nivel 0 hasta el nivel N; en el nivel i se sitúan tantos vértices q como puntos Q del conjunto $S_i' \subseteq \chi_i$, donde $S_0' = S_0$ y $S_i' = \pi_i^{-1}(S_{i-1})$ para $i \geq 1$. Es evidente que $S_i \subseteq S_i'$ para todo $i = 0, 1, \ldots, N$ y que $S_N = \emptyset$.

2) Dos vértices p y q del bosque correspondientes a los puntos P y Q se unen con una arista orientada de p a q si $P \in S_i$, $Q \in S_{i+1}'$ y $\pi_{i+1}(Q) = P$.

3) Sobre cada arista $\overline{pq}$ del bosque se coloca como peso el número $\rho_{pq} \doteq [k(Q) : k(P)]$, donde $k(P)$ y $k(Q)$ son los respectivos cuerpos residuales

de los anillos locales $\mathcal{O}_{\chi_i,P}$ y $\mathcal{O}_{\chi_{i+1},Q}$.

4) Si p es la raíz de algún árbol del bosque correspondiente al punto singular P de χ, entonces a p se le asigna un peso de entrada igual a $[k(P) : \mathbb{F}]$.

5) Sobre los restantes vértices del bosque pueden colocarse pesos de dos formas alternativas (equivalentes una vez conocidos los pesos sobre las aristas); en ambos casos, se colocará sobre un vértice p que se encuentre en uno de los árboles del bosque un peso en cada rama del árbol que pase por p, entendiéndose por rama del árbol a todo vértice del mismo del cual no salga ninguna arista, y diciendo que una tal rama q pasa por p si se puede llegar desde p hasta q ascendiendo por las aristas del árbol. Nótese que las ramas del árbol que pasan por p están en biyección con las ramas racionales sobre P en la curva correspondiente. Sea q una rama del árbol que pasa por el vértice p, y sean Q y P los puntos correspondientes; supongamos que $P \in \chi_i$. Las dos alternativas para dar un peso en q son las siguientes:

(I) Poner como peso la *multiplicidad* de la rama racional $\mathfrak{q}$ de χ_i en P correspondiente a la rama q del árbol que pasa por p (que corresponde a su vez a un punto $Q \in \tilde{\chi}$), es decir, la multiplicidad $e_{p,q}$ del anillo local noetheriano $\widehat{\mathcal{O}_{\chi_i,P}}/\mathfrak{q}$ de dimensión 1 (en este caso, $\mathfrak{q}$ denota el correspondiente ideal primo minimal del anillo $\widehat{\mathcal{O}_{\chi_i,P}}$).

(II) Poner como peso el *orden* en P de la rama $\mathfrak{q}$, es decir $m_{p,q} \doteq \mathit{mín}\,\{v_Q(f) \mid f \in \mathfrak{m}_{\chi_i,P}\}$, donde $\mathfrak{m}_{\chi_i,P}$ es el ideal maximal del anillo local $\mathcal{O}_{\chi_i,P}$ y v_Q denota la valoración normalizada (es decir, con grupo de valores $\mathbb{Z}$) correspondiente al punto Q considerado como punto de la normalización $\tilde{\chi}$. La equivalencia entre ambos pesos viene dada por la fórmula:

$$m_{p,q}\,[k(Q) : k(P)] = e_{p,q}$$

Nótese que el orden es, en realidad, la multiplicidad de cada una de las ramas geométricas conjugadas que están sobre el punto P, es decir, las ramas racionales de la curva considerándola definida sobre la clausura algebraica $\overline{\mathbb{F}}$ de $\mathbb{F}$. Además, existe una biyección entre las ramas racionales sobre P, las ramas de su árbol de equisingularidad que pasan por el correspondiente vértice

p, los puntos de χ_N que se proyectan sobre P mediante la correspondiente sucesión de explosiones, los correspondientes puntos de la normalización de χ, las valoraciones correspondientes a dichos puntos y los correspondientes anillos de valoración del cuerpo de fracciones de la curva que contienen al cuerpo base $\mathbb{F}$; esto nos permitirá identificar en todo momento estos conceptos, según nos interese.

2.2.2 Ramas y árboles geométricos

En el caso geométrico, se considera la curva definida sobre la clausura algebraica $\overline{\mathbb{F}}$ (o bien sobre una extensión algebraica suficientemente grande de $\mathbb{F}$ para que todos los puntos singulares de la curva χ y de sus explosiones χ_i sean racionales) y se repite exactamente el proceso anterior cambiando el cuerpo base, es decir, cambiando χ por la curva $\chi \otimes_{\mathbb{F}} \overline{\mathbb{F}}$; el bosque y los árboles obtenidos como resultado se denominan *bosque y árboles geométricos de equisingularidad*.

En este caso, los pesos sobre las aristas son siempre 1 y en consecuencia $m_{p,q} = e_{p,q}$. Además, el bosque geométrico se puede deducir del bosque racional, sin más que sustituir cada raíz de peso l por l raíces de peso 1 y, de forma sucesiva, cada arista de peso h por h aristas de peso 1, para luego copiar sobre cada uno de estos h vértices nuevos exactamente el mismo sub-árbol que teníamos sobre el correspondiente vértice del bosque racional y seguir el proceso hasta que todas las aristas tengan peso 1. En la etapa inicial, si el punto singular P de χ no es racional sobre $\mathbb{F}$, el primer paso consiste, de forma más precisa, en sustituir el árbol de raíz p por árboles idénticos al árbol de equisingularidad de P tantas veces como indique el peso de entrada $[k(P) : \mathbb{F}]$ en p. Así, se tiene en particular que las ramas racionales pueden verse también como clases de conjugación sobre $\mathbb{F}$ de las ramas geométricas.

Por ejemplo, si se considera en la curva sobre $\mathbb{F}_2$ dada por la ecuación

$$\mathrm{X}^2 + \mathrm{XY} + \mathrm{Y}^2 + \mathrm{Y}^3 = 0$$

el punto racional $P = (0, 0)$ con multiplicidad 2 y explotamos dicho punto, el resultado de la explosión es un punto cerrado liso Q de grado 2, correspondiendo a dos ramas geométricas Q_1 y Q_2 con tangentes $\mathrm{X} + \alpha\mathrm{Y}$ y $\mathrm{X} + \alpha^2\mathrm{Y}$, donde $\alpha \in \mathbb{F}_4$ es una raíz primitiva de la ecuación $\mathrm{T}^2 + \mathrm{T} + 1 = 0$. Los pesos que hay que poner son $e_{p,q} = 2$ (o bien $m_{p,q} = 1$) en el vértice p, y

$e_{q,q} = m_{q,q} = 1$ en el vértice q. Como además P es racional sobre $\mathbb{F}_2$, el peso de entrada en p es 1. Por tanto, el árbol racional de resolución en P consta de los puntos P (a nivel 1) y Q (a nivel 2) unidos por una arista de peso 2, junto con los pesos anteriormente citados sobre los vértices, mientras que el árbol geométrico consta del punto P (a nivel 1) junto con los puntos Q_1 y Q_2 (a nivel 2) unidos ambos a P mediante sendas aristas de peso 1, lo cual no da a simple vista ninguna relación entre los puntos Q_1 y Q_2 que, en realidad, son conjugados sobre el cuerpo base F_2. Además, es necesario considerar sobre el vértice p dos pesos (uno por cada rama q_i) en lugar de uno.

De los comentarios anteriores se deduce que el bosque racional es un invariante más preciso que el bosque geométrico, y está más adaptado a la estructura de χ sobre $\mathbb{F}$ con lo que, a nivel teórico, no es necesario en ningún momento extender el cuerpo de definición $\mathbb{F}$, tal y como se hace normalmente en la literatura, puesto que el objeto combinatorio considerado sería mucho más complejo que en el caso racional y la relación entre los correspondientes *árboles conjugados* no es clara a la vista del bosque geométrico.

Nota 2.1 *El bosque de equisingularidad se puede sustituir por un objeto combinatorio equivalente que consiste en un sólo árbol pesado. Para ello, basta con añadir al bosque un nuevo punto* 0*, que no corresponde geométricamente a ningún punto de la curva pero que guarda la información sobre el cuerpo base, y añadir aristas que unan* 0 *con cada raíz* p *de un árbol de* $\mathcal{T}_\chi$ *dando como peso a una tal arista el peso de entrada en* p*. El punto* 0 *es la raíz el árbol obtenido, y no lleva ningún peso de tipo 5) ni ningún peso de entrada. Dicho árbol puede llamarse "árbol aumentado" de equisingularidad de* χ*.*

El árbol geométrico aumentado de equisingularidad, es decir, el de la curva $\chi \otimes_{\mathbb{F}} \overline{\mathbb{F}}$*, puede obtenerse a partir del árbol aumentado racional de* χ *por el procedimiento descrito anteriormente, consistente en sustituir de forma sucesiva cada arista de peso* h *por* h *aristas de peso* 1*.*

2.3 Modelos planos singulares: ramas y parametrizaciones racionales

A partir de ahora consideraremos para la curva χ un modelo plano posiblemente singular, es decir, una curva plana birracionalmente equivalente a la

dada. Dichos modelos siempre existen, aplicando el *teorema del elemento primitivo* a su cuerpo de funciones racionales, al ser el cuerpo base $\mathbb{F}$ un cuerpo perfecto. Los cuerpos de funciones racionales de ambas curvas son isomorfos con lo que, con vistas a las aplicaciones en la teoría de códigos, da igual trabajar con el modelo no singular o con el modelo plano, según nos convenga.

Supondremos pues en adelante que χ es una curva plana definida sobre un cuerpo perfecto $\mathbb{F}$, y que hemos elegido convenientemente una carta afín que contenga a un punto cerrado P que queremos estudiar. Para dicha carta, sea $A = \mathbb{F}[\mathrm{X}, \mathrm{Y}]/(f(\mathrm{X}, \mathrm{Y}))$ el anillo afín de coordenadas, donde $f(\mathrm{X}, \mathrm{Y}) = 0$ es la correspondiente ecuación afín de la curva. El punto P puede ser considerado como un ideal primo no nulo del anillo A con lo que, usando la notación del apartado anterior, se tiene $k(P) \cong K \hookrightarrow \widehat{A_P}$. De hecho, en la práctica podrá escribirse $K = \mathbb{F}[\mathrm{Z}]/(Q(\mathrm{Z}))$ con $Q \in \mathbb{F}[\mathrm{Z}]$ irreducible, lo cual es interesante desde el punto de vista del cálculo efectivo.

De esta manera, todo polinomio en $\mathbb{F}[\mathrm{X}, \mathrm{Y}]$ puede verse de forma natural como un polinomio con coeficientes en K y, salvo una traslación en $K[\mathrm{X}, \mathrm{Y}]$, podemos suponer que el punto P es el origen de coordenadas. En definitiva, hemos cambiado el anillo A por

$$A \otimes_{\mathbb{F}} K \cong \frac{K[\mathrm{X}, \mathrm{Y}]}{(f(\mathrm{X}, \mathrm{Y}))}$$

donde podemos suponer que el punto cerrado P corresponde al ideal (X, Y). A partir de ahora, suponemos A definido sobre K y P es el origen de coordenadas.

Con la misma notación que en el apartado anterior, se tiene que $\widehat{R} \cong K[[\mathrm{X}, \mathrm{Y}]]/(f(\mathrm{X}, \mathrm{Y}))$, y en consecuencia un morfismo natural $K[[\mathrm{X}, \mathrm{Y}]] \to \widehat{R}$. Considerando el cuerpo K' introducido anteriormente, que puede escribirse como $K' = K[\mathrm{W}]/(H(\mathrm{W}))$ con $H \in K[\mathrm{W}]$ irreducible con vistas al cálculo efectivo, se deduce un morfismo $K[[\mathrm{X}, \mathrm{Y}]] \to K'[[t]]$ que satisface las propiedades de lo que se denomina *parametrización racional*, y que se expone de forma precisa en la siguiente definición.

Definición 2.4 *En las condiciones y notaciones anteriores, se llama parametrización racional de χ en el punto P relativa a las coordenadas* X, Y *a todo homomorfismo de K-álgebras*

$$r \ : \ K[[\mathrm{X}, \mathrm{Y}]] \to K_1[[t]]$$

continuo para las topologías (X,Y)*-ádica y* t*-ádica respectivamente, tal que* $Im(r) \nsubseteq K_1$ *y* $f \in ker(r)$*, donde* K_1 *es una extensión finita de* K *y* t *es una indeterminada. Es decir, equivale a dar series formales* $x(t), y(t) \in K_1[[t]]$ *con al menos una de ellas no idénticamente nula tales que* $f(x(t), y(t)) \equiv 0$*.*

A cada parametrización racional r le podemos asociar la rama racional dada por el ideal primo minimal $\mathfrak{p} = ker(\widehat{r})$, donde $\widehat{r} : \widehat{R} \to K_1[[t]]$ es el morfismo inducido por r. De esta manera, se dice que r es una parametrización racional de la rama $\mathfrak{p}$.

Se dice que otra parametrización racional $s : K[[\mathrm{X},\mathrm{Y}]] \to K_2[[u]]$ se deriva de r, y se escribe $s \succ r$, si existe una serie de potencias $t(u) \in K_2[[u]]$ de orden positivo y existe un morfismo de K-álgebras $\sigma : K_1[[t]] \to K_2[[u]]$ con $\sigma(t) = t(u)$, tales que $s = \sigma \circ r$. La relación $\succ$ es un preorden parcial, y se dice que dos parametrizaciones racionales r y s son equivalentes si $s \succ r$ y $r \succ s$. Se dice que la *parametrización* r es *primitiva* si es minimal (en relación al preorden parcial $\succ$) módulo equivalencia, y además la extensión de cuerpos $F|\mathbb{F}$ es también minimal (es decir, que $r(\mathrm{X})$ y $r(\mathrm{Y})$ no están simultáneamente en $F'[[t]]$ para algún cuerpo F' con $\mathbb{F} \subseteq F' \subset F$ y $F' \neq F$).

Pues bien, existe una última caracterización de las ramas racionales de una curva basada en un resultado que dice que existe una biyección entre clases de equivalencia de parametrizaciones racionales en P y las ramas racionales en P; este resultado implica en particular que existen parametrizaciones racionales, y se sigue de la definición 2.2 y de los comentarios anteriores y posteriores a dicha definición.

En consecuencia, podemos asignar a cada rama racional una parametrización primitiva dentro de la clase de equivalencia de parametrizaciones racionales que le corresponde, obteniendo lo que se llama un *conjunto estándar de parametrizaciones racionales*. Un problema interesante en la práctica es hallar tales conjuntos de parametrizaciones a partir de la ecuación de la curva; esto será abordado en la sección 2.7 mediante los llamados *desarrollos de Hamburger-Noether*.

Nota 2.2 *Los resultados de esta sección son válidos para modelos singulares no necesariamente planos sin más que sustituir las dos variables* X,Y *por tantas variables como indique la dimensión de inmersión local de la curva en cada punto* P*. Si* χ *es localmente plana (por ejemplo si* χ *está contenida en una superficie lisa), tomando dos parámetros locales en cada punto regular* P *el contenido de la sección permanece formalmente inalterado.*

2.4 Teoría de adjunción para curvas planas

En esta sección y en las que siguen dentro del presente capítulo nuestro interés se centra en el caso en que la curva χ es una curva plana, es decir, la consideraremos inmersa en el plano proyectivo sobre $\mathbb{F}$. Con más generalidad, consideraremos a χ inmersa en una superficie algebraica proyectiva y lisa $\mathcal{S}$ definida sobre $\mathbb{F}$, sin preocuparnos para nada de dónde puede estar $\mathcal{S}$ inmersa. Suponiendo $\chi \subset \mathcal{S}$, tenemos ecuaciones locales para cada punto de χ en relación al anillo local del la superficie $\mathcal{S}$ en dicho punto.

2.4.1 Divisor de adjunción para curvas planas

En primer lugar, consideramos nuevamente $\mathcal{C}_\chi$ el conductor de χ que, por definición, es un haz de ideales simultáneamente de χ y de $\tilde{\chi}$. Al ser $\mathcal{C}_\chi$ localmente principal en $\tilde{\chi}$ (por definición de explosión), el conductor puede ser considerado como un divisor en $\tilde{\chi}$; dicho divisor es efectivo, y se denomina *divisor de adjunción*. Mostremos ahora cómo calcular explícitamente el divisor de adjunción a partir del bosque de equisingularidad.

Sean $q_1, \ldots, q_l$ las ramas del bosque de resolución, y sean $Q_1, \ldots, Q_l$ los puntos correspondientes de la normalización; denotemos por $P_j = \pi(Q_j)$ (identificando $\tilde{\chi}$ con χ_N). Para cada Q_j se tiene una sucesión de puntos

$$P_j = P_{j,0}, P_{j,1}, \ldots, P_{j,n_j-1}, P_{j,n_j} = Q_j$$

donde $P_{j,k} \in \chi_k$ y $\pi_k(P_{j,k}) = P_{j,k-1}$ para $k > 0$. Entonces, el divisor de adjunción viene dado por la fórmula:

$$\mathcal{A} = \mathcal{A}_\chi = \sum_{j=1}^{l} \left(\sum_{k=0}^{n_j-1} m_{p_{j,k},q_j}(e_{p_{j,k}} - 1) \right) Q_j$$

donde e_p para un vértice p de $\mathcal{T}_\chi$ denota

$$e_p = \sum_{j=1}^{l} e_{p,q_j}$$

con el convenio de que $e_{p,q_j} = 0$ si la rama q_j no pasa por el vértice p. Alternativamente, se puede escribir el divisor de adjunción como

$$\mathcal{A} = \sum_{j=1}^{l} \left(\sum_{p \in \mathcal{T}_\chi} m_{p,q_j}(e_p - 1) \right) Q_j$$

puesto que $m_{p,q_j} = 0$ si la rama q_j no pasa por p, y $e_{q_j} = 1$. Por otra parte, el grado del divisor de adjunción es

$$deg\,\mathcal{A} = \sum_{j=1}^{l} \left(\sum_{p \in \mathcal{T}_\chi} m_{p,q_j}(e_p - 1) \right) deg\,Q_j = \sum_{p \in \mathcal{T}_\chi} \left(\sum_{j=1}^{l} m_{p,q_j} deg\,Q_j \right) (e_p - 1) =$$

$$= \sum_{p \in \mathcal{T}_\chi} \left(\sum_{j=1}^{l} e_{p,q_j} deg\,P \right) (e_p - 1) = \sum_{p \in \mathcal{T}_\chi} e_p(e_p - 1) deg\,P$$

puesto que $deg\,Q_j = deg\,P \cdot [k(Q_j) : k(P)]$ y $e_{p,q_j} = m_{p,q_j} \cdot [k(Q_j) : k(P)]$. Con el fin de simplificar la notación, para una rama q del bosque de resolución denotaremos en adelante por d_q la cantidad

$$d_Q \doteq d_q \doteq \sum_{p \in \mathcal{T}_\chi} m_{p,q}(e_p - 1)$$

Estas fórmulas reproducen exactamente las fórmulas del caso geométrico, sin más que sustituir las ramas racionales Q_j por las correspondientes sumas formales de ramas geométricas conjugadas, pero el resultado es menos preciso al olvidarnos de la estructura sobre $\mathbb{F}$ de los objetos involucrados en la misma.

En otras palabras, $\mathcal{A}$ es un divisor de $\tilde{\chi}$ racional sobre $\mathbb{F}$ y, por tanto, considerarlo de esta manera es más preciso que considerarlo como un divisor sobre $\overline{\mathbb{F}}$. Así, los coeficientes que aparecen en el divisor de adjunción pueden definirse sin necesidad de ampliar el cuerpo de definición $\mathbb{F}$. Por un lado, los $e_{p,q}$ pueden verse como la multiplicidad de cierto anillo local completo. Ahora bien, la multiplicidad de un anillo local se puede calcular a partir de la *función de Hilbert* de dicho anillo, y dicha multiplicidad es invariante por complección. Por otro lado, conocidos los $e_{p,q}$ y los cuerpos residuales $k(P), k(Q)$ se conocen teóricamente los órdenes $m_{p,q}$ utilizando el argumento del lema de Hensel en la sección 2.1 para calcular el grado de la extensión de los correspondientes cuerpos de coeficientes.

Recordemos por último la fórmula del género geométrico de una curva χ sumergida en una superficie $\mathcal{S}$ que, con la misma notación que antes, viene dado por

$$g = g(\chi) = p_a(\chi) - \sum_{p \in \mathcal{T}_\chi} \delta_p = p_a(\chi) - \sum_{p \in \mathcal{T}_\chi} \frac{e_p(e_p - 1)}{2} deg\,P = p_a(\chi) - \frac{1}{2} deg\,\mathcal{A}$$

donde el número $\delta_p \doteq dim_{\mathbb{F}}(\overline{\mathcal{O}}_{\chi,P}/\mathcal{O}_{\chi,P})$ es estrictamente positivo si y sólo si P es un punto singular de χ y $p_a(\chi) \doteq \dfrac{(K_{\mathcal{S}} + \chi) \cdot \chi}{2} + 1$ denota el género aritmético de la misma, siendo $K_{\mathcal{S}}$ un divisor canónico de la superficie $\mathcal{S}$ y denotando por " $\cdot$ " el número de intersección entre dos divisores.

En el caso particular de que la curva sea plana, es decir $\mathcal{S} = \mathbb{P}^2$, se tiene que $K_{\mathcal{S}} = -3L$, donde L es una sección hiperplana, y χ es equivalente a mL como divisor, siendo m el grado de la curva χ, con lo cual el género aritmético viene dado por la fórmula

$$p_a(\chi) = \frac{(m-3)\,m}{2} + 1 = \frac{(m-1)(m-2)}{2}$$

2.4.2 Divisores adjuntos de curvas planas

En las mismas condiciones que en el apartado anterior, fijado un punto cerrado P de χ, se tiene que P es también un punto cerrado de la superficie $\mathcal{S}$, y el cuerpo residual $k(P)$ no depende en realidad ni de χ ni de $\mathcal{S}$, según la teoría general de puntos cerrados sobre esquemas. Se consideran los dominios $R = \mathcal{O}_{\chi,P}$ y $\mathcal{O} = \mathcal{O}_{\mathcal{S},P}$, éste último regular de dimensión 2, y sean las sucesiones exactas de morfismos naturales

$$\mathcal{O} \to R \to 0$$

$$0 \to R \to \overline{R}$$

El núcleo del primer morfismo tiene altura 1, puesto que la imagen es de dimensión 1 y, por otra parte, el dominio $\mathcal{O}$ es factorial, al ser $\mathcal{O}$ de hecho regular; por lo tanto, dicho núcleo es un ideal primo principal de $\mathcal{O}$, aplicando el *teorema de Krull*, con lo cual se puede generar por un elemento de $\mathcal{O}_{\mathcal{S}}(U)$, donde U es un abierto afín de $\mathcal{S}$ que contiene al punto P. Nótese que $\mathcal{O} = \mathcal{O}_{\mathcal{S},P}$ es en realidad la localización de $\mathcal{O}_{\mathcal{S}}(U)$ en el ideal maximal que corresponde al punto P.

En el caso particular en que $\mathcal{S}$ sea una *superficie racional*, es decir, $\mathcal{S}$ birracionalmente equivalente al plano proyectivo $\mathbb{P}^2$ (o bien $\mathbb{F}(\mathcal{S}) \cong \mathbb{F}(\mathbb{P}^2)$), el elemento generador de dicho núcleo es de hecho un polinomio; esta propiedad es importante para el punto de vista computacional, con lo que en adelante supondremos que la curva χ está inmersa en una superficie racional $\mathcal{S}$ no singular.

Nótese que al explotar un punto cerrado de una superficie racional el resultado es nuevamente una superficie racional y, en particular, la explosión de un número finito de puntos cerrados del plano proyectivo $\mathbb{P}^2$ es una superficie racional. Recíprocamente, toda superficie racional (salvo isomorfismo) se obtiene a partir del plano proyectivo $\mathbb{P}^2$ explotando sucesivamente un número finito de puntos cerrados. En consecuencia, toda superficie racional $\mathcal{S}$ puede recubrirse por un número finito de abiertos afines que son isomorfos al plano afín sobre $\mathbb{F}$ (equivalentemente, tales que $\mathcal{O}_{\mathcal{S}}(U) = \mathbb{F}[\mathrm{X}, \mathrm{Y}]$), y recíprocamente.

En la situación anterior, consideramos nuevamente el ideal conductor

$$\mathcal{C}_P = \mathcal{C}_{\overline{R}/R} \doteq \{z \in \overline{R} \mid z\,\overline{R} \subseteq R\}$$

Por definición, $\mathcal{C}_P$ es simultáneamente un ideal de R y de $\overline{R}$, y es de hecho el máximo ideal con esta propiedad. Podemos por tanto hacer una doble interpretación de $\mathcal{C}_P$ de la manera siguiente:

(a) Como ideal de $\overline{R}$ no se considera para nada la inmersión en $\mathcal{S}$; teniendo en cuenta que $\overline{R}$ es un dominio de Dedekind con un número finito de ideales maximales $\overline{\mathfrak{m}}_Q$ (correspondiendo exactamente a las ramas racionales Q de χ en P), se tiene que el ideal conductor es un producto de ideales de la forma

$$\mathcal{C}_P = \prod_Q \overline{\mathfrak{m}}_Q^{\Delta_Q}$$

donde $div\,(\mathcal{C}_P) = \sum_Q \Delta_Q\, Q$ y Q recorre el conjunto de ramas racionales de χ en P. Se tiene que $\Delta_Q \in \mathbb{N}$ y además la longitud $\ell_{\overline{R}}(\overline{R}/\mathcal{C}_P) = \sum_Q \Delta_Q\, deg\, Q$, en virtud del *teorema chino de los restos*.

Por otro lado, al ser R plano se tiene que R es Gorenstein, con lo que se verifica la llamada *fórmula de Gorenstein*

$$\ell_{\overline{R}}(\overline{R}/\mathcal{C}_P) = 2\,\ell_R(R/\mathcal{C}_P)$$

En otras palabras, se tiene que $d_Q = 2\,\Delta_Q$ para todo Q.

(b) En cuanto ideal de R, existe otro ideal $\mathfrak{a}_P$ que contiene al núcleo del morfismo $\mathcal{O} \to R$ tal que $\mathfrak{a}_P$ se aplica sobre el conductor $\mathcal{C}_P$ por el morfismo anterior. Como R es noetheriano de dimensión 1 y $\mathcal{C}_P$ contiene

algún no divisor de cero, se deduce fácilmente que que el anillo

$$\frac{R}{\mathcal{C}_P} \cong \frac{\mathcal{O}}{\mathfrak{A}_P}$$

es artiniano, con lo que el ideal $\mathfrak{A}_P$ es primario para el ideal maximal $\mathfrak{m}(\mathcal{O})$ del anillo local $\mathcal{O}$. Por definición, se dice que el ideal $\mathfrak{A}_P$ es el ideal de las ecuaciones de los *gérmenes de adjuntas* en P sobre $\mathbb{F}$.

Se define globalmente el ideal de adjuntas $\mathfrak{A}$ como un haz de ideales de $\mathcal{O}_\mathcal{S}$ sobre la superficie $\mathcal{S}$ cuya fibra en P es el ideal $\mathfrak{A}_P$ si P es un punto de la curva χ, o bien es $\mathcal{O}_{\mathcal{S},P}$ si P es un punto de $\mathcal{S}$ que no está en la curva. De hecho, si $P \in \chi$ se tiene que $\mathfrak{A}_P = \mathcal{O}_{\mathcal{S},P}$ si y sólo si P es un punto no singular de χ, con lo que el haz de ideales $\mathfrak{A}$ está concentrado en el conjunto de puntos singulares de la curva χ, y por tanto tiene soporte finito. Así, dar $\mathfrak{A}$ es, en la práctica, equivalente a dar el número finito de datos $\mathfrak{A}_P$ para $P \in Sing\,(\chi)$.

A continuación daremos la definición de divisor adjunto sobre $\mathcal{S}$; dicha definición será de naturaleza local-global, pues en ella tanto χ como $\mathcal{S}$ podrán ser simultáneamente gérmenes de variedades o bien variedades (afines o proyectivas).

Definición 2.5 *Un divisor efectivo D sobre $\mathcal{S}$ se dice adjunto para la curva χ si para todo $P \in Sing\,(\chi)$ se tiene que la ecuación local de D en P está en el ideal $\mathfrak{A}_P$.*

Nótese que en el plano proyectivo $\mathbb{P}^2$ dar un divisor es equivalente a dar un ciclo de curvas $D = \sum n_i D_i$, donde n_i es un número entero y D_i es una curva plana irreducible (es decir, un *divisor de Weil*), y D es efectivo si $n_i \geq 0$ para todo i. En este caso, el hecho de que D sea adjunto significa que el polinomio homogéneo en tres variables $F = \prod F_i^{n_i}$ tiene un gérmen de adjunta en todo punto singular P de χ, donde F_i es el polinomio (unívocamente determinado salvo constante no nula en $\mathbb{F}$) que define la curva D_i.

Para una superficie arbitraria $\mathcal{S}$ podemos considerar *divisores de Cartier*, es decir, dar D equivale a dar un recubrimiento de $\mathcal{S}$ por abiertos de Zariski U no vacíos y dar para cada U un elemento $0 \neq f_U \in \mathcal{O}_\mathcal{S}(U)$ de forma que si $U \neq U'$ se tiene que $f_U = f_{U'}\, u_{U,U'}$ donde $u_{U,U'} \in \mathcal{O}_\mathcal{S}(U \cap U')^*$ es una unidad en el anillo de coordenadas del abierto intersección (que necesariamente es no vacío). Dos divisores de Cartier $\{(U, f_U)\}$ y $\{(V, g_V)\}$ se identifican si $f_U = g_V\, u_{U,V}$ para cualesquiera U y V, donde $u_{U,V} \in \mathcal{O}_\mathcal{S}(U \cap V)^*$.

En particular, si $\mathcal{S}$ es una superficie racional los abiertos U se pueden tomar siempre afines, es decir, $\mathcal{O}_{\mathcal{S}}(U)$ es un anillo de polinomios, con lo que dar D equivale a dar localmente un divisor de Weil. En realidad, si la superficie $\mathcal{S}$ es lisa, dar un divisor de Cartier equivale a dar un divisor de Weil, es decir, un ciclo de curvas $D = \sum n_i D_i$, donde n_i es un número entero y D_i es una curva irreducible inmersa en $\mathcal{S}$.

Por otro lado, cada divisor efectivo se encuentra en una clase de equivalencia lineal de divisores efectivos, cada una de las cuales se denomina *sistema lineal completo*. Por ejemplo, para el plano proyectivo $\mathbb{P}^2$ existe un sistema lineal completo $|O_{\mathbb{P}^2}(n)|$ para cada número natural $n \geq 0$ cuyos elementos se corresponden con los del proyectivizado del espacio vectorial de polinomios homogéneos de grado n sobre $\mathbb{F}$ en tres variables.

Sobre una superficie $\mathcal{S}$ arbitraria, todo sistema lineal completo $|G|$ contiene un subsistema lineal formado por los adjuntos $\mathcal{A}_G$ para la curva χ en la clase de G, es decir, la condición de adjunción es una condición lineal (por ser $\mathfrak{a}$ un ideal). En el caso de $\mathcal{S} = \mathbb{P}^2$ se tiene el subespacio lineal $\mathcal{A}_n \subseteq |O_{\mathbb{P}^2}(n)|$ de los divisores adjuntos de grado n (donde $\mathcal{A}_n$ puede ser vacío si n no es suficientemente grande); se puede considerar $\mathcal{A}_n$ como el proyectivizado $\mathbb{P}(\mathcal{F}_n)$ del conjunto $\mathcal{F}_n$ de polinomios homogéneos de grado n sobre $\mathbb{F}$ en tres variables que cumplen la condición de adjunción para la curva plana χ.

2.5 Resolución sumergida

Sea χ una curva sumergida en una superficie racional no singular $\mathcal{S}$ que, en la práctica, será una curva proyectiva plana; veamos cómo obtener las condiciones de adjunción para χ en términos de explosiones de la superficie $\mathcal{S}$ en puntos singulares de la curva χ.

En general, si Υ es un esquema noetheriano y $\mathcal{J}$ es un haz coherente de ideales, se define la explosión de Υ con centro $\mathcal{J}$ como un par $(\tilde{\Upsilon}, \pi)$, donde $\tilde{\Upsilon}$ es un esquema noetheriano y $\pi : \tilde{\Upsilon} \to \Upsilon$ es un morfismo birracional y propio tal que $\pi^{-1}(\mathcal{J} \cdot \mathcal{O}_{\Upsilon})$ es un haz inversible sobre $\tilde{\Upsilon}$; la explosión así definida es un objeto unívocamente determinado salvo Υ-isomorfismo. Además, π es un isomorfismo fuera del subesquema cerrado definido por $\mathcal{J}$.

En particular, $\tilde{\Upsilon}$ es una variedad sobre $\mathbb{F}$ si Υ es también una variedad sobre $\mathbb{F}$, y si además Υ es una superficie racional se tiene que también $\tilde{\Upsilon}$ es

una superficie racional, que será la propiedad que utilicemos a continuación.

Análogamente al caso no sumergido, podemos explotar el ideal conductor de la curva χ en la superficie $\mathcal{S}$, obteniéndose como resultado una curva no singular sumergida en una nueva superficie racional, pero es más interesante desde el punto de vista computacional el ir explotando sucesivamente los puntos singulares de la curva χ hasta obtener el mismo resultado teórico pero con las correspondientes ecuaciones locales para la curva sumergida que se obtiene.

Sean pues $\chi_0 = \chi$, $\mathcal{S}_0 = \mathcal{S}$ y S_0 el conjunto de todos los puntos cerrados de χ_0 que sean singulares; sea $I_0 = I(S_0)$ el haz de ideales sobre $\mathcal{S}_0$ que define S_0 como subvariedad cerrada de $\mathcal{S}_0$. Se considera entonces la explosión $\pi_1 : \mathcal{S}_1 \to \mathcal{S}_0$ de la superficie $\mathcal{S}_0$ con centro I_0, y se definen los objetos siguientes:

(i) La *transformada total* $\tilde{\chi}_1$ de χ_0 en $\mathcal{S}_1$, que es el divisor $\pi_1^*(\chi_0)$.

(ii) La *transformada estricta* χ_1 de χ_0 en $\mathcal{S}_1$, que consiste en la clausura proyectiva de $\pi_1^{-1}(\chi_0 \setminus S_0))$ en $\mathcal{S}_1$.

(iii) El *divisor excepcional* E_1 de π_1, que consiste en el divisor $\pi_1^{-1}(S_0)$ con la estructura reducida.

(iv) El *divisor excepcional* E_1^* *relativo a* χ_0 dado por

$$E_1^* = \sum_{P \in S_0} e_P(\chi_0)\, E_P$$

donde $e_P(\chi_0)$ es la multiplicidad de P como punto de la curva χ_0 y el divisor reducido $E_P = \pi_1^{-1}(P)$ es isomorfo a una recta proyectiva sobre el cuerpo residual $k(P) \supseteq \mathbb{F}$.

La relación entre los objetos anteriores es que

$$\tilde{\chi}_1 = \chi_1 + E_1^*$$

De forma inductiva, podemos iterar el proceso para obtener explosiones $\pi_{i+1} : \mathcal{S}_{i+1} \to \mathcal{S}_i$ con centro $I_i = I(S_i)$ y los consiguientes objetos $\tilde{\chi}_{i+1}$, χ_{i+1}, E_{i+1} y E_{i+1}^* definidos de forma análoga. Puesto que las explosiones son compatibles con las inmersiones, tras un número finito de pasos obtendremos que la transformada estricta χ_N será lisa y el proceso de desingularización

se habrá terminado, siendo éste exactamente el mismo que el proceso que dimos anteriormente de forma intrínseca para la curva χ_0.

No obstante, en este caso podemos seguir explotando $\mathcal{S}_N$ en aquellos puntos S_N en donde la transformada estricta χ_N no sea transversal al divisor excepcional E_N, y así sucesivamente hasta conseguir una curva no singular χ_M $(M \geq N)$ isomorfa a χ_N que sólo tiene cortes normales con el divisor excepcional E_M dentro de $\mathcal{S}_M$ (ver Hartshorne [53]), en cuyo caso el resultado obtenido

$$\tilde{\pi} = \pi_1 \circ \cdots \circ \pi_M \ : \ (\mathcal{S}_M, \chi_M) \to (\mathcal{S}, \chi)$$

se denomina *resolución sumergida minimal* de χ en $\mathcal{S}$.

Asociado al proceso de resolución sumergida se tiene un bosque pesado $\mathcal{T}^*_\chi$ llamado *bosque pesado de resolución sumergida*, en el que algunos pesos se sustituyen por una relación binaria entre vértices, llamada *relación de proximidad*. La descripción de dicho bosque se realiza de la forma siguiente:

1) Los puntos o vértices de la configuración se disponen en $M+1$ niveles, del nivel 0 al nivel M, colocándose en el nivel i-ésimo tantos vértices q como puntos Q del conjunto $S'_i \subseteq \chi_i$, donde $S'_0 = S_0$ y $S'_i = \chi_i \cap \pi_i^{-1}(S_{i-1})$ para $0 \leq i \leq M$.

2) Dos puntos p y q de la configuración se unen mediante una arista orientada de p a q en condiciones análogas al caso del bosque intrínseco de resolución, y sobre dicha arista se coloca igualmente el peso ρ_{pq} que depende de las extensiones residuales. Asimismo se colocan los pesos de entrada en las raíces de cada árbol del bosque con el mismo criterio que en el caso no sumergido.

3) Se añaden por último unas líneas de trazos (que representan las *relaciones de proximidad*) uniendo cada par de puntos próximos no triviales cualesquiera en dicha configuración, donde se dice que q es próximo a p, y se denota $q \to p$, si el punto Q está en el transformado estricto del divisor excepcional que crea el punto P al ser explotado, siendo P y Q respectivamente los puntos en χ_M que corresponden a los vértices p y q de la configuración (en particular, la relación de proximidad se verifica trivialmente si Q está en el divisor excepcional que crea P al ser explotado, pero dicha relación está ya puesta de manifiesto mediante la arista que necesariamente une P con Q).

La relación fundamental entre los bosques $\mathcal{T}_\chi$ y $\mathcal{T}_\chi^*$ se obtiene a partir de la *fórmula de Noether*

$$e_p = \sum_{\substack{r \to p \\ r \in \mathcal{T}_\chi^*}} e_r$$

donde e_p es la multiplicidad de la transformada estricta de χ en el punto P correspondiente a p; a su vez, a los e_q que aparecen en la fórmula anterior se les puede aplicar la misma fórmula extendida a sus respectivos puntos próximos y así sucesivamente con lo que, conocidos los cuerpos residuales $k(P)$, se pueden calcular los pesos e_p contando el número de relaciones de proximidad que se encuentran en la subárbol que comienza en el vértice p, puesto que las multiplicidades terminan siendo iguales a 1 en los puntos maximales del bosque.

Los vértices del bosque $\mathcal{T}_\chi$ se identifican con los vértices de $\mathcal{T}_\chi^*$ en los cuales $e_p > 1$ más los primeros de multiplicidad 1 de cada una de las ramas. El peso $e_{p,q}$ de $\mathcal{T}_\chi$ en el punto p correspondiente a la rama dada por q se puede obtener también por recurrencia inversa a partir de las fórmulas de Noether

$$e_{p,q} = \sum_{r \to p} e_{r,q} \quad , \quad e_{q,q} = 1$$

donde se sobreentiende que $e_{r,q} = 0$ si r no es un punto de la rama definida por q.

En conclusión, el bosque $\mathcal{T}_\chi^*$ tiene a priori más información que el bosque $\mathcal{T}_\chi$, ya que éste se puede deducir del anterior. En realidad, se puede ver que la información que hay en ambos es equivalente, ya que también $\mathcal{T}_\chi^*$ se puede deducir a partir de $\mathcal{T}_\chi$.

El bosque $\mathcal{T}_\chi^*$, y el sub-bosque $\mathcal{T}_\chi$, se pueden entender también como objetos combinatorios asociados a la llamada *configuración de puntos infinitamente próximos* $\mathfrak{C}_\chi^*$, asociada a su vez a la inmersión de χ en $\mathcal{S}$. Dicha configuración es la colección de puntos $S_0' \cup S_1' \cup \ldots \cup S_M'$. La geometría de los puntos de $\mathfrak{C}_\chi^*$, una vez que se consideran las relaciones de proximidad $Q \to P$ entre ellos y los cuerpos residuales $k(P)$, permite ir calculando los objetos combinatorios $\mathcal{T}_\chi^*$ y $\mathcal{T}_\chi$, incluidos sus pesos. A $\mathfrak{C}_\chi^*$ se le puede llamar *configuración de resolución sumergida* de χ en $\mathcal{S}$. A la subconfiguración $\mathfrak{C}_\chi$ de $\mathfrak{C}_\chi^*$ de los puntos correspondientes a los vértices de $\mathcal{T}_\chi$ se le llamará *configuración de resolución* de χ en $\mathcal{S}$.

Con esta terminología, dados dos puntos P y Q de la configuración de resolución sumergida de χ en $\mathcal{S}$, se dice que Q es *infinitamente próximo a* P, y se denota $Q \geq P$ (o bien $q \geq p$ si se toman sus correspondientes vértices en el bosque $\mathcal{T}_\chi^*$), si se puede obtener Q mediante una sucesión finita de explosiones empezando por P. Equivalentemente, Q es infinitamente próximo a P si existe una sucesión finita de puntos de dicha configuración de la forma

$$P = P_0, P_1, \ldots, P_l = Q$$

tales que p_i es próximo a p_{i-1} para todo $1 \leq i \leq l$.

A continuación volvemos a la teoría de adjuntas, para caracterizar la condición de adjunción en términos de la configuración de resolución. Para ello, dados $P \in S_0$ y $h \in \mathcal{O}_{\mathcal{S},P}$ con $e_P(h) \geq e_p - 1$, se denota por $H = div(h)$ el divisor definido por h en la superficie $\mathcal{S}$, y se considera la imagen inversa $\pi_P^* H = div\,(\pi_P^* h) = (e_p - 1)\,E_P + \tilde{H}$, donde π_P denota la explosión con centro P. En estas condiciones, a $\tilde{H}$ se le llama *transformada virtual* de H (respecto de P y con peso e_p) y a la multiplicidad $\mu_q(h) \doteq e_q(\tilde{H})$ (donde q es próximo a p) se le llama *multiplicidad virtual* de h en q relativa a $e_p - 1$.

En general, si Q es infinitamente próximo a P se puede pasar de P a Q a través de una sucesión finita de explosiones, y haciendo las transformadas virtuales sucesivas respecto de los valores $e_r - 1$ se tendría análogamente el concepto de multiplicidad virtual del correspondiente vértice q. En cada paso, se toma la multiplicidad virtual $\mu_r(h)$ en el lugar que $e_p(h)$ toma en la primera etapa.

Con esta notación, se tiene que

$$\begin{aligned}\mathfrak{A}_P &= \{h \in \mathcal{O}_{\mathcal{S},P} \mid \mu_q(h) \geq e_q - 1 \ \ \forall q \geq p, \ \ q \in \mathcal{T}_\chi\} = \\ &= \{h \in \mathcal{O}_{\mathcal{S},P} \mid \mu_q(h) \geq e_q - 1 \ \ \forall q \geq p, \ \ q \in \mathcal{T}_\chi^*\}\end{aligned}$$

con lo cual la condición de adjunción puede comprobarse localmente a partir del morfismo de resolución de la curva χ como subvariedad de $\mathcal{S}$.

Nota 2.3 *Existen cuatro formas equivalentes de definir el concepto de divisor adjunto a χ dentro de la superficie $\mathcal{S}$. Sea D un divisor sobre la superficie $\mathcal{S}$ que sea racional sobre $\mathbb{F}$.*

Adjunta por ramas: *Se dice que D es una adjunta por ramas si en cada rama q de χ el divisor D tiene un contacto (es decir, multiplicidad de intersección) con la curva χ mayor o igual que el coeficiente d_q que aparece en el divisor de adjunción $\mathcal{A}_\chi$.*

Adjunta divisorial: *Se dice que D es una adjunta divisorial si D restringido a la normalización $\tilde{\chi}$ es mayor o igual que el divisor de adjunción. Por restricción de D a $\tilde{\chi}$ se entiende el divisor $\mathbf{N}^*D$, donde $\mathbf{N} : \tilde{\chi} \to \mathcal{S}$ es la composición de la normalización $\mathbf{n}$ con la inclusión i de χ en $\mathcal{S}$.*

Adjunta aritmética: *Se dice que D es una adjunta aritmética si en cada punto P de χ la ecuación local de D en P pertenece a la fibra $\mathfrak{A}_P$ del haz de gérmenes inducido por el conductor.*

Adjunta geométrica: *Se dice que D es una adjunta geométrica si en todo punto Q infinitamente próximo sobre la curva χ la multiplicidad virtual de D es estrictamente mayor que la multiplicidad efectiva de la transformada estricta de χ en dicho punto. Por puntos infinitamente próximos sobre χ se entiende puntos infinitamente próximos de puntos de la superficie $\mathcal{S}$ que están sobre la transformada estricta de χ. Nótese que en la definición de adjunta geométrica es suficiente considerar los puntos de la configuración de resolución $\mathfrak{C}_\chi$.*

2.6 Algoritmo de Brill-Noether

En la situación global, si el subsistema lineal $\mathcal{A}_G \subseteq |G|$ definido en el párrafo 2.4.2 es no vacío, su elemento general es una adjunta para χ, pero no necesariamente está ajustada a las multiplicidades virtuales que hemos definido en la sección anterior. Esto quiere decir que las multiplicidades verdaderas de las transformadas estrictas en los puntos del soporte de los divisores genéricos de $\mathcal{A}_G$ pueden diferir de las multiplicidades virtuales $e_q - 1$, debido a que en la transformada virtual va incluido el divisor excepcional que crea el punto P al ser explotado.

A continuación revisaremos una serie de resultados clásicos sobre adjuntas que nos permitirán calcular de forma algorítmica una base para el $\mathbb{F}$-espacio vectorial $\mathcal{L}(G)$, siendo G un divisor racional.

2.6.1 Teoremas de adjunción

Sea $\mathcal{S} = \mathbb{P}^2$ y sea χ una curva en $\mathcal{S}$, es decir, una curva plana. Se considera el morfismo natural

$$\mathbf{N} : \tilde{\chi} \to \mathbb{P}^2$$

donde $\mathbf{N} = i \circ \mathbf{n}$, siendo $\mathbf{n}$ la normalización de χ e i la inclusión de χ en el plano $\mathbb{P}^2$. Para cada divisor adjunto $D \in \mathcal{A}_n$ se considera su *pull-back* que viene dado por $\mathbf{N}^* D = \mathcal{A} + D'$ para cierto divisor efectivo D'. El siguiente resultado, debido a Noether, nos proporciona (en el caso de curvas planas) una propiedad fundamental de las adjuntas globales; ver Gorenstein [49] para más detalles.

Teorema 2.1 (Teorema de adjunción) *En las condiciones anteriores, si* $n+3 \geq deg\,\chi$ *se tiene que los divisores* D' *que se obtienen cuando* D *recorre* $\mathcal{A}_n$ *son exactamente los del sistema lineal completo* $|K_{\tilde{\chi}}+(n-m+3)\,L|$*, siendo* $K_{\tilde{\chi}}$ *un divisor canónico de* $\tilde{\chi}$*,* L *el divisor sección hiperplana y* $m = deg\,\chi$*.*

Es decir, los cortes de las adjuntas de grado $n \geq m-3$ con la curva χ, fuera del divisor de adjunción, dan los divisores sobre $\tilde{\chi}$ del sistema lineal completo $|K_{\tilde{\chi}}+(n-m+3)\,L|$. Esto significa que las condiciones de adjunción locales son linealmente independientes si se imponen a divisores de grado n suficientemente grande (aplicando la fórmula de Riemann-Roch), y además esta independencia lineal no es sólo local (sobre gérmenes de $\mathcal{O}_{\mathbb{P}^2,P}$) sino que es de hecho global, es decir, las condiciones de adjunción son linealmente independientes sobre todos los puntos P simultáneamente. En particular, si $n = m-3$ se tiene el siguiente resultado, que permite comprender la fórmula del género en el contexto de los problemas de condiciones asignadas, es decir, condiciones de pasar virtualmente por puntos de configuraciones.

Corolario 2.1 *Si* $n = m-3$ *entonces los* D' *antes descritos son exactamente los divisores canónicos efectivos de* $\tilde{\chi}$*. En particular, se tiene un* $\mathbb{F}$*-isomorfismo de sistemas lineales completos*

$$\mathcal{A}_n \to |K_{\tilde{\chi}}|$$

$$D \mapsto \mathbf{N}^* D - \mathcal{A}$$

Nótese que la aplicación anterior es inyectiva al ser $n < m$. La dimensión sobre $\mathbb{F}$ del espacio vectorial de formas de dimensión $m-3$ (en tres variables) es $\begin{pmatrix} m-1 \\ 2 \end{pmatrix} = \dfrac{(m-1)(m-2)}{2}$, es decir, el género aritmético $p_a(\chi)$. Además, el número total de condiciones que impone la adjunción y que son linealmente independientes sobre $\mathbb{F}$ es igual a $\dfrac{1}{2} deg\,\mathcal{A}$ (localmente serían

$dim_{\mathbb{F}}(\mathcal{O}_{\mathbb{P}^2,P}/\mathcal{C}_P) = \frac{1}{2} deg\, \mathcal{A}_P$ por la *propiedad de Gorenstein*). La fórmula del género geométrico $g(\chi) = p_a(\chi) - \frac{1}{2} deg\, \mathcal{A}$ se puede interpretar así como el problema de condiciones asignadas de pasar virtualmente por los puntos Q de la configuración $\mathfrak{C}_\chi$ con multiplicidades virtuales $e_Q - 1$, siendo estas condiciones linealmente independientes para los divisores de grado $m - 3$.

A continuación presentamos un teorema clásico, pero que enunciaremos en una *versión racional*, es decir, sin hacer ninguna referencia a la clausura algebraica del cuerpo base $\mathbb{F}$, y por tanto más en consonancia con el lenguaje que venimos utilizando a lo largo de todo este capítulo. Los detalles sobre su demostración pueden verse en Polemi [87].

Teorema 2.2 (Teorema del resto) *Sea χ una curva algebraica proyectiva plana y absolutamente irreducible definida por un polinomio homogéneo $F \in \mathbb{F}[X_0, X_1, X_2]$, y sea $\mathcal{A}$ su divisor de adjunción. Sean G y G' dos divisores sobre χ, racionales sobre $\mathbb{F}$, linealmente equivalentes y tales que G' es efectivo. Si $H \in \mathbb{F}[X_0, X_1, X_2]$ es un polinomio homogéneo tal que*

$$\mathbf{N}^* H = G + \mathcal{A} + R$$

para cierto divisor efectivo R, entonces existe un polinomio homogéneo $H' \in \mathbb{F}[X_0, X_1, X_2]$ con $deg\, H' = deg\, H$ tal que

$$\mathbf{N}^* H' = G' + \mathcal{A} + R$$

2.6.2 Cálculo de bases para $\mathcal{L}(G)$ y $\Omega(G)$

A continuación enunciamos un resultado que se demuestra fácilmente a partir del *teorema del resto*, y que es la base teórica un algoritmo que nos permite calcular una base del espacio $\mathcal{L}(G)$. El enunciado no es la versión geométrica original para un cuerpo algebraicamente cerrado, sino que está adaptado a la estructura de la curva χ sobre el cuerpo base $\mathbb{F}$, es decir, que se trata también de una versión racional, cuya demostración puede encontrarse en Polemi [87].

Teorema 2.3 (Brill-Noether) *Sea χ una curva proyectiva plana y absolutamente irreducible definida por un polinomio homogéneo $F \in \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2]$, sea $\mathcal{A}$ su divisor de adjunción y sea G un divisor sobre χ que sea racional sobre $\mathbb{F}$. Sea una forma $H_0 \in \mathcal{F}_n$, con $n \in \mathbb{N} \setminus \{0\}$, definida sobre $\mathbb{F}$, que no sea divisible por F y tal que*

$$\mathbf{N}^* H_0 \geq G + \mathcal{A}$$

Entonces se tiene que

$$\mathcal{L}(G) = \{\frac{h}{h_0} \ \mid \ H \in \mathcal{F}_n, \ \ H \notin F \cdot \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2] \ \text{ y } \ \mathbf{N}^* H + G \geq \mathbf{N}^* H_0\} \cup \{0\}$$

donde $h, h_0 \in \mathbb{F}(\chi)$ denotan respectivamente las funciones racionales H, H_0 restringidas a la curva χ, y $\mathcal{F}_n \subset \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2]$ denota el conjunto de formas de grado n en tres variables definidas sobre $\mathbb{F}$.

Como consecuencia de este resultado, el algoritmo siguiente calcula una base de $\mathcal{L}(G)$ sobre $\mathbb{F}$, para cualquier divisor racional G (ver Haché [50] para más detalles).

Algoritmo 2.1 (Algoritmo de Brill-Noether)

Dado G, se definen $J = G + \mathcal{A}$ y $J_+ = máx\,\{J, 0\}$.

(1) *Se elige $n \in \mathbb{N}$ suficientemente grande para que existan formas $H \in \mathcal{F}_n$ con coeficientes en $\mathbb{F}$, no divisibles por F tales que $\mathbf{N}^* H \geq J_+$. Por ejemplo, se puede tomar*

$$n > máx\left\{m - 1, \frac{m}{2} + \frac{deg\, J_+}{m} - \frac{3}{2}\right\}$$

donde $m = deg\, F$ es el grado de la curva χ, suponiendo éste distinto de cero (ver Haché [50]).

(2) *Calcular una base sobre $\mathbb{F}$ del espacio vectorial*

$$V = \{H \in \mathcal{F}_n \ : \ F|H \ \text{ o } \ \mathbf{N}^* H \geq J_+\} \cup \{0\}$$

(3) *Suponiendo $n \geq m$, calcular un conjunto de formas de $\mathcal{F}_n$ que den una base sobre $\mathbb{F}$ del espacio vectorial $V' = V/W$, donde $W = \{A \in \mathcal{F}_n : F|A\} \cup \{0\}$.*

(4) *Elegir un elemento $H_0 \in V \setminus W$ y calcular el divisor $\mathbf{N}^* H_0$.*

(5) *Calcular, utilizando la base obtenida en* **(3)**, *un conjunto de formas de $\mathcal{F}_n$ linealmente independientes sobre $\mathbb{F}$ que generen, módulo W, el espacio de formas H que verifican $\mathbf{N}^* H \geq \mathbf{N}^* H_0 - G$ (o bien $H = 0$), es decir, $\mathbf{N}^* H \geq \mathcal{A} + R$ donde $R \doteq \mathbf{N}^* H_0 - J$.*

(6) *Si $\{H_1, \ldots, H_s\}$ es la base obtenida en* **(5)** *y para $i = 0, 1, \ldots, s$ denotamos por $h_i \in \mathbb{F}(\chi)$ las funciones H_i restringidas a la curva χ, se tiene que*

$$\mathcal{B} = \left\{ \frac{h_1}{h_0}, \ldots, \frac{h_s}{h_0} \right\}$$

es una base del espacio $\mathcal{L}(G)$ sobre $\mathbb{F}$.

Dada la dualidad entre los espacios de funciones $\mathcal{L}(G)$ y los espacios de diferenciales $\Omega(G)$, pueden calcularse a partir del algoritmo anterior bases sobre $\mathbb{F}$ de los espacios $\Omega(G)$ para cualquier divisor racional G. Con más precisión, sea η una forma diferencial no nula arbitraria definida sobre $\mathbb{F}$ y sea $K = (\eta)$ el correspondiente divisor canónico, que es obviamente racional; entonces, para cualquier divisor racional G se tiene el $\mathbb{F}$-isomorfismo

$$\mathcal{L}(K - G) \to \Omega(G)$$

$$f \mapsto f\eta$$

En consecuencia, calculada una $\mathbb{F}$-base $\{f_1, \ldots, f_s\}$ del espacio $\mathcal{L}(K - G)$ se tiene que el conjunto

$$\{f_1\eta, \ldots, f_s\eta\}$$

es una base sobre $\mathbb{F}$ del espacio vectorial $\Omega(G)$. El único problema adicional podría ser el cálculo del divisor de una forma diferencial, pero esto se puede hacer en cada punto en términos de una expresión local en dicho punto (ver Fulton [45]).

2.7 Algoritmo de Hamburger-Noether

En esta sección nos dedicaremos al estudio algorítmico del proceso de resolución de singularidades, así como el cálculo formal de parametrizaciones racionales de ramas mediante el método de Hamburger-Noether, poniendo además de manifiesto la relación entre ambos procesos. Esta parte algorítmica es esencial para la aplicación práctica de las ideas expuestas a lo largo del presente capítulo, y en consecuencia para la construcción efectiva de los códigos de la *geometría algebraica*.

2.7.1 Desarrollos de Hamburger-Noether

Aunque la definición general puede darse en curvas sumergidas en un espacio de dimensión arbitraria (véase Campillo [16] o Campillo-Castellanos [17]), nos vamos a restringir al caso de curvas planas por razones de efectividad algorítmica; así pues, sea $\rho : \mathbb{F}[[\mathrm{X},\mathrm{Y}]] \to F[[u]]$ una parametrización racional sobre $\mathbb{F}$ de una curva plana χ definida en el punto P (en las condiciones de la sección 2.3), siendo F una extensión finita del cuerpo base $\mathbb{F}$. Denotemos abreviadamente por $\mathcal{O}$ el anillo local de χ en el punto P. Como hemos mostrado en la sección 2.3, $\mathcal{O}$ se puede ver como un subanillo de $\mathbb{F}[[u]]$, siendo los elementos imagen de X e Y un sistema minimal de generadores prefijado en el ideal maximal de $\mathcal{O}$.

Definición 2.6 *Llamaremos* **desarrollo de Hamburger-Noether** *de χ en P siguiendo la rama dada por ρ a una sucesión finita $\mathbb{D} = (Z_{-1}, Z_0, Z_1, \ldots, Z_r)$ de expresiones del tipo:*

$$Z_{-1} = a_{0,1}Z_0 + a_{0,2}Z_0^2 + \ldots + a_{0,h_0}Z_0^{h_0} + Z_0^{h_0}Z_1$$

$$Z_0 = a_{1,2}Z_1^2 + a_{1,3}Z_1^3 + \ldots + a_{1,h_1}Z_1^{h_1} + Z_1^{h_1}Z_2$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$Z_{r-2} = a_{r-1,2}Z_{r-1}^2 + a_{r-1,3}Z_{r-1}^3 + \ldots + a_{r-1,h_{r-1}}Z_{r-1}^{h_{r-1}} + Z_{r-1}^{h_{r-1}}Z_r$$

$$Z_{r-1} = \sum_{i\geq 1} a_{r,i}Z_r^i$$

donde r es un entero no negativo, $a_{j,i} \in F$, $a_{k,1} = 0$ si $k > 0$, h_j son enteros estrictamente positivos y además se verifica que

$$f(Z_0(Z_r), Z_{-1}(Z_r)) = 0 \quad \text{en} \quad F((Z_r))$$

siendo $f \in \mathbb{F}[[\mathrm{X},\mathrm{Y}]]$ *un generador del ideal* $\ker(\rho)$.

La existencia de tales desarrollos, así como el hecho de que siempre admiten un número finito de líneas (es decir, $r < \infty$) se puede deducir a partir de la parametrización ρ mediante un proceso algorítmico basado en divisiones sucesivas de series de potencias (ver Campillo-Castellanos [17] o Rybowicz [91]). De hecho, un desarrollo de Hamburger-Noether $\mathbb{D}$ es siempre una parametrización racional primitiva equivalente a ρ (considerando $\mathrm{X} \equiv \mathrm{Z}_0$ e $\mathrm{Y} \equiv \mathrm{Z}_{-1}$ como función del parámetro $s = Z_r$ mediante sustituciones sucesivas). Además, $\mathbb{D}$ depende únicamente de la rama dada por ρ y de la elección de parámetros x, y en $\mathcal{O}$ dada por las imágenes de X, Y a través de la aplicación ρ. Así, fijados X e Y, el conjunto (finito) de todos los posibles desarrollos de Hamburger-Noether no equivalentes constituye un conjunto estándar de parametrizaciones racionales de χ en P (ver [17]).

Nota 2.4 *El papel que juegan los desarrollos de Hamburger-Noether en característica arbitraria es exactamente el mismo que juegan clásicamente los llamados desarrollos de Puiseux en el caso del cuerpo de los números complejos (o de característica* 0*). El problema principal de los desarrollos de Puiseux es que, en general, no se puede garantizar su existencia si la característica no es nula. Un desarrollo de Puiseux es una parametrización de la forma*

$$X(t) = \alpha t^{\nu}$$
$$Y(t) = \sum_{i \geq \nu} \lambda_i t^i$$

donde $\alpha \in F^*$ *y* $\lambda_i \in F$*. Una tal parametrización existe si y sólo si el grado de separabilidad de la extensión* $L|\mathbb{F}((\mathrm{X}))$ *es primo con la característica de* $\mathbb{F}$*, donde* L *es el cuerpo de fracciones del anillo local* $\widehat{\mathcal{O}}$*, en cuyo caso también son parametrizaciones racionales. Para que además estas parametrizaciones racionales sean primitivas, no sólo es necesario que* ν *sea igual al orden de la rama racional a la que representa, sino que para ello hay que elegir muy adecuadamente los valores de* α *y* λ_i*, siendo éste un problema no trivial (ver [17] o [35]). Una segunda ventaja de los desarrollos de Hamburger-Noether es que dan directamente parametrizaciones racionales primitivas.*

A continuación mostraremos cómo calcular desarrollos de Hamburger-Noether sin necesidad de conocer a priori ninguna parametrización local de

la curva, sino utilizando nada más el polígono de Newton de la ecuación local de χ en el punto P. El método será expuesto para el caso en que la curva sólo tiene una rama en P; para el caso general, el método funciona de manera análoga siempre que la curva sea reducida, basándose en la idea de que el polígono de Newton se obtiene pegando los polígonos de Newton de cada una de las ramas de manera que la pendiente de los sucesivos segmentos sea creciente. Este algoritmo proporciona, en particular, el árbol de resolución asociado a P; nos remitiremos a Rybowicz [91] o Campillo-Castellanos [17] para más detalles.

Para ello, daremos en primer lugar el concepto de polígono de Newton, puesto que será la herramienta fundamental en el algoritmo que sigue. Supongamos que $\mathbb{F}$ es un cuerpo perfecto, y que la curva χ está dada, en coordenadas afines, por la ecuación $f(\mathrm{X},\mathrm{Y}) = \sum_{\alpha,\beta\geq 0} c_{\alpha\beta}\mathrm{X}^{\alpha}\mathrm{Y}^{\beta} = 0$, donde f es un polinomio irreducible en $\mathbb{F}[\mathrm{X},\mathrm{Y}]$; supongamos que el punto que queremos estudiar es el origen de coordenadas $P = (0,0)$, y supongamos que en dicho punto sólo existe una rama racional sobre $\mathbb{F}$. Se considera el diagrama de Newton de f

$$D(f) \doteq \{(\alpha,\beta) \mid c_{\alpha\beta} \neq 0\}$$

Denominaremos *polígono de Newton* de f (en el origen) al conjunto de los segmentos acotados de la frontera del cierre convexo de $D(f) + \mathbb{R}_{+}^{2}$, y será denotado por $P(f)$.

Excluyendo los casos triviales en los que la curva es uno de los ejes de coordenadas, sea l (respectivamente n) el mínimo entero tal que $(l,0) \in D(f)$ (respectivamente $(0,n) \in D(f)$); podemos obviamente suponer que $n \leq l$. En este caso, la irreducibilidad de f como serie de potencias sobre $\mathbb{F}$ en el origen implica, usando el lema de Hensel, que el polígono de Newton consta de un solo segmento (con pendiente no nula) de extremos $(l,0)$ y $(0,n)$.

En estas condiciones, sea $\Delta = P(f)$ el polígono de Newton y se define

$$L(\mathrm{X},\mathrm{Y}) \doteq \sum_{(\alpha,\beta)\in\Delta} c_{\alpha\beta}\mathrm{X}^{\alpha}\mathrm{Y}^{\beta}$$

Como consecuencia del lema de Hensel, se tiene que $L(\mathrm{X},\mathrm{Y}) = c\,D(\mathrm{X},\mathrm{Y})$ para cierto $c \in \mathbb{F}^{*}$ y cierto $D(\mathrm{X},\mathrm{Y})$ polinomio mónico en Y casi-homogéneo de cierto peso $l'n'$ y definido sobre $\mathbb{F}$. De forma más precisa, si $e = m\,c\,d\,(l,n)$ se tiene

$$D(\mathrm{X},\mathrm{Y}) = \prod_{j=1}^{d}(\mathrm{Y}^{n'} - \delta_j\mathrm{X}^{l'})^{e}$$

con $\delta_j \in \overline{\mathbb{F}}^*$, siendo entonces el llamado *polinomio característico* de Δ

$$\Phi_\Delta(\lambda) \doteq \prod_{j=1}^{d}(\lambda - \delta_j)$$

un polinomio irreducible sobre $\mathbb{F}$ (es decir, los δ_j son entre sí conjugados por el grupo de Galois sobre $\mathbb{F}$). Se tiene además que $l = l'ed$ y $n = n'ed$, siendo $m\,c\,d\,(l', n') = 1$.

Escribiendo $l = qn + h$ con $0 \leq h < n$, nos encontraremos en uno de los dos casos siguientes:

Caso 1: $h = 0$; esto implica $ed = n$, $l' = q$ y $n' = 1$. Escribiendo

$$a_{0,1} = \ldots = a_{0,l'-1} = 0, \quad \text{y} \quad a_{0,l'} = \delta$$

donde δ es una raíz simbólica [1] del polinomio característico $\Phi_\Delta(\lambda)$, obtenemos que la primera línea del desarrollo de Hamburger-Noether comienza por

$$Z_{-1} = a_{0,l'} Z_0^{l'} + \ldots$$

Entonces se efectúa sobre f la transformación

$$T_1(f, \delta, l') = f(\mathrm{X}, \mathrm{Y} + \delta\,\mathrm{X}^{l'}) = f_1(\mathrm{X}, \mathrm{Y})$$

tras la cual f_1 tiene como polígono de Newton un segmento de extremos $(l_1, 0)$ y $(0, n)$ con $l_1 > l$, y se repite el proceso, teniendo en cuenta que f_1 tiene coeficientes en el cuerpo $\mathbb{F}_1 = \mathbb{F}[\lambda]/(\Phi_\Delta(\lambda))$ y que es irreducible sobre dicho cuerpo.

Caso 2: $h > 0$; en este caso, la primera línea del desarrollo de Hamburger-Noether es exactamente

$$Z_{-1} = Z_0^q Z_1$$

Es fácil ver que el polinomio $U(f, l, n) = f(\mathrm{Y}, \mathrm{X}\,\mathrm{Y}^q)$ es divisible por Y^{nq}, con lo que aplicando a f la transformación

$$T(f, l, n) = \frac{f(\mathrm{Y}, \mathrm{X}\,\mathrm{Y}^q)}{\mathrm{Y}^{nq}} = f_1(\mathrm{X}, \mathrm{Y})$$

[1] Por una raíz simbólica de $\Phi_\Delta(\lambda)$ queremos decir que se sustituye $\mathbb{F}$ por el cuerpo $\mathbb{F}_1 = \mathbb{F}[\lambda]/(\Phi_\Delta(\lambda))$ y se toma como δ la clase residual de λ en dicho cuerpo.

el polígono de Newton Δ_1 obtenido tiene por extremos $(n,0)$ y $(0,h)$ con $h<n$, y su polinomio característico es $\Phi_{\Delta_1}(\lambda)=\lambda^e\,\Phi_\Delta(1/\lambda)$. Se repite entonces el proceso y pasaríamos a buscar la siguiente línea del desarrollo de Hamburger-Noether, efectuando en $T(f,l,n)$ la identificación $\mathrm{X}\equiv\mathrm{Z}_1$ e $\mathrm{Y}\equiv\mathrm{Z}_0$.

En caso de repetirse varias veces seguidas el caso $h=0$ en el cálculo de la $k+1$-ésima línea del desarrollo de Hamburger-Noether, donde $k\in\{0,1,\ldots,r-1\}$, se irían sumando los nuevos resultados obtenidos a la parte anterior de dicha línea, es decir, se obtendría un $l''>l'$ de forma análoga al l' definido en dicho caso, y se escribe

$$a_{k,l'+1}=\ldots=a_{k,l''-1}=0,\quad \text{y}\quad a_{k,l''}=\delta'$$

con δ una nueva raíz simbólica del correspondiente polinomio característico, obteniéndose entonces que dicha línea resulta ser

$$Z_{-1}=a_{0,l'}Z_0^{l'}+a_{0,l''}Z_0^{l''}+\ldots$$

y así sucesivamente hasta que caigamos en el caso $h>0$, en cuyo caso se añade el término $Z_0^qZ_1$ y se cambia de línea.

En consecuencia, aplicando un número finito de transformaciones de tipo T_1 o de tipo T, llegaremos al final a un polígono de Newton trivial (es decir, tal que $mín\,(l,n)=1$ y quizás sin ningún punto en el eje vertical), con lo que el algoritmo se terminaría y obtendríamos sucesivamente las líneas del desarrollo de Hamburger-Noether buscado.

Nótese que cuando el polígono de Newton es trivial la ecuación $f(\mathrm{X},\mathrm{Y})$ se ha convertido en una ecuación $g(\mathrm{Z}_r,\mathrm{Z}_{r-1})$ donde g está definido sobre un cuerpo $\mathbb{F}'$ obtenido por sucesivas extensiones simbólicas de $\mathbb{F}$ (es decir, añadiendo a $\mathbb{F}$ sucesivas raíces simbólicas) y se tiene que $\dfrac{\partial g}{\partial \mathrm{Z}_{r-1}}(0,0)\neq 0$. Esto significa que a partir del polinomio $g(\mathrm{Z}_r,\mathrm{Z}_{r-1})$ se puede obtener la última línea del desarrollo de Hamburger-Noether por medio del *teorema de la función implícita*. Dicha línea presenta a Z_{r-1} como serie de potencias en la variable Z_r [2]. En la práctica no es necesario calcular esta serie, ya que

[2]En particular, si la rama en la que estamos trabajando es no-singular, el desarrollo de Hamburger-Noether consta de una sola línea en la que se presenta $\mathrm{Z}_{-1}\equiv\mathrm{Y}$ como serie de potencias en la variable $\mathrm{Z}_0\equiv\mathrm{X}$, y dicha serie se obtiene a partir de la ecuación local de la curva, que coincide con el polinomio g.

su ecuación implícita g da la información necesaria para efectuar cualquier cálculo o algoritmo.

El producto final del algoritmo anterior es una parametrización racional *implícita* de la única rama racional en P, en el sentido de que está dada por un conjunto finito de expresiones de las cuales la última de ellas está dada en forma implícita, pero podremos trabajar con ellas perfectamente en el caso de que queramos comprobar con ellas, por ejemplo, la condición de adjunción local, puesto que esto no supone más que calcular el orden de una función en la rama y esto se puede realizar perfectamente con la información simbólica dada en el desarrollo de Hamburger-Noether de dicha rama mediante el método de derivación implícita formal (es decir, por coeficientes indeterminados).

Aparece, por tanto, una tercera ventaja de los desarrollos de Hamburger-Noether sobre los de Puiseux: el cálculo efectivo de tales desarrollos. Dicho cálculo se apoya simplemente en transformaciones sucesivas de tipo T_1 o de tipo T y en los *tres principios* siguientes:

(1) En la primera etapa se calculan los puntos cerrados del plano que son puntos singulares de χ. Esto se consigue resolviendo el sistema $f = f_{\mathrm{X}} = f_{\mathrm{Y}} = 0$ (por ejemplo mediante el método de triangulación del *álgebra computacional*) y escribiendo cada una de las las soluciones en una extensión simbólica inicial del cuerpo base $\mathbb{F}$.

(2) En las etapas del trabajo con el polígono de Newton, los sucesivos coeficientes de las líneas del desarrollo de Hamburger-Noether son raíces simbólicas de sucesivas extensiones simbólicas de $\mathbb{F}$ (extensiones que, frecuentemente, serán triviales).

(3) En la última etapa se obtiene el polinomio $g(\mathrm{Z}_r, \mathrm{Z}_{r-1})$ que resulta una información más completa y computacionalmente mejor que la última línea del desarrollo de Hamburger-Noether. Esta última línea, que es la única expresión que, en dicho desarrollo, constituye una serie posiblemente infinita, queda por tanto evitada en el proceso anterior, aunque sea en realidad la expresión introducida originalmente en los trabajos de Hamburger y Noether.

Los tres principios anteriores justifican cómo el método de cálculo del desarrollo de Hamburger-Noether es verdaderamente un algoritmo efectivo.

El principio (3) nos indica que, por razones de precisión, al resultado de sustituir la última línea en la definición de desarrollo de Hamburger-Noether por el polinomio g se le puede llamar (y así lo haremos en el resto del capítulo) *expresión simbólica de Hamburger-Noether*.

En el caso de varias ramas en P, el polígono de Newton constará de varios lados de distinta pendiente y bastará ir aplicando el algoritmo anterior a cada uno de los lados Δ con pendiente inferior a -1 y con anchura distinta de 1 (es decir, $mín\,(l,n) > 1$), eligiendo sucesivamente las raíces simbólicas δ de los sucesivos polinomios característicos $\Phi_\Delta(\lambda)$ y aplicando transformaciones similares al caso de una sola rama hasta que no se pueda seguir adelante con este procedimiento, es decir, hasta que no se pueda encontrar un nuevo Δ en las condiciones anteriormente dichas (es decir, Δ trivial). Nótese que $\Phi_\Delta(\lambda)$ no es necesariamente irreducible en este caso, y por tanto da lugar a varias raíces simbólicas correspondientes a sus factores irreducibles.

El método anterior funciona gracias al hecho de que el polinomio característico de un lado Δ es el producto de los polinomios característicos de todas las ramas en P con la misma pendiente que Δ, y se termina gracias a que, al ser f libre de cuadrados, las transformaciones efectuadas consiguen disminuir la anchura de los lados del polígono en un número finito de pasos (más detalles en [91]). Al final del algoritmo, no sólo se consigue desingularizar las ramas de χ en P, sino también separar unas de otras.

En consecuencia, existe un algoritmo efectivo para el cálculo de las expresiones simbólicas de Hamburger-Noether posibles para f en P (en particular, parametrizaciones racionales primitivas de las ramas de f en P) en términos de los tres principios anteriormente expuestos, donde al principio (2), en general, hay que añadir en cada etapa la descomposición efectiva del polinomio característico en sus factores irreducibles.

Por otro lado, las expresiones simbólicas de Hamburger-Noether se pueden considerar también como subproducto del algoritmo de resolución de singularidades (ver más detalles en Campillo-Castellanos [17]). De hecho, ambos procesos son equivalentes, y en el siguiente apartado haremos una descripción explícita de cómo obtener dicha resolución a partir del algoritmo de Hamburger-Noether anteriormente descrito. En particular, se obtendrán las configuraciones y bosques de resolución (sumergida o no) de la curva.

2.7.2 Cálculo de la desingularización de una curva plana y de su configuración de resolución

El algoritmo de cálculo de las expresiones simbólicas de Hamburger-Noether describe, en particular, la resolución de singularidades de la curva en cada uno de sus puntos singulares y constituye, en consecuencia, un camino alternativo (de hecho equivalente) al método clásico de explosiones sucesivas para encontrar de forma efectiva dicha resolución y los correspondientes objetos combinatorios asociados a la misma.

En efecto, siguiendo la notación del párrafo anterior, $f \in \mathbb{F}[\mathrm{X}, \mathrm{Y}]$ es una ecuación local de la curva en el punto P, ya supuesto racional sobre $\mathbb{F}$ (en caso contrario, se sustituye $\mathbb{F}$ por una extensión simbólica inicial $\mathbb{F}'$ de forma que P sea racional sobre dicha extensión) y de hecho $P = (0, 0)$ en relación a las coordenadas afines X, Y. Supongamos primero que f es irreducible como elemento de $\mathbb{F}[[\mathrm{X}, \mathrm{Y}]]$, es decir, que la curva tiene una única rama racional en P. Si escribimos $l = qn + h$ como en el párrafo anterior, entonces los primeros puntos infinitamente próximos $P = P_0, P_1, \ldots, P_{q-1}$ son racionales sobre $\mathbb{F}$ y, de hecho, se tiene que $P_i = (0, 0)$, para $0 \leq i \leq q - 1$, en relación a las coordenadas (afines) locales $\{\mathrm{X}, \dfrac{\mathrm{Y}}{\mathrm{X}^i}\}$ en P_i. Si $h = 0$, el punto P_q tiene cuerpo residual igual al cuerpo simbólico $\mathbb{F}_1 = \mathbb{F}[\lambda]/(\Phi_\Delta(\lambda))$, donde $\Phi_\Delta(\lambda)$ es el polinomio característico de Δ y $P_q = (0, 0)$ en relación a las coordenadas locales afines relativas a $\mathbb{F}_1$ dadas por $\{\mathrm{X}, \dfrac{\mathrm{Y}}{\mathrm{X}^q} - \delta\}$, donde δ es una raíz simbólica de $\Phi_\Delta(\lambda)$. Si $h > 0$ entonces las nuevas coordenadas serán $\{\mathrm{Z}_1, \mathrm{Z}_0\}$, el punto P_q es racional sobre $\mathbb{F}$ y éste está representado por $P_q = (0, 0)$ en dichas coordenadas, siendo ahora $\mathrm{Z}_1 = 0$ el divisor excepcional y no $\mathrm{Z}_0 = 0$ como venía siendo antes del cambio de línea. En todo caso, haciendo los sucesivos cambios de variables en cada uno de los puntos anteriormente considerados, se encuentran fácilmente las correspondientes transformadas total, estricta o virtual, según se necesite.

Iterando el proceso se encuentra la resolución de singularidades cuando se llega al polígono trivial, es decir, cuando las coordenadas lleguen a ser $\{\mathrm{Z}_r, \mathrm{Z}_{r-1}\}$ y la ecuación local sea $g(\mathrm{Z}_r, \mathrm{Z}_{r-1})$ con $\dfrac{\partial g}{\partial \mathrm{Z}_{r-1}}(0, 0) \neq 0$. La resolución sumergida, no obstante, continúa con tantas explosiones adicionales, que no alteran el cuerpo residual, como indica el número entero s tal que Z_r^s es el monomio de menor grado que aparece en el polinomio $g(\mathrm{Z}_r, \mathrm{Z}_{r-1})$,

puesto que $\mathrm{Z}_r = 0$ es ahora el divisor excepcional obtenido. Estas explosiones corresponden en el algoritmo a varias transformaciones de tipo T_1 en el caso particular $n = 1$.

En el caso de varias ramas racionales, la resolución se puede comprender a partir de lo anterior teniendo en cuenta que, en el algoritmo descrito en el párrafo anterior, cada vez que aparezca un polinomio característico no irreducible, resulta que su descomposición en factores irreducibles da lugar a tantos puntos infinitamente próximos en el divisor excepcional de la explosión correspondiente como factores en dicha descomposición. Las raíces simbólicas de dichos factores darán lugar a coordenadas locales afines convenientes para representar dichos puntos.

Para estudiar los bosques de resolución, hay que tener en cuenta que éstos se pueden estudiar rama a rama, así que podemos reducirnos nuevamente al caso de una sola rama racional. Nótese que los puntos $P_0, P_1, \ldots, P_q$ anteriormente descritos no tienen entre ellos relaciones de proximidad no triviales, ya que no están en la transformada estricta de las explosiones anteriores. Cuando se itera el proceso aparecen dichas relaciones de proximidad. Si $h = 0$ los puntos de la siguiente etapa siguen sin tener relaciones de proximidad entre ellos ni con los anteriores. Cuando se tiene la situación $h > 0$, entonces si $n = q'h + h'$ resulta que los $q' + 1$ puntos infinitamente próximos de la siguiente etapa son próximos del punto P de partida (ver Campillo [16] para más detalles). Por otro lado, las aristas $\overline{p_{i-1}p_i}$, donde p_j corresponde a P_j, tienen peso 1 si $i < q$ o si $i = q$ y $h > 0$, y peso d si $i = q$ y $h = 0$, en la notación del párrafo anterior. El valor $e \cdot n'$ que aparece en dicho párrafo es el *orden* que hay que poner como peso de la rama en los puntos $P_0, \ldots, P_{q-1}$ en el bosque $\mathcal{T}_\chi$, y el valor $n = d \cdot e \cdot n'$ es la *multiplicidad* que puede ponerse de forma alternativa como peso de la rama en dichos puntos. Los pesos de las ramas en P_q aparecen en la segunda etapa del algoritmo, en la cual P_q juega el papel de $P_0 = P$, y así sucesivamente.

En consecuencia, y tal como habíamos dicho en la introducción a este párrafo, el algoritmo de cálculo de las expresiones simbólicas de Hamburger-Noether tiene la información completa sobre las configuraciones de resolución y de resolución sumergida, así como sobre los bosques pesados de resolución correspondientes.

Ejemplo 2.1 *Sea χ la curva plana proyectiva sobre $\mathbb{F}_2$ dada por la ecuación*

$$F(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) = \mathrm{X}^{10} + \mathrm{Y}^8\mathrm{Z}^2 + \mathrm{X}^3\mathrm{Z}^7 + \mathrm{Y}\mathrm{Z}^9 = 0$$

con un único punto singular $P = (0 : 1 : 0)$ *que es racional sobre* $\mathbb{F}_2$ *, y además es el único punto de* χ *en el infinito. Sea una ecuación local*

$$f(\mathrm{X}, \mathrm{Z}) = \mathrm{X}^{10} + \mathrm{X}^3\mathrm{Z}^7 + \mathrm{Z}^9 + \mathrm{Z}^2$$

de χ *tal que* P *es el origen de coordenadas, y apliquemos el algoritmo de Hamburger-Noether a dicha ecuación.*

Según la notación dada en el apartado anterior, se tiene que $L(\mathrm{X}, \mathrm{Z}) = \mathrm{Z}^2 + \mathrm{X}^{10} = (\mathrm{Z} + \mathrm{X}^5)^2$ *; por lo tanto* $m = 10$*,* $m' = 5$*,* $n = e = 2$ *y* $n' = d = 1$*, con lo que* $q = 5$ *y estamos en el caso* $h = 0$*. El polinomio característico es* $\Phi(\lambda) = \lambda + 1$ *y la raíz simbólica es* $\delta = 1$*, es decir, no se necesita en este caso ampliar el cuerpo base* $\mathbb{F}_2$ *. En consecuencia, se tiene*

$$a_{0,0} = \ldots = a_{0,4} = 0 \qquad a_{0,5} = 1$$

y realizamos el cambio

$$f_1(\mathrm{X}, \mathrm{Z}) = f(\mathrm{X}, \mathrm{Z} + \mathrm{X}^5) = \mathrm{Z}^2 + \mathrm{X}^{38} + \ldots$$

siendo ahora $L(\mathrm{X}, \mathrm{Z}) = (\mathrm{Z} + \mathrm{X}^{19})^2$ *y por tanto* $m = 38$*,* $m' = 19$*,* $n = e = 2$*,* $n' = d = 1$*,* $q = 19$ *y otra vez* $h = 0$*, con lo que el polinomio característico es de nuevo* $\Phi(\lambda) = \lambda + 1$ *y la raíz simbólica es también* $\delta = 1$*. Así, se tiene*

$$a_{0,6} = \ldots = a_{0,18} = 0 \qquad a_{0,19} = 1$$

y se realiza la transformación

$$f_2(\mathrm{X}, \mathrm{Z}) = f_1(\mathrm{X}, \mathrm{Z} + \mathrm{X}^{19}) = \mathrm{Z}^2 + \mathrm{X}^{45} + \ldots$$

En este caso, se tiene $L(\mathrm{X}, \mathrm{Z}) = \mathrm{Z}^2 + \mathrm{X}^{45}$ *y obtenemos* $m = m' = 45$*,* $n = n' = 2$*,* $d = e = 1$ *y* $q = 22$*, con lo que caemos en el caso* $h = 1 > 0$ *y tenemos que cambiar de línea en el desarrollo de Hamburger-Noether sin necesidad tampoco de ampliar el cuerpo base. La transformación que tenemos que realizar ahora es*

$$f_3(\mathrm{X}, \mathrm{Z}) = \frac{f_2(\mathrm{Z}, \mathrm{X}\mathrm{Z}^{22})}{\mathrm{Z}^{44}} = \mathrm{Z} + \mathrm{X}^2 + \ldots$$

obteniendo entonces que el origen es un punto no singular de la nueva ecuación y el proceso se termina con $r = 1$*, con lo que las expresiones simbólicas*

de Hamburger-Noether en P son

$$\left\{\begin{array}{rcl} Z_{-1} & = & Z_0^5 + Z_0^{19} + Z_0^{22} Z_1 \\ g(Z_1, Z_0) & = & Z_1^9 Z_0^{154} + Z_1^8 Z_0^{151} + Z_1^8 Z_0^{137} + Z_1 Z_0^{130} + Z_0^{127} + Z_1^7 Z_0^{113} + \\ & + & Z_1^6 Z_0^{110} + Z_0^{113} + Z_1^5 Z_0^{107} + Z_1^4 Z_0^{104} + Z_1^3 Z_0^{101} + Z_1^6 Z_0^{96} + \\ & + & Z_1^2 Z_0^{98} + Z_1 Z_0^{95} + Z_1^4 Z_0^{90} + Z_0^{92} + Z_1^2 Z_0^{84} + Z_1^5 Z_0^{79} + \\ & + & Z_1^4 Z_0^{76} + Z_0^{78} + Z_1 Z_0^{67} + Z_1^4 Z_0^{62} + Z_0^{64} + Z_0^{50} + \\ & + & Z_1^3 Z_0^{45} + Z_1^2 Z_0^{42} + Z_1 Z_0^{39} + Z_0^{36} + Z_1^2 Z_0^{28} + Z_0^{22} + \\ & + & Z_1 Z_0^{18} + Z_0^{15} + Z_1 Z_0^{11} + Z_0^8 + Z_1^2 + Z_0 \end{array}\right.$$

En cuanto al árbol de resolución de χ en P, y según lo señalado en el presente párrafo, se obtiene una cadena de vértices

$$P \equiv p_0 - p_1 - \ldots - p_{21} - p_{22} \equiv q$$

correspondiendo a puntos racionales de multiplicidad $e_{p_i,q} = 2$ si $i = 0, \ldots, 21$, y $e_{p_{22},q} = 1$, siendo los pesos de todas las aristas iguales a 1, al igual que el peso de entrada. Para obtener la resolución sumergida y las relaciones de proximidad, habría que añadir dos explosiones más con el fin de que el divisor excepcional $\mathrm{Z}_1 = 0$ sea transversal a la transformada estricta de la curva χ, tal y como se ha dicho en el presente párrafo, es decir, añadir los vértices p_{23} y p_{24} de multiplicidad 1 y cuerpo residual $\mathbb{F}_2$, de forma que los puntos p_{22}, p_{23} y p_{24} son próximos al punto p_0 de partida. Como consecuencia, el divisor de adjunción es $\mathcal{A} = 44\,Q$ y, en particular, el género geométrico de la curva es $g = 14$.

2.8 Aplicaciones del algoritmo de Hamburger-Noether

En esta última sección del presente capítulo estudiaremos las principales aplicaciones del algoritmo descrito en la sección anterior para calcular las expresiones simbólicas de Hamburger-Noether en la construcción efectiva de los códigos álgebro-geométricos, como son el cálculo de bases para los espacios $\mathcal{L}(G)$, siendo G un divisor racional dado, y el cálculo del semigrupo de Weierstrass en P, siendo P un punto de χ racional sobre $\mathbb{F}$ dado.

2.8.1 Cálculo efectivo de bases de $\mathcal{L}(G)$ en términos de modelos planos

El teorema de Brill-Noether 2.3 reduce el cálculo de bases para el espacio $\mathcal{L}(G)$, donde G es un divisor racional sobre $\mathbb{F}$ definido sobre la curva normalizada $\tilde{\chi}$ de una curva plana χ, al problema de saber calcular bases para los espacios de ecuaciones de adjuntas de un grado n conveniente.

En la práctica, se conoce el polinomio $F(\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2) \in \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2]$ que define la curva absolutamente irreducible χ en el plano proyectivo y el dato es un divisor G de χ racional sobre $\mathbb{F}$, que vendrá especificado por una cantidad finita de ramas racionales concretas de χ (en puntos regulares o singulares) y unos coeficientes enteros concretos. El problema del cálculo de $\mathcal{L}(G)$ es, desde esta perspectiva, el problema computacional de generar una base de este espacio a partir de los datos anteriores. Daremos pues, a continuación, una solución a este problema computacional reuniendo los resultados de varios de los apartados de este capítulo.

En primer lugar, por el teorema 2.3 , se puede calcular un valor de n tal que existe y se puede encontrar explícitamente un adjunta concreta de grado n cuya ecuación H_0 satisface [3]

$$\mathbf{N}^* H_0 \geq \mathcal{A} + G$$

Ahora se calcula el resto $R = \mathbf{N}^* H_0 - \mathcal{A} - G$ y se ha de describir convenientemente el espacio de los polinomios H homogéneos de grado n tales que $\mathbf{N}^* H \geq \mathcal{A} + R$. Convenientemente quiere decir que se han de detectar elementos de dicho espacio que den una base módulo el espacio de múltiplos de F, según el teorema de Brill-Noether 2.3 .

Dicho teorema da una cota para el valor de n, pero el problema de calcular H_0 consiste en saber imponer a H_0 la condición de ser adjunta además de tener ceros extras sobre el divisor G. Por otro lado, para describir convenientemente $\mathcal{L}(G)$ una vez hallada la adjunta H_0, el problema básico es nuevamente saber imponer la condición de ser adjunta a un polinomio homogéneo de grado n además de tener ceros extras sobre el resto R.

Así, el problema computacional que nos ocupa se reduce al problema de determinar analíticamente las condiciones (que de hecho son lineales) que

[3] Estamos suponiendo que $G \geq 0$, pero en general se puede considerar el divisor J_+ en lugar de $J = \mathcal{A} + G$, según la notación empleada en el algoritmo 2.1 .

impone sobre un polinomio homogéneo de grado n la propiedad de que la curva que define sea una adjunta para χ. Para encontrar dichas ecuaciones lineales, utilizaremos el algoritmo de la sección 2.7 para calcular las expresiones simbólicas de Hamburger-Noether.

Hay dos formas de proceder. En primer lugar, supongamos que a partir de la expresión simbólica de Hamburger-Noether calculamos, mediante *evaluación perezosa* (es decir, cada vez que lo necesitemos calculamos un término más de la serie $Z_{r-1}(Z_r)$), la parametrización racional primitiva $(X(Z_r), Y(Z_r))$ dada por el correspondiente desarrollo de Hamburger-Noether. Considerando todas las ramas racionales en los puntos singulares de la curva χ tendríamos de esta manera un conjunto estándar de parametrizaciones racionales primitivas en dichos puntos.

La *fórmula de Dedekind*

$$\mathcal{D}_{\mathrm{X}} \cdot \mathcal{C} = disc_{\mathrm{Y}}(f) \cdot \overline{\mathcal{O}}$$

que expresa el conductor $\mathcal{C}$ de $\overline{\mathcal{O}}$ en $\mathcal{O}$ en términos de la *diferente* $\mathcal{D}_{\mathrm{X}}$ (es decir, el ideal de $\overline{\mathcal{O}}$ generado por $X'(t)$) y del discriminante de la ecuación afín f de la curva nos permite, de hecho, encontrar el divisor de adjunción, ya que el coeficiente d_q de $\mathcal{A}$ relativo a la rama racional q vendrá entonces dado por la fórmula

$$d_q = ord_t\left(\frac{f_Y(X(t),Y(t))}{X'(t)}\right) = ord_t\left(\frac{f_X(X(t),Y(t))}{Y'(t)}\right)$$

donde $(X(t), Y(t))$ es una parametrización racional primitiva de la rama q y $X'(t), Y'(t)$ denotan respectivamente las derivadas con respecto del parámetro t de $X(t), Y(t)$ (nótese que o bien $X'(t) \neq 0$ o bien $Y'(t) \neq 0$). El algoritmo de la sección 2.7 nos ha proporcionado una tal parametrización racional primitiva, y hay una etapa conveniente en la evaluación perezosa que nos permite calcular cualquiera de los dos órdenes en t que aparecen en la fórmula anterior.

Una vez calculados los valores d_q, se considera el coeficiente r_q del divisor R anteriormente considerado en la rama q de χ, y así la condición local en q impuesta por la fórmula $\mathbf{N}^* H \geq \mathcal{A} + R$ al polinomio homogéneo H viene dada por

$$ord_t h(X(t), Y(t)) \geq d_q + r_q$$

siendo h la ecuación local afín de H en términos de las coordenadas X, Y elegidas en el punto $P = \mathbf{N}(q)$ para calcular la expresión simbólica de Hamburger-Noether correspondiente a la rama q. Nuevamente, no es difícil de ver que una etapa conveniente de la evaluación perezosa es suficiente para describir en términos de los coeficientes de los monomios de H los $d_q + r_q$ primeros términos del desarrollo en t de $h(X(t), Y(t))$. La anulación de tales términos produce las ecuaciones lineales requeridas, y cuando q varía entre todas las ramas de los puntos singulares de χ y entre las del soporte de R, el resultado son las ecuaciones lineales que impone globalmente la condición $\mathbf{N}^* H \geq \mathcal{A} + R$.

La segunda forma de encontrar tales condiciones lineales es simplemente imponer las condiciones de *paso virtual* por los puntos infinitamente próximos de la configuración de resolución con multiplicidades $e_p - 1$. Tener multiplicidad en un punto (en general cerrado) mayor o igual que una cantidad dada impone condiciones lineales a los polinomios. El algoritmo de cálculo de las expresiones simbólicas de Hamburger-Noether, como ya hemos indicado en la sección anterior, permite encontrar la configuración de resolución, los pesos de los objetos combinatorios asociados a la misma y coordenadas locales en todos los puntos de dicha configuración; se concluye, por tanto, que siguiendo los pasos de dicho algoritmo podemos ir imponiendo en paralelo las sucesivas condiciones de paso virtual necesarias para que $\mathbf{N}^* H \geq \mathcal{A}$.

El número total de condiciones lineales que se imponen es

$$\sum_P \frac{e_p\,(e_p - 1)}{2} deg\, P$$

donde P varía en la configuración de resolución (es decir, todos los puntos infinitamente próximos P tales que $e_p \geq 2$), ya que la condición $\mu_p(h) \geq e_p - 1$ equivale a la anulación de los coeficientes de $\dfrac{e_p - 1}{2} e_p$ monomios y da lugar, por tanto, a ese número de condiciones lineales sobre un cuerpo isomorfo al cuerpo residual $k(P)$ y, por tanto, a $\dfrac{1}{2} e_p\,(e_p - 1)\, deg\, P$ condiciones lineales sobre el cuerpo base $\mathbb{F}$. Sabemos además que para $n \geq m - 3$ (en las condiciones del teorema 2.1) tales condiciones son linealmente independientes sobre $\mathbb{F}$.

Siguiendo el algoritmo de cálculo para obtener las expresiones simbólicas de Hamburger-Noether, la ecuación de la transformada virtual de h en cada punto P está escrita simbólicamente como un polinomio en dos variables

sobre el cuerpo dado por la extensión simbólica sucesiva de $\mathbb{F}$ correspondiente a P. Las condiciones lineales consisten así en anular los coeficientes de los monomios de grado estrictamente menor que $e_p - 1$ de tal polinomio.

A las condiciones dadas por $\mathbf{N}^*H \geq \mathcal{A}$ hay que añadir las impuestas por el divisor R para poder aplicar el teorema de Brill-Noether y calcular así una base de $\mathcal{L}(G)$. Si el soporte de R no contiene ningún punto singular (es decir, si la adjunta definida por H_0 pasa no sólo virtualmente por los puntos de la configuración de resolución, sino con verdaderas multiplicidades $e_p - 1$ en tales puntos) entonces la condición $\mathbf{N}^*H \geq \mathcal{A} + R$ equivale a imponer simultáneamente las condiciones $\mathbf{N}^*H \geq \mathcal{A}$ y $\mathbf{N}^*H \geq R$; por lo tanto, es suficiente añadir a las condiciones impuestas por $\mathbf{N}^*H \geq \mathcal{A}$ las que vienen dadas por la nueva condición $\mathbf{N}^*H \geq R$, que son también lineales y fáciles de imponer a partir de las expresiones simbólicas de Hamburger-Noether, con lo que se obtiene la totalidad de las condiciones requeridas.

Geométricamente, no obstante, no es práctico buscar polinomios H_0 que produzcan multiplicidades verdaderas $e_p - 1$ (tales polinomios existen para n suficientemente grande debido a un teorema de Serre sobre la anulación de la cohomología, pero es difícil estimar tales valores de n).

Hemos de asumir, por consiguiente, que el soporte de R contiene ramas en los puntos singulares. Denotemos por r_q el coeficiente de R correspondiente a la rama racional q; como R es un divisor efectivo, se tiene que $r_q \geq 0$ para toda rama q. Veremos a continuación cómo la condición $\mathbf{N}^*H \geq \mathcal{A} + R$ se puede expresar también con condiciones de paso virtual sobre H.

Para ello, consideremos la *configuración* $\mathfrak{C}_\chi^{+,R}$ consistente en añadir a la configuración de resolución $\mathfrak{C}_\chi$ los r_q primeros puntos de multiplicidad 1 de la cadena de puntos infinitamente próximos correspondientes a la rama q, para cada rama racional q en el soporte de R. Nótese que la rama racional q puede ser o no una rama en un punto singular de χ, luego la configuración $\mathfrak{C}_\chi^{+,R}$ puede tener más constelaciones (constelación es el análogo de árbol cuando configuración se interpreta como el análogo de bosque) que $\mathfrak{C}_\chi$.

La condición $\mathbf{N}^*H \geq \mathcal{A} + R$ se puede expresar, tal y como ya se ha hecho anteriormente, mediante las condiciones locales

$$ord_t h(X_q(t), Y_q(t)) \geq d_q + r_q \qquad (\star)$$

para toda rama racional q representada en $\mathfrak{C}_\chi^{+,R}$, siendo $(X_q(t), Y_q(t))$ una parametrización racional primitiva correspondiente a dicha rama q. De las desigualdades $(\star)$ se deriva el siguiente resultado.

Proposición 2.1 *En las condiciones anteriores, la desigualdad* $\mathbf{N}^*H \geq \mathcal{A} + R$ *es equivalente a la condición de que la hipersuperficie definida por* H *pasa por los puntos de la configuración* $\mathfrak{C}_\chi^{+,R}$ *con multiplicidades virtuales* $e_p - 1$ *en los puntos* p *de* $\mathfrak{C}_\chi$ *y* 1 *en los puntos de* $\mathfrak{C}_\chi^{+,R} \setminus \mathfrak{C}_\chi$ *.*

Demostración:

Si $\mathbf{N}^*H \geq \mathcal{A} + R$ entonces $\mathbf{N}^*H \geq \mathcal{A}$, ya que $R \geq 0$. Por lo tanto, la hipersuperficie definida por H pasa por los puntos p de $\mathfrak{C}_\chi$ con multiplicidades virtuales $e_p - 1$. Por otro lado, la fórmula $(\star)$ muestra que la transformada virtual de la hipersuperficie en el primer punto de multiplicidad 1 sobre la rama correspondiente a q tiene multiplicidad de intersección mayor o igual que r_q con la transformada estricta de dicha rama; por lo tanto, pasa por los r_q puntos de $\mathfrak{C}_\chi^{+,R} \setminus \mathfrak{C}_\chi$ correspondientes a la rama q con multiplicidad virtual 1.

Recíprocamente, si la hipersuperficie dada por H pasa por los puntos de $\mathfrak{C}_\chi$ con multiplicidades virtuales $e_p - 1$ y por los de $\mathfrak{C}_\chi^{+,R} \setminus \mathfrak{C}_\chi$ con multiplicidad virtual 1, entonces se satisface la desigualdad $(\star)$ para toda rama q representada en $\mathfrak{C}_\chi^{+,R}$.

□

Nota 2.5 *La proposición anterior aparece considerada en [20] y [21] para el caso en que* $r_q = e_{\mathbf{N}(q),q} - 1$*, donde* $\mathbf{N}(q)$ *denota el vértice del bosque de resolución correspondiente al punto del plano* $\mathbf{N}(Q)$*, como resultado auxiliar básico para la determinación del comportamiento de la curva polar* [4] *de una curva plana en característica cero. En realidad, el resultado es cierto también en cualquier característica y para valores arbitrarios de* r_q *siempre que* $r_q \geq 0$*. Nótese que la proposición da un número de condiciones lineales igual a* $\frac{1}{2} deg\, \mathcal{A} + deg\, R$*, pero posiblemente tales condiciones son linealmente dependientes.*

Nota 2.6 *La teoría de Enriques sobre curvas planas con singularidades asignadas (o en términos modernos la teoría de Zariski-Lipman de ideales completos) permite sustituir los pesos* $e_p - 1$ *en* $\mathfrak{C}_\chi$ *y* 1 *en* $\mathfrak{C}_\chi^{+,R} \setminus \mathfrak{C}_\chi$ *por otros pesos*

[4] Dado un germen de curva en el origen definido por el polinomio $f(\mathrm{X}, \mathrm{Y})$, el llamado haz de curvas polares viene dado por la expresión $\lambda f_{\mathrm{X}} + \mu f_{\mathrm{Y}}$, donde al menos una de las constantes λ, μ es no nula.

$\overline{e_p}$ *sobre* $\mathfrak{C}_\chi^{+,R}$ *que satisfacen las llamadas "desigualdades de proximidad", es decir*

$$\overline{e_p} \geq \sum_{r \to p} \overline{e_r} \qquad \forall p \in \mathfrak{C}_\chi^{+,R}$$

de tal manera que las condiciones impuestas por los pesos antiguos y por los nuevos sean equivalentes. El paso de los pesos antiguos a los nuevos se realiza por medio de un algoritmo en el marco de la combinatoria conocido como "principio de descarga de Enriques" (ver [20], por ejemplo). En el marco de la combinatoria quiere decir que si la configuración $\mathfrak{C}_\chi^{+,R}$ *se considera como configuración de resolución sumergida (siempre lo es para alguna curva adecuada, aunque no necesariamente sea* χ*), entonces el principio de descarga se puede describir en términos del bosque de resolución sumergida asociado a la configuración* $\mathfrak{C}_\chi^{+,R}$ *(es decir, el objeto combinatorio dado por tantos puntos como en dicha configuración más la especificación de la relación binaria de proximidad entre tales puntos).*

La utilidad geométrica del principio de descarga consiste en encontrar pesos en la correspondiente configuración cuya imposición como multiplicidades virtuales dé lugar a condiciones linealmente independientes, al menos localmente y para grados suficientemente grandes; de esta manera, se economiza en la práctica el número de condiciones. Globalmente las condiciones no son en general independientes, ni podemos esperar que en general lo sean; el caso $R = 0$ *y* $n \geq m - 3$ *es un caso especial en el que las condiciones son independiente gracias al teorema 2.1 .*

Nota 2.7 *Los* r_q *puntos de multiplicidad* 1 *añadidos en cada rama* q *pueden deducirse en la práctica de las expresiones simbólicas de Hamburger-Noether, evaluando los* r_q *primeros términos del desarrollo de Taylor de la función implícita dada por el polinomio* $g(\mathrm{Z}_r, \mathrm{Z}_{r-1})$*.*

Como conclusión de lo expuesto hasta ahora en el segundo capítulo podemos enunciar, a modo de resumen, el siguiente resultado, cuyo contenido constituye el objetivo principal de dicho capítulo.

Teorema 2.4 *Sea* χ *una curva plana absolutamente irreducible definida sobre el cuerpo finito* $\mathbb{F}$ *dada por un polinomio* $F(\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2) \in \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2]$*. Sea* G *un divisor racional de la curva normalizada* $\tilde{\chi}$*, representado su soporte por ramas racionales de* χ *especificadas en ciertos puntos. Entonces existe*

un algoritmo de "cálculo simbólico" que permite calcular bases sobre $\mathbb{F}$ *para el espacio vectorial* $\mathcal{L}(G)$ *y que consta de las siguientes etapas:*

(1) *Calcular los puntos cerrados del plano proyectivo que son singulares para* χ *por cualquier procedimiento estándar de álgebra computacional.*

(2) *Calcular las expresiones simbólicas de Hamburger-Noether en los puntos singulares de* χ *mediante el algoritmo dado en la sección 2.7 .*

(3) *Calcular una adjunta para* χ *de ecuación* H_0 *y grado* $n \geq m-3$ *tal que* $\mathbf{N}^* H_0 \geq \mathcal{A}+G$*, donde* $\mathcal{A}$ *es el divisor de adjunción de* χ *y* $\mathbf{N} : \tilde{\chi} \to \mathbb{P}^2$ *es la inmersión de* χ *compuesta con el morfismo de normalización* $\mathbf{n}$*, y calcular posteriormente el resto* $R = \mathbf{N}^* H_0 - \mathcal{A} - G$*.*

(4) *Escribir las condiciones lineales* $\mathbf{N}^* H \geq \mathcal{A} + R$ *tomando como variables los coeficientes de un polinomio homogéneo genérico* H *de grado* n *y usando, además de las expresiones simbólicas de Hamburger-Noether, el método dado por la proposición 2.1 (o bien el refinamiento dado por el principio de descarga).*

(5) *Utilizar el teorema de Brill-Noether para calcular, según el método dado por el algoritmo 2.1 , una base sobre* $\mathbb{F}$ *del espacio vectorial* $\mathcal{L}(G)$*.*

Nota 2.8

i) *Algoritmo de "cálculo simbólico" quiere decir, en este caso, que la técnica de cálculo que se utiliza consiste en añadir a* $\mathbb{F}$ *sucesivas raíces simbólicas (en las etapas (1) y (2)). La localización de estas raíces simbólicas requiere la factorización de polinomios de una variable en sus componentes irreducibles, problema que también tiene una resolución efectiva en el terreno del cálculo formal.*

ii) *El terreno es válido para cuerpos perfectos arbitrarios siempre que éstos sean "computables", es decir, que se puedan realizar sobre ellos cálculos elementales de una forma efectiva. Por ejemplo, el teorema tiene su aplicación al cálculo de adjuntas de curvas planas definidas sobre* $\mathbb{Q}$ *o sobre un cuerpo de números algebraicos (situación habitual en la práctica cuando se esté en característica cero).*

2.8.2 Cálculo de semigrupos de Weierstrass

En la teoría de decodificación de Feng y Rao expuesta en el párrafo 1.3.4 el interés práctico consiste en encontrar bases para los espacios $\mathcal{L}(lP)$ donde P es un punto racional de $\tilde{\chi}$, de forma que si $l \in \Gamma_P$, donde Γ_P es el *semigrupo de Weierstrass* de $\tilde{\chi}$ en P (es decir, por definición, el subsemigrupo aditivo de $\mathbb{N}$ formado por las *no-lagunas de Weierstrass* en P, que ya fueron definidas en dicho párrafo), la base de $\mathcal{L}(lP)$ se obtiene añadiendo a una base de $\mathcal{L}((l-1)\,P)$ una función f_l con un polo de orden l en P y regular en $\tilde{\chi} \setminus \{P\}$.

Veremos a continuación cómo los resultados de las secciones precedentes se pueden aplicar para dar un algoritmo que calcule las funciones f_l sucesivamente, y obtener de aquí las bases de los espacios $\mathcal{L}(lP)$ requeridas en el método de decodificación de Feng y Rao.

Manteniendo la notación y las hipótesis del párrafo anterior, supongamos que $G = lP$, donde l es un entero no negativo y P es un punto racional (sobre $\mathbb{F}$) de $\tilde{\chi}$, es decir, una rama racional definida sobre $\mathbb{F}$ en algún punto de la curva χ.

La fórmula de Riemann-Roch aplicada a los divisores lP y $(l-1)\,P$ da lugar a la igualdad

$$(\ell(lP) - \ell((l-1)\,P)) - (i(lP) - i((l-1)\,P)) = 1$$

siendo $0 \leq \ell(lP) - \ell((l-1)\,P) \leq 1$ y $-1 \leq i(lP) - i((l-1)\,P) \leq 0$. Por lo tanto, se tendrá que $l \notin \Gamma_P$ si y sólo si $l \geq 1$ y existe una forma diferencial regular sobre $\tilde{\chi}$ con un cero de orden $l-1$ en P.

Nótese que si $l \geq 2g$ entonces $l \in \Gamma_P$, es decir, el orden de un cero en P de una diferencial regular sobre $\tilde{\chi}$ está acotado por $2g-2$. Más aún, se sabe que existe una diferencial regular sobre $\tilde{\chi}$ con un cero en P de orden $2g-2$ si y sólo si la curva $\tilde{\chi} \setminus \{P\}$ es intersección completa afín (ver Delgado [28] o Sathaye [96]). [5]

Como consecuencia de lo anterior, y utilizando el corolario del teorema 2.1 se deduce el siguiente resultado.

Proposición 2.2 *Sea l un entero tal que $1 \leq l \leq 2g-2$. Entonces:*

[5] De hecho esta propiedad es equivalente a que el semigrupo Γ_P sea simétrico respecto de $2g-1$, es decir, $2g-1 \geq l \in \Gamma_P$ si y sólo si $2g-1-l \notin \Gamma_P$, y a su vez equivalente a que el conductor del semigrupo sea $c = 2g$, a que la última laguna sea $\bar{l} = 2g-1$, y a que $K = (2g-2)P$ sea un divisor canónico.

(a) *$l \notin \Gamma_P$ si y sólo si existe un polinomio homogéneo H_0 de grado $m-3$ tal que $\mathbf{N}^* H_0 \geq \mathcal{A} + (l-1)P$ y P no está en el soporte del divisor efectivo $\mathbf{N}^* H_0 - \mathcal{A} - (l-1)P$.*

(b) *Existe $l' \geq l$ con $l' \notin \Gamma_P$ si y sólo si existe un polinomio homogéneo H_0 de grado $m-3$ tal que $\mathbf{N}^* H_0 \geq \mathcal{A} + (l-1)P$.*

Demostración:

El apartado (a) es inmediato a partir de los comentarios precedentes, con lo que sólo probaremos el segundo apartado de la proposición. Si existe $l' \geq l$ con $l' \notin \Gamma_P$, entonces existe una forma diferencial regular con un cero de orden $l'-1$ en P. Aplicando el corolario 2.1 existe una adjunta de grado $m-3$ cuyo divisor es mayor o igual que $(l'-1)P$ fuera de $\mathcal{A}$, es decir, se tiene

$$\mathbf{N}^* H_0 \geq \mathcal{A} + (l'-1)P \geq \mathcal{A} + (l-1)P$$

Recíprocamente, si existe un polinomio homogéneo H_0 de grado $m-3$ con $\mathbf{N}^* H_0 \geq \mathcal{A} + (l-1)P$, entonces existe una forma diferencial $\omega \neq 0$ tal que $(\omega) \geq (l-1)P$. Si $l'-1$ es el orden del cero de ω en P, entonces $l' \geq l$ y $l' \notin \Gamma_P$.

□

Como consecuencia, el siguiente teorema nos proporciona un método algorítmico para calcular el semigrupo de Weierstrass y bases sobre $\mathbb{F}$ para los espacios $\mathcal{L}(lP)$ mediante las técnicas estudiadas en el presente capítulo.

Teorema 2.5 *En las condiciones anteriores, existe un algoritmo fundamentado en la teoría de adjuntas para calcular el semigrupo de Weierstrass Γ_P así como funciones f_l con un polo de orden l en P y regulares en $\tilde{\chi} \setminus \{P\}$, para todo $l \in \Gamma_P$.*

Demostración:

Tomando el divisor $G = (l-1)P$ en lugar del divisor R en la proposición 2.1 y usando la configuración $\mathfrak{C}_\chi^{+,G}$ se pueden imponer sobre los polinomios H de grado $m-3$ las condiciones dadas por $\mathbf{N}^* H \geq \mathcal{A} + (l-1)P$. Gracias a la citada proposición, estas condiciones son equivalentes a pasar virtualmente

por los puntos q de $\mathfrak{C}_\chi$ con multiplicidades $e_q - 1$ y por los puntos de $\mathfrak{C}_\chi^{+,G} \setminus \mathfrak{C}_\chi$ con multiplicidad 1.

Para valores crecientes de l a partir de $l = 0$ (que siempre está en el semigrupo Γ_P y no impone, por tanto, ninguna condición sobre H) se van imponiendo sucesivamente las condiciones lineales dadas por las desigualdades $\mathbf{N}^* H \geq \mathcal{A} + lP$, lo cual añade una condición por cada unidad que aumente el valor de l. Entonces, la condición impuesta por el nuevo l que se ha aumentado en una unidad será independiente de las anteriores, por la proposición 2.2 , si y sólo si el valor l no está en el semigrupo Γ_P. Como hay g lagunas en dicho semigrupo, es decir, que el cardinal de $\mathbb{N} \setminus \Gamma_P$ es exactamente g, el proceso se termina con la aparición de g condiciones independientes de las anteriores, tras lo cual tendríamos calculadas las g lagunas y por tanto el semigrupo de Weierstrass Γ_P. Nótese que $g \geq 0$, al ser la curva χ absolutamente irreducible, y por tanto g es menor o igual que el género aritmético $p_a(\chi)$, el cual coincide con la dimensión del espacio de formas de grado $m-3$; en consecuencia, el proceso anterior determina todas las lagunas del semigrupo Γ_P.

Calculado el *semigrupo*, nuestro propósito es hallar una función para cada uno de los valores de dicho semigrupo, para lo cual el problema se reduce a calcular un sistema de generadores del semigrupo y hallar una función para cada uno de dichos generadores. Desde el punto de vista teórico, puede buscarse el *sistema minimal de generadores*, que es por definición el formado por los elementos irreducibles del semigrupo, pero en la práctica es más efectivo buscar un *sistema de generadores de Apéry* pues, como se verá con detalle en el próximo capítulo, será tremendamente útil para calcular la llamada *distancia de Feng y Rao* de un elemento cualquiera del semigrupo. En todo caso, supondremos encontrado un sistema cualquiera de generadores y mostraremos cómo hallar las correspondientes *funciones*, lo cual consistirá básicamente en aplicar de forma conveniente el algoritmo de Brill-Noether para el caso $G = lP$.

Sea pues $\tilde{l}$ el mayor elemento del sistema de generadores que tenemos para el semigrupo Γ_P y tomemos un polinomio homogéneo H_0 no divisible por F de grado n suficientemente grande tal que $\mathbf{N}^* H_0 \geq \mathcal{A} + \tilde{l}P$. Este polinomio H_0 puede utilizarse para localizar elementos no nulos de $\mathcal{L}(lP) \setminus \mathcal{L}((l-1)\,P)$ para $l \leq \tilde{l}$ con $l \in \Gamma_P$.

En efecto, si $\mathbf{N}^* H_0 = \mathcal{A} + lP + R_l$ resulta que $R_{l-1} = R_l + P$. Tomando ahora valores decrecientes de l se pueden imponer (puesto que los divisores

R_l son efectivos) las condiciones $\mathbf{N}^*H \geq \mathcal{A} + R_l$ mediante la proposición 2.1 dando lugar a la localización de polinomios homogéneos H_l también de grado n y no divisibles por F que satisfacen la condición $\mathbf{N}^*H_l \geq \mathcal{A} + R_l$ pero que no satisfacen la condición $\mathbf{N}^*H_l \geq \mathcal{A} + R_{l-1}$. Este proceso equivale a aplicar sucesivamente el algoritmo de Brill-Noether a los divisores $G = lP$ para $l = \tilde{l}, \ldots, 0$ y $l \in \Gamma_P$, utilizando constantemente H_0 como divisor de la funciones obtenidas, y adjuntas de grado n como denominadores. De esta manera, la función $f_l = H_l/H_0$ es regular sobre $\tilde{\chi} \setminus \{P\}$ y tiene un polo de orden l en P. En particular, este procedimiento puede aplicarse a los elementos l dentro del sistema de generadores prefijado.

□

Ejemplo 2.2 *Sea χ la cuártica de Klein sobre $\mathbb{F}_2$ dada por la ecuación*

$$F(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) = \mathrm{X}^3\mathrm{Y} + \mathrm{Y}^3\mathrm{Z} + \mathrm{Z}^3\mathrm{X} = 0$$

cuyo divisor de adjunción es $\mathcal{A} = 0$, puesto que la curva χ es no singular. Veamos cómo calcular el semigrupo de Weierstrass de dicha curva en $P = (0 : 0 : 1)$ utilizando el método que acabamos de exponer.

Como el punto P es no singular, se obtiene fácilmente por evaluación perezosa una parametrización local de χ en P mediante las expresiones

$$\begin{cases} X(t) = t^3 + t^{10} + \ldots \\ Y(t) = t \end{cases}$$

Para calcular las lagunas de Γ_P utilizaremos adjuntas de grado $m - 3 = 1$, cuya ecuación genérica [6] *viene dada por*

$$H(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) = a\mathrm{X} + b\mathrm{Y} + c\mathrm{Z}$$

con lo que al sustituir los primeros términos de la parametrización local en P se obtiene como resultado

$$h(X(t), Y(t)) = c + bt + at^3 + at^{10} + \ldots$$

y aplicamos el procedimiento descrito en el teorema 2.5 :

[6] Nótese que toda curva plana es adjunta a χ, al ser $\mathcal{A} = 0$.

- *$l = 1$ es necesariamente la primera laguna del semigrupo, puesto que el género de la curva es $g = p_a(\chi) = 3 > 0$; no obstante, este hecho es detectado por nuestro algoritmo, ya que la desigualdad $ord_t h(X(t), Y(t)) \geq 1$ equivale a la condición $c = 0$, y ésta es linealmente independiente de las que impone $l = 0$, puesto que en realidad $l = 0$ no impone ninguna condición.*

- *Si $l = 2$, la desigualdad $ord_t h(X(t), Y(t)) \geq 2$ equivale a la condición $c = b = 0$, que también es linealmente independiente de la anterior, con lo que $l = 2$ es una nueva laguna de Weierstrass.*

- *Para $l = 3$, la desigualdad $ord_t h(X(t), Y(t)) \geq 3$ equivale también a que $c = b = 0$, por lo que la condición impuesta es linealmente dependiente de las anteriores y se tiene que $3 \in \Gamma_P$.*

- *Por último, si $l = 4$ la desigualdad $ord_t h(X(t), Y(t)) \geq 4$ equivale a que $c = b = a = 0$; la condición impuesta es linealmente independiente de las anteriores, con lo que $l = 4$ es la tercera y última laguna de Γ_P y se termina el proceso.*

En consecuencia, las lagunas de Weierstrass son $l = 1, 2, 4$ (como puede comprobarse fácilmente a partir de la caracterización dada por la proposición 2.2), y el sistema minimal de generadores del semigrupo es $\{3, 5, 7\}$. Nótese en particular que el semigrupo no es simétrico respecto de $2g - 1$, puesto que el conductor es $c = 5 < 6 = 2g$.

Veamos ahora cómo calcular una función para cada uno de los elementos del sistema minimal de generadores [7] *que acabamos de calcular. Para ello, empezaremos por aplicar parte del algoritmo de Brill-Noether al divisor $G = 7P$, para obtener una forma H_0 de grado $n = 4$ que no sea divisible por F, y tal que $\mathbf{N}^* H_0 \geq J_+ = J = G = 7P$. En definitiva, si H_0 es una forma genérica de grado 4 dada por coeficientes indeterminados, la condición anterior equivale a que $ord_t H_0(X(t), Y(t), 1) \geq 7$, donde $(X(t), Y(t))$ es la parametrización local de χ en P que (mediante evaluación perezosa) hemos considerado anteriormente; además, la condición lineal de que F no divida*

[7] En realidad, hemos obtenido un sistema de generadores de Apéry relativo al elemento $\ell = 3$; este concepto será introducido en la última sección del próximo capítulo, e implica unas propiedades aritméticas muy buenas para dicho sistema, según veremos en dicha sección.

a H_0 equivale en este caso, dado que ambos tienen igual grado, a que no sean proporcionales sobre $\mathbb{F}$. Estas dos observaciones nos permiten imponer fácilmente las condiciones lineales precisas sobre los coeficientes de H_0 para determinar una forma cualquiera con las propiedades requeridas, como por ejemplo $H_0 = \mathrm{X}^2\mathrm{YZ}$.

El siguiente paso es el cálculo del divisor $\mathbf{N}^*H_0$; para ello, llamando $Q_1 = (1:0:0)$ y $Q_2 = (0:1:0)$ y utilizando, dada la simetría de F respecto de las tres variables, parametrizaciones locales en dichos puntos totalmente análogas a la utilizada en el punto $P = (0:0:1)$, se comprueba primero fácilmente que

$$\begin{array}{rcrcr} \mathbf{N}^*(\mathrm{X}) & = & Q_2 & + & 3P \\ \mathbf{N}^*(\mathrm{Y}) & = & P & + & 3Q_1 \\ \mathbf{N}^*(\mathrm{Z}) & = & Q_1 & + & 3Q_2 \end{array}$$

con lo cual se deduce que

$$\mathbf{N}^*H_0 = 2\,\mathbf{N}^*(\mathrm{X}) + \mathbf{N}^*(\mathrm{Y}) + \mathbf{N}^*(\mathrm{Z}) = 7P + 4Q_1 + 5Q_2$$

A continuación, se toma $l = 7$ y se calcula el resto $R_7 = 4Q_1 + 5Q_2$, pasando ahora a buscar, mediante el mismo procedimiento con el que hemos encontrado H_0 , una forma H_7 de grado 4 distinta de F tal que $\mathbf{N}^*H_7 \geq R_7$ pero que no verifique la desigualdad $\mathbf{N}^*H_7 \geq R_6 = R_7 + P$; esto es equivalente a que se verifique la condición $\mathbf{N}^*H_7 \geq R_7$ junto con la condición local en P dada por

$$ord_t H_7(X(t), Y(t), 1) = 0$$

lo que permite fácilmente comprobar que $H_7 = \mathrm{Z}^4$ cumple las condiciones requeridas, y por tanto la función $f_7 = \dfrac{\mathrm{Z}^3}{\mathrm{X}^2\mathrm{Y}}$ tiene un único polo en P de orden $l = 7$.

De forma análoga, se comprueba fácilmente que $H_5 = \mathrm{Y}^2\mathrm{Z}^2$ verifica la condición $\mathbf{N}^*H_5 \geq R_5$ pero no la condición $\mathbf{N}^*H_5 \geq R_4$, con lo que la función $f_5 = \dfrac{\mathrm{YZ}}{\mathrm{X}^2}$ tiene un único polo en P de orden $l = 5$, y que $H_3 = \mathrm{XYZ}^2$ verifica la condición $\mathbf{N}^*H_3 \geq R_3$ pero no la condición $\mathbf{N}^*H_3 \geq R_2$, con lo que la función $f_3 = \dfrac{\mathrm{Z}}{\mathrm{X}}$ tiene un único polo en P de orden $l = 3$. En particular, se obtiene una base de $\mathcal{L}(7P)$ sobre $\mathbb{F}_2$ de la forma

$$\{1, \frac{\mathrm{Z}}{\mathrm{X}}, \frac{\mathrm{YZ}}{\mathrm{X}^2}, \frac{\mathrm{Z}^2}{\mathrm{X}^2}, \frac{\mathrm{Z}^3}{\mathrm{X}^2\mathrm{Y}}\}$$

según el método que se expondrá en párrafo 3.4.2 del siguiente capítulo.

Nota 2.9 *El algoritmo dado por el teorema anterior tiene una complejidad muy elevada y necesita, en particular, el cálculo previo de las expresiones simbólicas de Hamburger-Noether. En el siguiente capítulo estudiaremos un caso particular de mucho interés en la práctica, como es el caso en el que P es la única rama racional de χ sobre una recta del plano proyectivo (usualmente la recta del infinito). En este caso, el teorema de Abhyankar-Moh y la teoría de raíces aproximadas nos proporcionará un algoritmo completamente diferente, que resulta ser más rápido y más adecuado al problema que se quiere resolver.*

Chapter 3

Semigrupos de Weierstrass y curvas planas con una única rama en el infinito

En este capítulo, estudiaremos un método alternativo al algoritmo de Brill-Noether para el caso de que el divisor considerado sea de la forma $G = mP$, donde el punto P es racional sobre el cuerpo base $\mathbb{F}$, de gran interés para los códigos geométricos de Goppa llamados *códigos sobre un punto*. Más precisamente, estudiaremos el caso en que P se visualiza como el único punto geométrico en la recta del infinito de una curva plana definida sobre $\mathbb{F}$, siendo entonces necesariamente P racional sobre $\mathbb{F}$, y de forma que exista una única rama racional sobre él, que necesariamente estará también definida sobre $\mathbb{F}$. El algoritmo que describiremos calcula de hecho el semigrupo de Weierstrass en el punto P y una función para cada posible valor en dicho semigrupo, obteniéndose de paso una base de $\mathcal{L}(mP)$, la distancia de Feng y Rao del semigrupo de Weierstrass y un criterio de irreducibilidad absoluta para la curva considerada.

3.1 Semigrupos en el infinito

A lo largo de todo este capítulo, $\tilde{\chi}$ denotará una curva algebraica proyectiva no singular definida sobre un cuerpo perfecto $\mathbb{F}$ tal que $\tilde{\chi}$ sea irreducible sobre $\overline{\mathbb{F}}$; asimismo, denotaremos por χ un modelo plano para $\tilde{\chi}$ con una sola

rama racional en el infinito que esté definida sobre $\mathbb{F}$, es decir, tal que se tiene un morfismo birracional

$$\mathbf{n} \ : \ \tilde{\chi} \to \chi \subseteq \mathbb{P}^2$$

y una recta $L \subseteq \mathbb{P}^2$ definida sobre $\mathbb{F}$ tal que $L \cap \chi$ consiste en un único punto P que es racional sobre $\mathbb{F}$ y χ tiene una sola rama racional en P que está definida sobre $\mathbb{F}$. De esta manera hay un único punto de $\tilde{\chi}$ sobre P, que denotaremos por $\overline{P}$. Se consideran entonces las curvas afines $\tilde{C} = \tilde{\chi} \setminus \{\overline{P}\}$ y $C = \chi \setminus \{P\}$. Esta notación se mantendrá a lo largo de todo el presente capítulo.

En las condiciones anteriores podemos suponer, salvo un cambio lineal de coordenadas, que la ecuación afín de la curva C está dada por un polinomio $F(\mathrm{X}, \mathrm{Y}) \in \mathbb{F}[\mathrm{X}][\mathrm{Y}]$ que es mónico en la variable Y y cuyo grado total coincide con el grado en Y. La definición que damos a continuación es fundamental en lo que sigue.

Definición 3.1 *Se tienen los dos subsemigrupos aditivos de* $\mathbb{N}$ *siguientes:*

$$\Gamma_P \doteq \{-\upsilon_{\overline{P}}(f) \mid f \in \mathcal{O}_{\tilde{\chi}}(\tilde{C})\}$$
$$S_P \doteq \{-\upsilon_{\overline{P}}(f) \mid f \in \mathcal{O}_{\chi}(C)\}$$

El primero de ellos no es otra cosa que el semigrupo de Weierstrass de $\tilde{\chi}$ en $\overline{P}$, que ya fue definido de una forma equivalente en el párrafo 2.8.2; este semigrupo contiene al segundo, pero no coinciden en general salvo que la curva χ sea no singular en la parte afín.

La principal observación es que ambos semigrupos son de complemento finito, es decir, tanto $\mathbb{N} \setminus \Gamma_P$ como $\mathbb{N} \setminus S_P$ son finitos. De hecho $\mathbb{N} \setminus \Gamma_P$ tiene g elements, donde g es el género de $\tilde{\chi}$, y son las llamadas lagunas de Weierstrass. Con el fin de calcular el cardinal de $\mathbb{N} \setminus S_P$, probaremos el siguiente resultado.

Lema 3.1 (Algoritmo de triangulación) *Sean* $\overline{A}$ *y* A *respectivamente las* $\mathbb{F}$*-álgebras afines de* $\tilde{C}$ *y* C*, es decir,* $\overline{A} = \mathcal{O}_{\tilde{\chi}}(\tilde{C})$ *y* $A = \mathcal{O}_{\chi}(C)$*, siendo* $\overline{A}$ *la normalización del anillo* A*; entonces se tiene:*

$$\sharp(\Gamma_P \setminus S_P) = dim_{\mathbb{F}}(\overline{A}/A) = \sum_{Q \in C} \delta_Q(C)$$

donde Q *recorre todos los puntos cerrados de* C *y* $\delta_Q(C) = dim_{\mathbb{F}}(\overline{\mathcal{O}}_{\chi,Q}/\mathcal{O}_{\chi,Q})$*, siendo* $\overline{\mathcal{O}}_{\chi,Q}$ *la normalización del anillo* $\mathcal{O}_{\chi,Q}$*.*

Demostración:

La segunda igualdad es consecuencia de que

$$\overline{A}/A = \bigoplus_{Q \in Sing\, C} \overline{\mathcal{O}}_{\chi,Q}/\mathcal{O}_{\chi,Q}$$

donde $Sing\, C$ es el conjunto de los puntos singulares de la curva C. Para probar la primera igualdad, tomamos una base $\{h_1, \ldots, h_l\}$ de $\overline{A}/A$ sobre $\mathbb{F}$; dicha base puede ser calculada previamente a partir del *algoritmo de la base entera*, y equivale geométricamente al proceso de resolución de singularidades de la curva que están en la parte afín.

A continuación mostraremos un procedimiento efectivo, que llamaremos *algoritmo de triangulación*, para encontrar los valores de $\Gamma_P \setminus S_P$, así como funciones que alcancen dichos valores.

Sea $A^i \doteq A + \mathbb{F}h_1 + \ldots + \mathbb{F}h_i$, para $0 \leq i \leq l$; vamos a proceder por inducción, así que sea $0 \leq i < l$ y supongamos que hemos encontrado funciones $g_1, \ldots, g_i$ linealmente independientes sobre $\mathbb{F}$ tales que

$$\begin{gathered} \Gamma_P^i \doteq S_P \cup \{-v_{\overline{P}}(g_1), \ldots, -v_{\overline{P}}(g_i)\} \subseteq \Gamma_P \\ -v_{\overline{P}}(g_j) \notin \Gamma_P^{i-1} \\ A + \mathbb{F}g_1 + \ldots + \mathbb{F}g_i = A^i \end{gathered}$$

Tomamos ahora h_{i+1}; si $-v_{\overline{P}}(h_{i+1}) \notin \Gamma_P^i$, entonces escribimos $g_{i+1} = h_{i+1}$ y seguimos el proceso.

En caso contrario, existe $f \in A^i$ tal que

$$\begin{gathered} v_{\overline{P}}(h_{i+1}) = v_{\overline{P}}(f) \\ -v_{\overline{P}}(h_{i+1} - f) < -v_{\overline{P}}(h_{i+1}) \end{gathered}$$

De esta manera reemplazamos h_{i+1} por $h_{i+1} - f$ y repetimos el proceso con $h_{i+1} - f$ en vez de h_{i+1}; puesto que $h_{i+1} \notin A^i$, se sigue que en un número finito de pasos podremos reemplazar h_{i+1} por

$$g_{i+1} \equiv h_{i+1} \pmod{A^i}$$

con

$$-v_{\overline{P}}(g_{i+1}) \notin \Gamma_P^i$$

Al final del proceso, habremos añadido l elementos diferentes de $\Gamma_P \setminus S_P$, con lo que $\sharp(\Gamma_P \setminus S_P) \geq dim_{\mathbb{F}}(\overline{A}/A)$.

Por otro lado, puesto que $\overline{A} = A^l = A + \mathbb{F}g_1 + \ldots + \mathbb{F}g_l$, se tiene que todo $h \in \overline{A}$ puede escribirse de manera única en la forma $h = g + \lambda_1 g_1 + \ldots + \lambda_l g_l$ con $g \in A$ y $\lambda_i \in \mathbb{F}$; puesto que los valores $v_{\overline{P}}(g_i)$ y $v_{\overline{P}}(g)$ son diferentes dos a dos se tiene que, o bien $-v_{\overline{P}}(h) \in S_P$, o bien $-v_{\overline{P}}(h) = -v_{\overline{P}}(g_i)$ para un único i, lo cual prueba la igualdad buscada.

□

Nótese que el conjunto Γ_P^i no es necesariamente un semigrupo, puesto que al añadir un elemento a un semigrupo deberíamos para ello añadir también (entre otros) todos los múltiplos del nuevo elemento añadido. Esta idea podría incorporarse al proceso de triangulación, pero no puede asegurarse que el algoritmo obtenido sea más rápido (ni más claro) que el anteriormente descrito, puesto que no se puede saber a priori cuales de los elementos que quedan por añadir en la base de $\overline{A}/A$ sobre $\mathbb{F}$ nos van a proporcionar valores que están ya en el semigrupo suma del anterior y el generado por el nuevo elemento.

Nuestro propósito en lo que queda de capítulo es el siguiente: intentaremos describir el semigrupo Γ_P en dos etapas, calculando en primer lugar un sistema de generadores del semigrupo S_P con buenas propiedades aritméticas, dando a la vez explícitamente una función para cada uno de los elementos de dicho semigrupo, y en segundo lugar completar los elementos que faltan a partir de una base de $\overline{A}/A$ como $\mathbb{F}$-espacio vectorial mediante el procedimiento de triangulación descrito en el lema anterior, con el cual obtenemos también tanto los valores como funciones explícitas que los alcanzan. En particular, una vez descrito el semigrupo de Weierstrass Γ_P habremos calculado de paso el género geométrico de la curva, pues éste nos es más que el número de lagunas de dicho semigrupo.

En cuanto a la segunda etapa, podemos realizar el cálculo de una base de $\overline{A}/A$ como $\mathbb{F}$-espacio vectorial utilizando una base de $\overline{A}$ como $\mathbb{F}[\mathrm{X}]$-módulo obtenida mediante el algoritmo de la base entera. Como veremos más adelante, dicha base entera es de la forma

$$\mathcal{B}_1 = \{1, \frac{a_{1,0}(\mathrm{X}) + a_{1,1}(\mathrm{X})\,\mathrm{Y}}{b_1(\mathrm{X})}, \ldots, \frac{a_{m-1,0}(\mathrm{X}) + \ldots + a_{m-1,m-1}(\mathrm{X})\,\mathrm{Y}^{m-1}}{b_{m-1}(\mathrm{X})}\}$$

donde m es el grado de la curva y ésta está dada por un polinomio mónico en

Y de grado m con coeficientes en $\mathbb{F}[X]$ (para más detalles, ver Trager [104]). En particular, $\mathcal{B}_1$ es un sistema de generadores de $\overline{A}$ como A-módulo, puesto que $A \supseteq \mathbb{F}[X]$.

Por otro lado, una base de A sobre $\mathbb{F}$ está dada por

$$\mathcal{B}_2 = \{X^i Y^j \mid i \geq 0, 0 \leq j \leq m-1\}$$

En consecuencia, el conjunto $\mathcal{G} = \{\alpha \cdot \beta \mid \alpha \in \mathcal{B}_1, \beta \in \mathcal{B}_2\}$ es un sistema de generadores de $\overline{A}$ sobre $\mathbb{F}$ y contiene al sistema libre $\mathcal{B}_2$, con lo que existe una base $\mathcal{B}_0$ de A sobre $\mathbb{F}$ tal que $\mathcal{B}_2 \subseteq \mathcal{B}_0 \subseteq \mathcal{G}$, y se tiene que $\mathcal{B} = \mathcal{B}_0 \setminus \mathcal{B}_2$ es una base de $\overline{A}/A$ sobre $\mathbb{F}$. El problema práctico es cómo calcular $\mathcal{B}$ a partir de $\mathcal{G}$ en un número finito de pasos.

Para ello, en primer lugar basta considerar en $\mathcal{G}$ los elementos de $\mathcal{B}_1$ que no estén en A; además, si cada uno de estos elementos tiene un denominador $b(X)$, basta multiplicarlo por los elementos de $\mathcal{B}_2$ con grado en X estrictamente menor que el grado de $b(X)$, pues el resto son linealmente dependientes sobre $\mathbb{F}$ módulo A de los anteriormente considerados. Ambas observaciones dan lugar a un número finito de elementos a considerar en $\mathcal{G}$ y por tanto nos permiten obtener $\mathcal{B}$ mediante un número finito de comprobaciones.

Por ejemplo, si se considera la curva $Y^9 + X^2Y^2 + X^7$ (en característica cero, por ejemplo), el algoritmo de la base entera nos proporciona una base de $\overline{A}$ como $\mathbb{F}[X]$-módulo de la forma

$$\{1, Y, Y^2, Y^3, \frac{Y^4}{X}, \frac{Y^5}{X}, \frac{Y^6}{X}, \frac{Y^7}{X^2}, \frac{Y\,(X^2+Y^7)}{X^4}\}$$

con lo que, a partir de las observaciones anteriores, se deduce fácilmente que una base de $\overline{A}/A$ como espacio vectorial sería

$$\{\frac{Y^4}{X}, \frac{Y^5}{X}, \frac{Y^6}{X}, \frac{Y^7}{X}, \frac{Y^7}{X^2}, \frac{Y\,(X^2+Y^7)}{X}, \frac{Y\,(X^2+Y^7)}{X^2}, \frac{Y\,(X^2+Y^7)}{X^3}, \frac{Y\,(X^2+Y^7)}{X^4}\}$$

que tiene justamente 9 elementos, puesto que la contribución en el género geométrico del origen de coordenadas, única singularidad en la parte afín, es exactamente de 9 unidades, como puede verse fácilmente a partir del polígono de Newton de la curva entorno al origen.

Por último, en cuanto a la primera etapa haremos uso del teorema de Abhyankar-Moh, basado en el concepto de raíces aproximadas que pasaremos a exponer a continuación.

3.2 Raíces aproximadas

Sea S un anillo, $G \in S[\mathrm{Y}]$ un polinomio mónico de grado e y $F \in S[\mathrm{Y}]$ un polinomio mónico de grado n tal que $e|n$. Si escribimos $n = eb$, podemos efectuar sucesivas divisiones por G empezando con el polinomio F hasta obtener una expresión del tipo

$$F = G^b + \sum_{i=0}^{b-1} C_i G^i$$

donde $C_i \in S[\mathrm{Y}]$ verifica que $deg\, C_i < e$. De hecho, esta expresión es única, y es análoga a la expresión de un número entero en base k, siendo k un entero positivo fijo.

Definición 3.2 *En las condiciones anteriores, al término C_{b-1} se le llama coeficiente de Tschirnhausen de G con respecto a F, lo denotaremos por $C_F(G)$. Si además b es una unidad en S, se define la transformada de Tschirnhausen $\tau_F(G)$ de G con respecto a F mediante la expresión*

$$\tau_F(G) \doteq G + b^{-1} C_F(G)$$

El polinomio $\tau_F(G)$ es obviamente mónico de grado e con coeficientes en S, al igual que G. Por otra parte, si $C_F(G) = 0$ se tiene que $C_F(\tau_F(G)) = 0$; en caso contrario, como $C_{b-1} G^{b-1}$ es el término de mayor grado de $\sum_{i=0}^{b-1} C_i G^i$, se tiene que

$$deg\, C_F(G) = deg\, (F - G^b) - e\, (b-1)$$

Con vistas a iterar el proceso, es conveniente acotar el grado del coeficiente de Tschirnhausen de la transformada $\tau_F(G)$, a fin de asegurar que el proceso sea finito. Dicha acotación viene dada por el siguiente resultado.

Lema 3.2 *Si $C_F(G) \neq 0$, entonces $deg\, C_F(\tau_F(G)) < deg\, (C_F(G))$.*

Demostración:

Escribiendo $H = \tau_F(G) = G + b^{-1} C_F(G)$ se tiene

$$H^b = G^b + C_F(G)\, G^{b-1} + K$$

donde K consiste en los restantes términos del desarrollo del binomio Newton; sea $c \doteq deg\, C_F(G)$. De la definición de $C_F(G)$ se deduce que

$$deg\, K \leq 2c + (b-2)\, e < c + (b-1)\, e$$

Pero $F - H^b = F - G^b - C_F(G)\, G^{b-1} - K = \left(\sum_{i=0}^{b-2} C_i G^i\right) - K$, y además

$$deg\, \left(\sum_{i=0}^{b-2} C_i G^i\right) < b-1)\, e$$

Combinando las dos últimas desigualdades, se tiene que $deg\,(F - H^b) < c + (b-1)\, e$, y como $deg\,(C_F(\tau_F(G))) = deg\,(F - H^b) - (b-1)\, e$ se tiene que $deg\,(C_F(\tau_F(G))) < c = deg\, C_F(G)$, como queríamos demostrar.

□

En consecuencia, si se itera la transformada de Tschirnhausen un número suficiente de veces j (que denotaremos por $(\tau_F)^j(G)$) se tiene evidentemente que $C_F((\tau_F)^j(G)) = 0$ para algún j (por ejemplo si $j \geq e$, aunque eventualmente podemos obtener el resultado para un j más pequeño).

Lema 3.3 *Las condiciones siguientes son equivalentes:*

a) $deg\,(F - G^b) < n - e = e\,(b-1)$.

b) $C_F(G) = 0$.

Demostración:

Si $C_F(G) \neq 0$, como $deg\, C_F(G) = deg\,(F - G^b) - (b-1)\, e$ se tiene que $deg\,(F - G^b) \geq n - e = e\,(b-1)$. Recíprocamente, si $C_F(G) = 0$, entonces $F - G^b = \sum_{i=0}^{b-2} C_i G^i$, y como $deg\, \left(\sum_{i=0}^{b-2} C_i G^i\right) < b-1)\, e$ se deduce el resultado.

□

Definición 3.3 *Se dice que G es una raíz aproximada b-ésima de F si verifica cualquiera de las dos condiciones equivalentes del lema anterior.*

Dicho de otra manera, la raíz aproximada b-ésima de F es la mejor solución polinómica posible de la ecuación $F = G^b$, en el sentido de que minimiza el grado de la diferencia $F - G^b$. Como consecuencia de todo lo anterior es muy fácil probar el siguiente resultado, que es fundamental en la teoría de raíces aproximadas de polinomios.

Proposición 3.1 *Sea $F \in S[\mathrm{Y}]$ un polinomio mónico de grado n y sea b un divisor de n que sea inversible en S; entonces existe una única raíz aproximada b-ésima de F.*

Demostración:

Para probar la existencia, es suficiente con iterar la transformada de Tschirnhausen $(\tau_F)^j(G)$ de G con respecto de F un número suficiente de veces hasta que $C_F((\tau_F)^j(G)) = 0$, como ya hemos visto anteriormente.

En cuanto a la unicidad, si G, H son dos raíces aproximadas b-ésimas de F, puesto que $deg\,(F - G^b) < n - e$ y $deg\,(F - H^b) < n - e$ se tiene que $deg\,(G^b - H^b) < n - e$. Por otro lado, como

$$G^b - H^b = (G - H) \sum_{i+j=b-1} G^i H^j$$

y el segundo factor tiene grado $e(b-1) = n-e$, se tiene que $deg\,(G-H) < 0$ y en consecuencia $G = H$.

□

Nota 3.1 *Nótese que, debido a la unicidad del teorema anterior y a la independencia de la raíz aproximada b-ésima del anillo de coeficientes, si $S \hookrightarrow S'$, $F \in S[\mathrm{Y}]$ y $G \in S'[\mathrm{Y}]$ es la raíz aproximada b-ésima de $F \in S'[\mathrm{Y}]$, se tiene de hecho que $G \in S[\mathrm{Y}]$.*

Nota 3.2 *Aplicando también la unicidad del teorema anterior, si H, G, F son polinomios mónicos en $S[\mathrm{Y}]$ de grados c, cb, cbe respectivamente y b, e son inversibles en S, se tiene que si H es la raíz aproximada b-ésima de G y G es la raíz aproximada e-ésima de F, entonces H es la raíz aproximada be-ésima de F.*

En cuanto al *cálculo efectivo de raíces aproximadas*, tenemos en principio la opción teórica de iterar la transformada de Tschirnhausen, tomando inicialmente un polinomio mónico arbitrario G del grado adecuado, puesto que al final estamos seguros de obtener la raíz aproximada que buscamos y ésta es única; no obstante, hay un método mucho más rápido para obtener dicha raíz, que describiremos a continuación.

Dado F un polinomio mónico de grado n, y dado b un divisor de n, escribimos un polinomio G mónico de grado n/b por coeficientes indeterminados; si efectuamos la operación $H = F - G^b$, para imponer a G que sea la raíz aproximada b-ésima de F no hay más que obligar a H a que tenga grado estrictamente menor que $n - e$, con $e = n/b$, según uno de los lemas precedentes. En consecuencia, basta con ir igualando a 0 los monomios de $F - G^b$ de grado más alto, con lo que el problema queda reducido a resolver un sistema no lineal de e ecuaciones con e indeterminadas, triangular y con unos en la diagonal. De forma más precisa, si éste se resuelve empezando por el término de grado más alto $n - 1$ y descendiendo progresivamente grado a grado, en cada etapa aparece un incógnita nueva, y la ecuación que hay que resolver en dicha etapa es lineal en la nueva incógnita, llevando ésta un 1 como coeficiente. En conclusión, el sistema tiene una única solución (como ya sabíamos), y es fácil ver que su resolución tiene una complejidad semejante a la del método de eliminación Gaussiana.

Por ejemplo, si se considera el polinomio $F = \mathrm{Y}^9 + \mathrm{Y}^7 + \mathrm{X}\mathrm{Y}^4 + \mathrm{Y}^2 + \mathrm{X} + 1$ definido sobre el cuerpo finito $\mathbb{F}_2$, vamos a calcular su raíz cúbica aproximada, que será de la forma $G = \mathrm{Y}^3 + A\,\mathrm{Y}^2 + B\,\mathrm{Y} + C$, donde A, B, C son coeficientes indeterminados con valores en $\mathbb{F}_2[\mathrm{X}]$. Se calcula el polinomio

$$H = F - G^3 = A\,\mathrm{Y}^8 + (1 + A^2 + B)\,\mathrm{Y}^7 + (A^3 + C)\,\mathrm{Y}^6 + \ldots$$

y se igualan a cero los coeficientes de grado mayor o igual a $n - e = 9 - 3 = 6$, obteniéndose el sistema

$$\left\{\begin{array}{rcrcrcl} A & & & & & = & 0 \\ A^2 & + & B & & & = & 1 \\ A^3 & & & + & C & = & 0 \end{array}\right.$$

cuya solución es $A = 0$, $B = 1$ y $C = 0$, y por tanto la raíz cúbica aproximada de F es $G = \mathrm{Y}^3 + \mathrm{Y}$.

3.3 Teorema de Abhyankar-Moh

En esta sección nos ocuparemos del resultado fundamental del presente capítulo, debido a S.S. Abhyankar y T.T. Moh, y que nos proporciona un conjunto de generadores para el semigrupo S_P con buenas propiedades aritméticas, junto con funciones en el anillo A cuyos polos en P tienen orden igual a dichos generadores. Dichos generadores y las correspondientes funciones pueden ser calculados de manera algorítmica, y las propiedades aritméticas de los generadores nos permiten de hecho calcular una función en A con un polo en P de orden igual a cualquiera de los elementos del semigrupo S_P.

Teorema 3.1 (Abhyankar-Moh) *En las mismas condiciones y notaciones que en la sección 3.1 , supongamos que char* $\mathbb{F}$ *no divide simultáneamente a* $\deg \chi$ *y a* $e_P(\chi)$*; entonces existen un entero* h *y una sucesión de enteros* $\delta_0, \ldots, \delta_h \in S_P$ *que generan* S_P *tales que:*

(I) $d_{h+1} = 1$ *y* $n_i > 1$ *para* $2 \leq i \leq h$*, donde* $d_i \doteq m\,c\,d\ (\delta_0, \ldots, \delta_{i-1})$ *para* $1 \leq i \leq h+1$ *y* $n_i \doteq d_i/d_{i+1}$ *para* $1 \leq i \leq h$*.*

(II) $n_i\delta_i$ *pertenece al semigrupo generado por* $\delta_0, \ldots, \delta_{i-1}$ *para* $1 \leq i \leq h$*.*

(III) $n_i\delta_i > \delta_{i+1}$ *para* $1 \leq i \leq h-1$*.*

Demostración:

A continuación esbozaremos los pasos de la demostración de este resultado; para más detalles, ver Abhyankar [1] o Pinkham [86].

Etapa 1. Sean $p = char\,\mathbb{F}$, X e Y las coordenadas afines en el plano, y sean x, y sus correspondientes imágenes en A; sean $m = -v_{\overline{P}}(x)$ y $n = -v_{\overline{P}}(y)$ (es decir, respectivamente el grado en Y y el grado en X de la ecuación de la curva plana). Puesto que la curva tiene una sola rama racional en el infinito y ésta está definida sobre el cuerpo base $\mathbb{F}$, se puede suponer (salvo un cambio lineal de coordenadas) que el grado de la curva es m, con lo que el polinomio $F(\mathrm{X}, \mathrm{Y})$ que define la ecuación de C es mónico en la variable Y, y tiene a Y^m como monomio de grado más alto; en particular, se tiene $n < m$.

Si aún fuese necesario, haciendo un cambio de coordenadas de la forma $(\mathrm{X},\mathrm{Y}) \mapsto (\mathrm{X}+P(\mathrm{Y}),\mathrm{Y})$ podemos obviamente suponer que m no es múltiplo de p, por las hipótesis sobre la característica (nótese que m es el grado de la curva χ, y que n es m menos la multiplicidad del punto del infinito).

Con el fin de trabajar localmente en el único punto del infinito, consideramos a continuación el cambio de variables

$$\mathrm{X} = \frac{1}{\mathrm{U}}, \mathrm{Y} = \frac{\mathrm{W}}{\mathrm{U}}$$

que nos proporciona coordenadas U,W en una nueva carta afín de la curva, en la cual el punto P es el origen de coordenadas y la curva χ está dada por el polinomio

$$H(\mathrm{U},\mathrm{W}) = \mathrm{U}^m F(\frac{1}{\mathrm{U}}, \frac{\mathrm{W}}{\mathrm{U}})$$

Etapa 2. Por las hipótesis en el infinito, la curva afín $H = 0$ tiene una única rama racional en el origen y dicha rama está definida sobre $\mathbb{F}$, es decir, admite una parametrización del tipo $u = u(t)\,,\ w = w(t)$ donde $u(t), w(t)$ son series de potencias formales inversibles en $\mathbb{F}[[t]]$. De hecho, como p no divide a m y se tiene que $ord_t u(t) = m$, el parámetro t puede elegirse de forma que $u(t) = c\,t^m \ \ ,\ \ w(t) = \sum_{i \geq m-n} a_i t^i$, donde $c, a_i \in \mathbb{F}$ y $c \neq 0$.

Utilizando esta parametrización, podemos calcular la sucesión característica $(\beta_0, \ldots, \beta_h)$ del anillo local R de la curva $H = 0$ en el origen, y se define $z_e \doteq \sum_{0<i<\beta_e} a_i t^i$ para $1 \leq i \leq h$.

Si se toma $g_e \in \mathbb{F}((t^m))[\mathrm{W}]$ el polinomio mínimo de z_e sobre $\mathbb{F}((t^m))$, se tiene que los enteros $r_0 \doteq m$ y $r_e \doteq \upsilon(g_e)$ satisfacen las propiedades (I) y (II), pero se tiene que $n_i r_i < r_{i+1}$ en lugar de la propiedad (III). En realidad, la propiedad que se necesita de g_e es que defina un germen que tenga contacto maximal de género $e-1$ con la curva χ en P (ver Campillo [16]). Existen muchas curvas con esta propiedad y, salvo truncación, podríamos suponer que los gérmenes son de curvas algebraicas, es decir, que g_e es un polinomio. En todo caso, veremos

que podemos conseguir esto último, es decir, cambiar $g_e \in \mathbb{F}((\mathrm{U}))[\mathrm{W}]$ por un polinomio en las variables X, Y, mediante otro camino que nos será de gran utilidad práctica.

Etapa 3. Deshaciendo ahora el cambio de variables en los g_j, obtenemos $F_1, \ldots, F_h, F_{h+1} = F$, que son elementos de $\mathbb{F}((\mathrm{X}))[\mathrm{Y}]$, con la propiedad de que F_i es mónico de grado m/d_i en la variable Y y que $\upsilon(f_i) = r_i - \dfrac{m^2}{d_i} \doteq s_i$, donde f_i denota la clase de F_i en $\mathbb{F}((\mathrm{X}))[\mathrm{Y}]/(F)$.

Es fácil ver que $d_i = m\,c\,d\,(m, s_1, \ldots, s_{i-1})$ y que $d_{h+1} = 1$, en consecuencia se puede comprobar que los valores $\delta_i = -s_i$ son los generadores con las propiedades requeridas en el enunciado.

Etapa 4. Para transformar F_i en polinomios, utilizaremos la teoría de raíces aproximadas de la sección anterior. La última función $F_{h+1} = F \in \mathbb{F}[\mathrm{X}, \mathrm{Y}]$ es en realidad un polinomio; por inducción, supongamos que hemos obtenido polinomios $F_{e+1}, \ldots, F_{h+1}$ con los mismos grados en Y y los mismos valores en el infinito que los obtenidos en la etapa 3.

Entonces se cambia la función F_e por la n_e-ésima raíz aproximada de F_{e+1} ($n_e \doteq d_e/d_{e+1}$), con lo que el grado en Y no cambia, y el nuevo F_e es un polinomio en X, Y, utilizando la nota 3.2.1 con $S = \mathbb{F}[\mathrm{X}]$ y $S' = \mathbb{F}((\mathrm{X}))$.

De hecho tampoco cambia el valor en el infinito, pues al hacer la transformada de Tschirnhausen de F_e con respecto a F_{e+1}, utilizando las propiedades aritméticas de los n_e se puede probar que

$$\upsilon(C_{n_e-1}F_e^{n_e-1}) > \upsilon(F_e^{n_e}) = n_e\upsilon(F_e)$$

y en consecuencia $\upsilon(C_{n_e-1}) > \upsilon(F_e)$; de esta manera, esta desigualdad se mantiene al iterar la transformada de Tschirnhausen y por tanto sigue siendo cierta para la correspondiente raíz aproximada. El resultado final obtenido es un conjunto de funciones polinómicas que alcanzan los valores de los generadores del semigrupo obtenidos en la etapa 3.

□

Nota 3.3 *Nótese que la restricción sobre la característica de* $\mathbb{F}$ *es necesaria, puesto que si sobre* $\mathbb{F}_2$ *se considera la curva plana definida por la ecuación*

$$\mathrm{Y}^8 + \mathrm{Y} = \mathrm{X}^2(\mathrm{X}^8 + \mathrm{X})$$

se tiene que el semigrupo de Weierstrass en la única rama racional P *en el infinito (que está definida sobre* $\mathbb{F}$*) es igual a* S_P*, al no tener la curva ninguna singularidad a distancia afín; ahora bien, dicho semigrupo está generado por los elementos* $\{8, 10, 12, 13\}$*, y en consecuencia no admite ningún sistema de generadores con las propiedades del teorema de Abhyankar-Moh. Este ejemplo da una respuesta negativa a una cuestión planteada por Sathaye en [96] en la que se pregunta si, además de en característica nula,* S_P *es siempre un semigrupo generado por una sucesión de elementos con las citadas propiedades. Por lo tanto, la descripción general del semigrupo* S_P *en términos de un sistema de generadores con buenas propiedades aritméticas es aún un problema abierto cuando* $p|deg\,\chi$ *y* $p|e_P(\chi)$*.*

Nótese también que el semigrupo S_P *en el ejemplo, si bien no satisface las propiedades del teorema de Abhyankar-Moh, sí que tiene propiedades aritméticas buenas; por ejemplo es un semigrupo intersección completa, es decir, el álgebra del semigrupo* $k[S_P] = k[t^8, t^{10}, t^{12}, t^{13}]$ *es una* k*-álgebra intersección completa (puesto que el núcleo de la correspondiente aplicación* $k[\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3, \mathrm{X}_4] \to k[S_P]$ *está generado por los elementos* $\mathrm{X}_2^2 - \mathrm{X}_1\mathrm{X}_3$*,* $\mathrm{X}_3^2 - \mathrm{X}_1^3$ *y* $\mathrm{X}_4^2 - \mathrm{X}_1^2\mathrm{X}_2$*), siendo en este caso* $k = \mathbb{F}_2$ *. Por otro lado,* S_P *es siempre un semigrupo simétrico, es decir, simétrico respecto de* $c-1$*, donde* $c = 2g = 28$ *es el conductor del semigrupo.*

El ejemplo propuesto proviene en realidad de la teoría de códigos álgebro-geométricos (ver Hansen-Stichtenoth [52] o Høholdt-Pellikaan [57]), y la razón por la que falla el teorema de Abhyankar-Moh es que tanto el grado de la curva como la multiplicidad del punto del infinito son múltiplos de 2*, que es la característica del cuerpo de definición de la curva.*

Nota 3.4 *Nótese también que, de hecho, se tiene que* $\delta_0 > \delta_1$ *, y que en la práctica se puede suponer que* p *no divide a* δ_0 *. Los semigrupos generados por sucesiones numéricas con las propiedades (I), (II) y (III) del teorema 3.1 son llamados telescópicos por algunos autores (ver Kirfel-Pellikaan [65]); tales semigrupos son de hecho simétricos.*

3.4 Algoritmo de raíces aproximadas

Todos los polinomios F_e que se van obteniendo en la demostración del teorema de Abhyankar-Moh son, de hecho, raíces aproximadas de la ecuación de la curva plana F, como consecuencia de la nota 3.2.2 . De esta manera, el algoritmo para describir el semigrupo S_P con sus correspondientes funciones tratará de encontrar raíces aproximadas de F de ciertos órdenes apropiados.

Por otra parte, se puede utilizar una parametrización de la rama del infinito para calcular el semigrupo S_P y sus correspondientes funciones directamente de la ecuación de la curva, pero podemos evitar el cálculo de dichas ecuaciones paramétricas para evitar el incremento excesivo de la complejidad. La parametrización racional de la rama del infinito, que puede calcularse por ejemplo mediante las expresiones simbólicas de Hamburger-Noether del apartado 2.7 , nos permite calcular valores en el punto del infinito con bastante facilidad, si bien nos resultará útil que éstos puedan calcularse de forma alternativa mediante el uso resultantes, tal y como se mostrará más adelante. De hecho, las expresiones simbólicas de Hamburger-Noether nos permiten también hallar el semigrupo, que se calcularía en el marco de la aritmética a partir de tales expresiones (ver Campillo [16]). Esto nos permitiría conseguir la etapa 2 de la demostración del teorema de Abhyankar-Moh, pero sería necesario aún llegar hasta la etapa 4 en la demostración de dicho teorema.

Con el fin de describir con precisión el citado algoritmo, recordaremos un resultado también probado por Abhyankar que nos proporciona un criterio para saber si una curva con un solo punto (racional) en el infinito tiene o no una sola rama racional (definida sobre $\mathbb{F}$) en dicho punto, en cuyo caso se tiene, en particular, una condición suficiente de irreducibilidad absoluta; dicho criterio utiliza de hecho el algoritmo que nos interesa, y que describimos a continuación.

3.4.1 Descripción del algoritmo

Sea χ un modelo afín plano para una curva dado por la ecuación

$$F = F(\mathrm{X}, \mathrm{Y}) = \mathrm{Y}^m + a_1(\mathrm{X})\,\mathrm{Y}^{m-1} + \ldots + a_m(\mathrm{X})$$

y supongamos que m es el grado total de F. Nótese que bajo las hipótesis del teorema de Abhyankar-Moh podemos suponer que m no es múltiplo de

la característica de $\mathbb{F}$, pues en caso contrario podemos hacer un cambio de coordenadas de la forma $(\mathrm{X}, \mathrm{Y}) \mapsto (\mathrm{X} + \mathrm{Y}^l, \mathrm{Y})$, eligiendo el l apropiado a tal fin, al ser la curva obtenida birracionalmente equivalente a la dada y no modificarse los semigrupos de valores en el infinito. Denotemos la raíz aproximada d-ésima de F por $app(d, F)$.

El **algoritmo de raíces aproximadas** funciona de la manera siguiente (como el caso en que Y divide a F es trivial, supondremos lo contrario):

$$F_0 = \mathrm{X}\,,\ \delta_0 = d_1 = m\,,\ F_1 = \mathrm{Y}\,,\ \delta_1 = deg_{\mathrm{X}} Res_{\mathrm{Y}}(F, F_1)$$

$$\left[\begin{array}{lcl} d_n & = & m\,c\,d\,(\delta_0, \delta_1, \ldots, \delta_{n-1}) \\ F_n & = & app(d_n, F) \\ \delta_n & = & deg_{\mathrm{X}} Res_{\mathrm{Y}}(F, F_n) \end{array}\right.$$

y se continúa de forma inductiva. Por convenio, se escribe

$$deg_{\mathrm{X}} Res_{\mathrm{Y}}(F, F_i) = -\infty \ \text{ si } \ Res_{\mathrm{Y}}(F, F_i) = 0$$

y

$$m\,c\,d\,(\delta_0, \delta_1, \ldots, \delta_i) = m\,c\,d\,(\delta_0, \delta_1, \ldots, \delta_j)$$

si $\delta_0, \delta_1, \ldots, \delta_j$ son números enteros, $j < i$ y $\delta_{j+1} = \delta_{j+2} = \ldots = \delta_i = -\infty$.

Con las mismas notaciones, puesto que $\{d_n\}_{n \geq 2}$ es una sucesión decreciente de enteros positivos, existe un único entero positivo h tal que $d_2 > d_3 > \ldots > d_{h+1} = d_{h+2}$; de esta manera, estamos en condiciones de establecer el resultado siguiente, cuya demostración se remite a Abhyankar [3].

Teorema 3.2 (Criterio para una sola rama en el infinito) *La curva χ tiene una sola rama racional (definida sobre $\mathbb{F}$) en el infinito si y sólo si $d_{h+1} = 1$, $\delta_1 d_1 > \delta_2 d_2 > \ldots > \delta_h d_h$ y $n_i \delta_i$ pertenece al semigrupo generado por $\delta_0, \delta_1, \ldots, \delta_{i-1}$ para $1 \geq i \geq h$, donde $n_i \doteq d_i / d_{i+1}$ también para $1 \geq i \geq h$.*

Nótese que las propiedades anteriores son exactamente las dadas por el enunciado del teorema de Abhyankar-Moh; de hecho, los elementos δ_i calculados por el algoritmo anterior son los generadores del semigrupo S_P que da dicho teorema, como lo muestra el siguiente resultado (ver Abhyankar [1] para más detalles).

Lema 3.4 *En las condiciones del teorema de Abhyankar-Moh, y con la misma notación que en la etapa 2 de la demostración de dicho teorema, para* $1 \leq e \leq h$ *se tiene que*

$$\delta_e = I_P(F, F_e) = ord_t F_e(ct^m, \omega(t)) = deg_{\mathrm{X}} Res_{\mathrm{Y}}(F, F_e)$$

donde $F_e = app(d_e, F)$.

En definitiva, cada uno de los generadores del semigrupo S_P calculados por el teorema de Abhyankar-Moh es en realidad el orden de contacto de la curva F con la raíz aproximada correspondiente al máximo común divisor de los anteriores generadores, con lo que éstos pueden calcularse inductivamente por medio de resultantes de polinomios, según el procedimiento indicado en el algoritmo anterior.

De esta manera, el algoritmo de raíces aproximadas calcula a la vez los generadores que da el teorema de Abhyankar-Moh y las funciones que alcanzan estos valores de una manera efectiva. Es más, si el algoritmo consigue llegar con éxito hasta el final, estaremos seguros (si es que aún no lo sabíamos) que sólo hay una rama racional que está definida sobre $\mathbb{F}$ en P y en consecuencia la curva es (absolutamente) irreducible, cosa de gran interés en la teoría de códigos álgebro-geométricos. En caso contrario (es decir, cuando las condiciones requeridas en el criterio anterior no se cumplan en cualquiera de los pasos del algoritmo) podemos concluir que la curva tiene más de una rama en el punto P. El caso de una singularidad con varias ramas es mucho más difícil de estudiar, si bien el algoritmo de raíces aproximadas proporciona alguna información sobre dicha singularidad (ver [27]).

Nótese que hay dos caminos alternativos para disminuir la complejidad del algoritmo descrito:

(i) En caso de conocer de alguna manera una parametrización de la singularidad de la rama en P, podríamos usarla para calcular con más rapidez órdenes de contacto en P (es decir, valores de funciones en el punto del infinito) en lugar de usar resultantes de polinomios.

Esta alternativa se puede hacer efectiva si a priori se calcula la correspondiente expresión simbólica de Hamburger-Noether y después se usa como parametrización mediante evaluación perezosa. Nótese que el algoritmo descrito en la sección 2.7 da también en la práctica otra condición suficiente de irreducibilidad.

(ii) En vez de utilizar curvas definidas por una ecuación dada, podríamos proceder fijando previamente un semigrupo descrito en la forma del teorema de Abhyankar-Moh e intentar entonces encontrar una curva plana F con una sola rama en el infinito realizando el semigrupo prefijado en el punto del infinito, incluso en el caso en que p divida a $m\,c\,d\,(\delta_0, \delta_1)$.

Esto último es el proceso inverso al que hemos expuesto en el presente capítulo, es decir, dados números $\delta_0, \delta_1, \ldots, \delta_h$ con las propiedades (I), (II), y (III) del teorema de Abhyankar-Moh, entonces se pueden construir de forma recurrente sucesiones de polinomios llamados *aproximantes* de un polinomio F tales que $F = 0$ es una curva con una única rama P en el infinito y semigrupo S_P generado por $\delta_0, \delta_1, \ldots, \delta_h$ (resultado probado por Reguera en [90], en donde se pueden comprobar más detalles). Esta vía tiene la ventaja de que se pueden construir directamente los ejemplos junto con las funciones (los aproximantes) asociados a los generadores de un semigrupo S_P prefijado. Además, Reguera construye tales ejemplos satisfaciendo las condiciones de Abhyankar-Moh sin la restricción aritmética sobre la característica que aparece en dicho teorema.

Ejemplo 3.1 *Consideramos curva plana afín* $\mathrm{Y}^8 + \mathrm{Y}^2 + \mathrm{X}^3 = 0$ *definida sobre* $\mathbb{F}_2$*, con sólo un punto* $P = (1 : 0 : 0)$ *en el infinito. El grado de la curva es múltiplo de la característica, así que se necesita efectuar el cambio de variables* $\mathrm{X} = \mathrm{X} + \mathrm{Y}^3$*,* $\mathrm{Y} = \mathrm{Y}$ *para obtener el modelo plano* $F(\mathrm{X}, \mathrm{Y}) = \mathrm{Y}^9 + \mathrm{Y}^8 + \mathrm{XY}^6 + \mathrm{X}^2\mathrm{Y}^3 + \mathrm{Y}^2 + \mathrm{X}^3$ *y poder aplicar el algoritmo de raíces aproximadas a* F*:*

$$F_0 = \mathrm{X}\,,\ \delta_0 = d_1 = 9\,,\ F_1 = \mathrm{Y}$$

$$\delta_1 = deg_{\mathrm{X}} Res_{\mathrm{Y}}(F, \mathrm{Y}) = 3\,,\ d_2 = m\,c\,d\,(9, 3) = 3$$

$$F_2 = app(3, F) = \mathrm{Y}^3 + \mathrm{Y}^2 + \mathrm{Y} + \mathrm{X} + 1$$

$$\delta_2 = deg_{\mathrm{X}} Res_{\mathrm{Y}}(F, F_2) = 8\,,\ d_3 = m\,c\,d\,(9, 3, 8) = 1$$

así $h = 2$ *y* $S_P = \langle 9, 3, 8\rangle$*. En consecuencia, existe una sola rama en el infinito puesto que las propiedades (I), (II) y (III) del teorema de Abhyankar-Moh se verifican para la sucesión obtenida.*

Por otro lado, con las mismas notaciones que en el lema 3.1 , se toma una base sobre $\mathbb{F}_2$ de $\overline{A}/A$, como por ejemplo:

$$h_1 = \frac{\mathrm{Y}(1+\mathrm{Y}^6)}{\mathrm{X}+\mathrm{Y}^3} \quad h_2 = \frac{\mathrm{Y}(1+\mathrm{Y}^6)}{(\mathrm{X}+\mathrm{Y}^3)(\mathrm{Y}^2+\mathrm{Y}+1)}$$

$$h_3 = \frac{\mathrm{X}^2+\mathrm{Y}^6}{\mathrm{Y}^2+\mathrm{Y}+1} \quad h_4 = \frac{\mathrm{Y}^2(1+\mathrm{Y}^3)(\mathrm{Y}^2+\mathrm{Y}+1)}{\mathrm{X}+\mathrm{Y}^3}$$

Los valores de estas funciones (obtenidos mediante resultantes) son $-\upsilon_P(h_1) = 13 \notin S_P$, $-\upsilon_P(h_2) = 7 \notin \Gamma_P^1$, $-\upsilon_P(h_3) = 10 \notin \Gamma_P^2$ y $-\upsilon_P(h_4) = 13 \in \Gamma_P^3$. Cambiamos por tanto h_4 por

$$g_4 = h_4 + h_1 = \frac{\mathrm{Y}(1+\mathrm{Y}^3)(\mathrm{Y}^2+\mathrm{Y}+1)}{\mathrm{X}+\mathrm{Y}^3}$$

y ahora $-\upsilon_P(g_4) = 10 \in \Gamma_P^3$, con lo que aún se tiene que considerar la función

$$g_4 = h_4 + h_1 + h_3 = \frac{\mathrm{Y}(1+\mathrm{Y}^3)(\mathrm{Y}^4+\mathrm{Y}^2+1) + (\mathrm{X}+\mathrm{Y}^3)^3}{(\mathrm{X}+\mathrm{Y}^3)(\mathrm{Y}^2+\mathrm{Y}+1)}$$

obteniéndose $-\upsilon_P(g_4) = 4 \notin \Gamma_P^3$. En consecuencia, el semigrupo de Weierstrass en P es

$$\Gamma_P = \{0, 3, \mathbf{4}, 6, \mathbf{7}, 8, 9, \mathbf{10}, 11, 12, \mathbf{13}, 14, \ldots\}$$

y en particular se obtiene que el género de la curva es $g = 3$.

□

3.4.2 Cálculo de una base para $\mathcal{L}(lP)$

Mostraremos ahora cómo calcular una base para el espacio vectorial $\mathcal{L}(lP)$ para cualquier $l \in \Gamma_P$ a partir de los resultados anteriores. Sobre el anillo afín $\overline{A}$ se puede dar una filtración de la siguiente manera:

$$\mathbb{F} = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \ldots \subseteq \overline{A}$$

Obviamente se tiene que $\overline{A} = \bigcup_{l=0}^{\infty} \mathcal{L}(lP)$ y es de hecho una $\mathbb{F}$-álgebra graduada de la forma

$$\overline{A} = \bigoplus_{l=0}^{\infty} \frac{\mathcal{L}(lP)}{\mathcal{L}((l-1)P)}$$

que es isomorfa al álgebra de semigrupo $\mathbb{F}[\Gamma_P]$ debido a la desigualdad $0 \leq dim_{\mathbb{F}} \frac{\mathcal{L}(lP)}{\mathcal{L}((l-1)P)} \leq 1$.

Partiendo de este hecho, con el fin de calcular una base de $\mathcal{L}(lP)$ para cualquier entero no negativo l, lo único que se necesita es encontrar una función que tenga un único polo en P de orden n, para cada $0 \leq n \leq l$ tal que $n \in \Gamma_P$; esto puede hacerse fácilmente a partir de los resultados del presente capítulo, en la manera que se expone a continuación.

Si $n \in S_P$, n puede escribirse fácilmente de manera única en términos de los generadores del teorema de Abhyankar-Moh en la forma

$$n = \sum_{i=0}^{h} \lambda_i \delta_i$$

con $\lambda_0 \geq 0$ y $0 \leq \lambda_i < n_i$ para $1 \leq i \leq h$ (ver Kirfel-Pellikaan [65] o Pinkham [86]); así, si $\upsilon_P(f_i) = -\delta_i$, entonces $f_n = \prod_{i=0}^{h} f_i^{\lambda_i}$ tiene un único polo en P de orden n. En caso contrario, si $n \in \Gamma_P \setminus S_P$ las funciones pueden construirse a partir de una base de $\overline{A}/A$ sobre $\mathbb{F}$ mediante el algoritmo de triangulación mostrado en el lema 3.1 .

3.5 Construcción de modelos planos con una sola rama en el infinito

En esta sección expondremos con más detalle el proceso inverso al algoritmo de raíces aproximadas, es decir, la construcción explícita de curvas con una sola rama en el infinito cuyo semigrupo S_P en dicha rama es un semigrupo telescópico Γ prefijado, tal y como se dijo en la sección anterior. Para ello, introduciremos en primer lugar las herramientas y conceptos básicos que se utilizarán posteriormente en la construcción de dichas curvas.

3.5.1 Teoría de aproximantes

Recordemos en primer lugar la definición del polígono de Newton de una curva en el entorno de un punto, tal y como fue dada en la sección 2.7 . Sea $\mathbb{F}$ un cuerpo perfecto, y sea $f(\mathrm{U},\mathrm{V}) = \sum_{\alpha,\beta\geq 0} c_{\alpha\beta}\mathrm{U}^{\alpha}\mathrm{V}^{\beta}$ un polinomio en $\mathbb{F}[\mathrm{U},\mathrm{V}]$ que define un germen de curva en el origen de coordenadas $P = (0,0)$; supongamos que en dicho punto sólo existe una rama racional sobre $\mathbb{F}$, y que dicha rama es un punto racional sobre $\mathbb{F}$ (como punto de la normalización). Lo que sigue es una precisión del algoritmo que calcula las expresiones simbólicas de Hamburger-Noether y puede encontrarse en [90]. Se considera el diagrama de Newton de f

$$D(f) \doteq \{(\alpha,\beta) \mid c_{\alpha\beta} \neq 0\}$$

y se denomina *polígono de Newton* de f (en el origen) al conjunto de los segmentos acotados de la frontera del cierre convexo de $D(f) + \mathbb{R}_+^2$, y será denotado por $P(f)$. Suponiendo que $v(\mathrm{U}) < v(\mathrm{V})$, donde v es la valoración natural asociada a la rama de f en el origen, debe ocurrir una de las dos situaciones siguientes:

(A) $P(f)$ consta sólo del punto $(0,1)$, si $v(\mathrm{V}) = \infty$.

(B) $P(f)$ es el segmento de vértices $(l,0)$ y $(0,n)$, si $v(\mathrm{V}) < \infty$.

En el caso (A) no hay nada que hacer y el proceso que describiremos a continuación se termina. En el caso (B) pueden darse a su vez dos posibilidades:

(B1) $l = ne$ para cierto entero positivo e; entonces existen $a, \lambda \in \mathbb{F}^*$ tales que

$$\sum_{(\alpha,\beta)\in P(f)} c_{\alpha\beta}\mathrm{U}^{\alpha}\mathrm{V}^{\beta} = a\,(\mathrm{V} - \lambda\mathrm{U}^{e})^{n}$$

De esta manera, mediante el cambio de variables $\mathrm{U}' = \mathrm{U}$, $\mathrm{V}' = \mathrm{V} - \lambda\,(\mathrm{U}')^{e}$ el polígono de Newton se transforma en el segmento de extremos $(l',0)$ y $(0,n)$ con $l' > l$; este cambio de coordenadas se denomina *transformación de tipo* $B1$, y está unívocamente determinado por al ecuación de f.

(B2) En caso contrario, sea $e_1 = m\,c\,d\,(l,n) < n$, y sea (σ,τ) la única solución entera de la ecuación

$$|\tau l - \sigma n| = e_1$$

que cumple las condiciones $\sigma,\tau \geq 0$, $2\sigma \leq l/e_1$ y $2\tau \leq n/e_1$; en este caso, se efectúa la transformación $\mathrm{U}' = \mathrm{U}^{n/e_1}\mathrm{V}^{\tau}$, $\mathrm{V}' = \mathrm{U}^{l/e_1}\mathrm{V}^{\sigma}$ (es decir, una sucesión finita de explosiones) y se considera la transformada estricta de f en dicha transformación. De esta manera, el polígono de Newton se transforma en un segmento vertical de extremos $(0,0)$ y $(0,e_1)$. La transformación anterior está también unívocamente determinada por la ecuación de f y se denomina *transformación de tipo* $B2$.

Al ser f irreducible como serie de potencias centrada en el origen (pues sólo hay una rama), siempre que $\upsilon(\mathrm{V}) < \infty$ y $n > 1$ podemos efectuar el siguiente proceso algorítmico:

(a) Mientras n divida a l, hacemos sucesivas transformaciones de tipo $B1$ hasta obtener un polígono de Newton cuyas proyecciones sobre los ejes coordenados sean l_0 y $n = e_0$ tales que $e_0 < l_0$ y $e_1 = m\,c\,d\,(e_0,l_0) < e_0$.

(b) En caso contrario, efectuamos la transformación de tipo $B2$ apropiada tras la cual, siempre que $e_1 > 1$, podemos hacer de nuevo una sucesión de transformaciones de tipo $B1$ hasta conseguir que el nuevo polígono de Newton verifique que $e_2 = m\,c\,d\,(l_1,e_1) < e_1$, y se sigue el proceso.

Puesto que la sucesión e_i es estrictamente decreciente, existirá un entero h tal que $e_h = 1$, con lo que el proceso anterior termina en un número finito de pasos. Al final de este algoritmo, obtenemos h polígonos de Newton $(P_i)_{i=0}^{h-1}$ que son segmentos de vértices $(l_i,0)$ y $(0,e_i)$ verificando:

(i) $m\,c\,d\,(e_i,l_i) < e_i$ para $0 \leq i \leq h-1$.

(ii) $e_{i+1} = m\,c\,d\,(e_i,l_i)$ para $0 \leq i \leq h-1$.

En las condiciones anteriores, se tiene que el semigrupo de valores en el origen P de la curva definida por f está generado por la sucesión $\overline{\beta}_0, \overline{\beta}_1, \ldots, \overline{\beta}_h$

donde $\overline{\beta}_0 = e_0$ y $\overline{\beta}_i = \dfrac{e_0 l_0 + \ldots + e_{i-1} l_{i-1}}{e_{i-1}}$ para $1 \leq i \leq h$ (ver Campillo [16]). Este semigrupo es siempre simétrico en virtud de un teorema de Angermuller [7], y lo que acabamos de exponer significa que dicho semigrupo puede calcularse a partir del polígono de Newton de la rama de f en P.

Recíprocamente, sea χ una curva plana reducida con un solo punto P en el infinito, y sea $f(\mathrm{U}, \mathrm{V})$ una ecuación local de la curva en P; si es posible realizar todos los pasos del algoritmo anterior hasta obtener los polígonos de Newton con las propiedades anteriores, entonces la curva tiene una única rama racional en el punto del infinito y ésta está definida sobre $\mathbb{F}$. Daremos a continuación la definición fundamental que se usará en lo que sigue.

Definición 3.4 *Sea $F(\mathrm{X}, \mathrm{Y})$ un polinomio mónico en la variable Y sobre $\mathbb{F}[\mathrm{X}]$ que define una curva plana χ con una sola rama racional en el infinito que está definida sobre $\mathbb{F}$, y sea υ la valoración natural asociada a dicha rama; sea $f(\mathrm{U}, \mathrm{V})$ una expresión local de la curva en un entorno del punto del infinito ($\mathrm{U} = \mathrm{Y}/\mathrm{X}$ y $\mathrm{V} = 1/\mathrm{X}$) y se considera la sucesión de polígonos de Newton construida mediante el algoritmo anterior. Llamaremos aproximantes de F a toda sucesión de polinomios $g_0(\mathrm{X}, \mathrm{Y}), \ldots, g_{h+1}(\mathrm{X}, \mathrm{Y})$ tales que:*

(i) $g_0(\mathrm{X}, \mathrm{Y}) = \mathrm{X}$.

(ii) $g_i(\mathrm{X}, \mathrm{Y})$ *es un polinomio en la variable* Y *de grado* $\overline{\delta}_0/d_i$ *para* $i = 1, \ldots, h+1$ *, donde*

$$\overline{\delta}_0 = -\upsilon(g_0(\mathrm{X}, \mathrm{Y})) = deg_{\mathrm{Y}} f(\mathrm{X}, \mathrm{Y})$$

$$\overline{\delta}_i = -\upsilon(g_i(\mathrm{X}, \mathrm{Y})) \quad \text{para} \quad i = 1, \ldots, h+1$$

$$d_i = m\,c\,d\,(\overline{\delta}_0, \ldots, \overline{\delta}_{i-1}) \quad \text{para} \quad i = 1, \ldots, h+1$$

(iii) *Para $r = 1, \ldots, h+1$ la sucesión de polígonos de Newton de cada curva $g_r(\mathrm{X}, \mathrm{Y}) = 0$ en la rama del infinito consiste en r segmentos de vértices e_i/d_r y l_i/d_r para $i = 0, \ldots, r-1$ y un último segmento de extremos 1 y γ_r con $\gamma_r > l_r/d_r$, y la sucesión de transformaciones para obtener dichos polígonos son exactamente las mismas que para la curva f; esto significa que g_r tiene contacto maximal de género r con f (más detalles en Campillo [16]).*

En las condiciones del teorema de Abhyankar-Moh, las raíces aproximadas que da dicho teorema son aproximantes para f, según la definición anterior, y su existencia estaría por tanto garantizada. En particular, el concepto de aproximante es más débil que el concepto de raíz aproximada.

3.5.2 Construcción de curvas asociadas a semigrupos

A continuación, fijados un cuerpo $\mathbb{F}$ y un semigrupo $S = \langle \delta_0, \ldots, \delta_h \rangle$ con las propiedades (I), (II) y (III) del teorema de Abhyankar-Moh, expondremos el método de [90] para obtener curvas concretas con una sola rama racional P en el infinito que está definida sobre $\mathbb{F}$, tales que tienen una secuencia de aproximantes y cumplen $S_P = S$.

Puesto que se cumplen las propiedades (I), (II) y (III), para $1 \leq i \leq h$ se tiene que $n_i\delta_i$ puede escribirse de manera única en la forma

$$n_i\delta_i = a_{i,0}\delta_0 + \ldots + a_{i,i-1}\delta_{i-1}$$

con $a_{i,0} \geq 0$ y $0 \leq a_{i,j} < n_j$ para $1 \leq j < i$. Entonces, para cada elección $t_1, \ldots, t_h \in \mathbb{F} \setminus \{0\}$ se definen de manera recurrente los polinomios siguientes:

$$g_0 = \mathrm{X}, \quad g_1 = \mathrm{Y}$$

$$g_{i+1} = g_i^{n_i} - t_i g_0^{a_{i,0}} \cdots g_{i-1}^{a_{i,i-1}} \quad \text{para} \quad 1 \leq i \leq h$$

Para $0 \leq i \leq h$, cada polinomio $g_{i+1} \in \mathbb{F}[\mathrm{X}, \mathrm{Y}]$ verifica que

$$deg\,(g_{i+1}) = deg_{\mathrm{Y}}(g_{i+1}) = \frac{\delta_0}{d_{i+1}}$$

De hecho, para $i \geq 1$ este grado es igual al grado del término $g_i^{n_i}$, puesto que el grado del otro término que aparece en la definición es estrictamente menor que δ_0/d_{i+1}. Además, para $i = 1, \ldots, h$ las curvas dadas por $g_{i+1} = 0$ tienen a P como única rama en el infinito.

Por otro lado, se definen los números

$$\varepsilon_0 = \delta_0 - \delta_1$$

$$\varepsilon_i = \frac{d_i\delta_i - d_{i+1}\delta_{i+1}}{d_{i+1}} \quad \text{para} \quad i = 1, \ldots, h-1$$

y también los números

$$\alpha_1^i(\Gamma) = -\delta_0 \left(\frac{a_{i,0}}{\delta_0} + \frac{a_{i,1}}{d_1} + \ldots + \frac{a_{i,i-1}}{d_{i-1}} - \frac{1}{d_{i+1}} \right)$$

$$\alpha_k^i(\Gamma) = n_{k-1} \left[\varepsilon_{k-2} \left(\frac{a_{i,k-1}}{d_{k-1}} + \ldots + \frac{a_{i,i-1}}{d_{i-1}} - \frac{1}{d_{i+1}} \right) + \alpha_{k-1}^i(\Gamma) \right]$$

para $i = 1, \ldots, h$ y $k = 2, \ldots, i$. Los números $\alpha_k^i = \alpha_k^i(\Gamma)$ son estrictamente positivos para $i = 1, \ldots, h$ y $k = 1, \ldots, i$, y además, se tiene que $\alpha_i^i = \varepsilon_{i-1}/d_{i+1}$.

Con esta notación, si hacemos el cambio de variables anteriormente citado para expresar las curvas $g_i = 0$ en un entorno del punto del infinito P, obtenemos las expresiones siguientes:

$$\tilde{g}_0 = 1, \quad \tilde{g}_1 = \mathrm{U}$$

$$\tilde{g}_2 = \tilde{g}_1^{n_1} - t_1 \mathrm{V}^{\frac{\delta_0}{d_2} - a_{1,0}}$$

$$\tilde{g}_{i+1} = \tilde{g}_i^{n_i} - t_i \tilde{g}_1^{a_{i,1}} \cdots \tilde{g}_{i-1}^{a_{i,i-1}} \mathrm{V}^{\alpha_1^i} \quad \text{para} \quad 2 \leq i \leq h$$

Pues bien, si se efectúa el algoritmo de los polígonos de Newton descrito anteriormente sobre el polinomio $\tilde{f} = \tilde{g}_{h+1}$ y examinamos la sucesión de polígonos obtenida (distinguiendo el caso en que $\delta_0 - \delta_1$ divida a δ_0 o no), se deduce que los polinomios $g_0, g_1, \ldots, g_h$ son aproximantes de $f = g_{h+1}$, con lo que la curva $f = 0$ tiene una sola rama racional $P = (1 : 0 : 0)$ en el infinito que está definida sobre $\mathbb{F}$, en la cual el semigrupo S_P está generado por la sucesión $\delta_0, \ldots, \delta_h$ fijada al principio (más detalles en Reguera [90]). Esta construcción es explícita y resuelve el problema que nos proponíamos en esta sección incluso aunque la característica p de $\mathbb{F}$ divida a $d_2 = m\,c\,d\,(\delta_0, \delta_1)$; las curvas obtenidas tienen, además, una sucesión de aproximantes, que es la generalización de lo que en el teorema de Abhyankar-Moh eran las raíces aproximadas en el caso en que p divida a d_2.

En principio, no se puede asegurar que la curva obtenida sea lisa en la parte afín, con lo que el semigrupo obtenido no es el semigrupo de Weierstrass en P salvo que se añadan condiciones adicionales (ver Reguera [90]). Si esto sucediese, el género de la curva podría calcularse como el número de lagunas de dicho semigrupo, y se tendría una fórmula explícita en términos de los

generadores y sus relaciones; en todo caso, se puede dar una fórmula en la que se incluya además la aportación de las singularidades en la parte afín, obteniéndose como resultado

$$g = \frac{(\delta_0 - 1)(\delta_0 - 2)}{2} - \sum_{Q \in \tilde{\chi}} \delta(Q) =$$

$$= \frac{1}{2}\left[1 - \delta_0 - \delta_1 + d_h\delta_h + \sum_{i=1}^{h-1}(n_i\delta_i - \delta_{i+1})\right] - dim_{\mathbb{F}}(\overline{A}/A)$$

puesto que δ_0 es el grado de la curva χ obtenida (ver [65]).

Ejemplo 3.2 *Fijado el semigrupo telescópico S generado por*

$$\delta_0 = 42, \quad \delta_1 = 30, \quad \delta_2 = 57, \quad \delta_3 = 10$$

nuestro propósito es hallar una curva definida sobre $\mathbb{F}_2$ cuyo semigrupo S_P en el infinito sea S. Para ello, vemos que

$$d_1 = 42, \quad d_2 = 6, \quad d_3 = 3, \quad d_4 = 1$$

$$n_1 = 7, \quad n_2 = 2, \quad n_3 = 3$$

y en particular $h = 3$. Por otra parte, se tiene que

$$n_1\delta_1 = 5\delta_0, \;\; n_2\delta_2 = 2\delta_0 + \delta_1, \;\; n_3\delta_3 = \delta_1$$

con lo que, según el procedimiento descrito en el presente párrafo, la sucesión

$$\begin{cases} g_0 = \mathrm{X} \\ g_1 = \mathrm{Y} \\ g_2 = \mathrm{Y}^7 + \mathrm{X}^5 \\ g_3 = g_2^2 + \mathrm{X}^2\mathrm{Y} \\ g_4 = g_3^3 + \mathrm{Y} \end{cases}$$

constituye una sucesión de aproximantes para la curva plana dada por $f \equiv g_4 = 0$, que es la solución buscada. Nótese que la característica $p = 2$ divide a d_2 , a pesar de lo cual hemos podido construir la curva plana a partir del semigrupo fijado.

3.6 Algoritmo de la base entera

A continuación describiremos brevemente el llamado *algoritmo de la base entera*, debido originalmente a Ford y Zassenhaus, que nos permite obtener con técnicas de *álgebra computacional* una base de $\overline{A}$ como $\mathbb{F}[X]$-módulo, según la notación empleada en la sección 3.1 . Introduciremos para ello una notación muy parecida a la empleada en la tesis de Polemi (ver [87]), y empezaremos recordando conceptos fundamentales de *álgebra conmutativa*.

Un elemento u de un anillo B se llama *nilpotente* si $u^n = 0$ para algún entero positivo n. Se tiene que el conjunto de todos los elementos nilpotentes de un anillo B, denotado por R_B, es un ideal de B y el anillo cociente B/R_B no tiene ningún elemento nilpotente distinto de cero.

Por otro lado, para cualquier ideal I del anillo B se define el *radical* de I como el ideal

$$rad(I) \doteq \{u \in B \mid u^k \in I, \quad \exists k \in \mathbb{Z}\}$$

Nótese que $rad(I)$ es la imagen inversa del conjunto $R_{B/I}$ a través del homomorfismo natural $\phi : B \to B/I$.

Por último, si B es un dominio de integridad se define el *idealizador* (o *conductor*) de un ideal I de B como el conjunto

$$Id(I) \doteq \{u \in Fr(B) \mid u\, I \subseteq I\}$$

donde $Fr(B)$ denota el cuerpo de fracciones de B; dicho de otra manera, $Id(I)$ es el subanillo más grande de $Fr(B)$ en el cual I sigue siendo un ideal. $Id(I)$ también se denota usualmente por $\mathcal{C}(B, I)$.

A continuación pasamos a plantear con precisión el problema que nos interesa resolver. Sea $\mathbb{F}$ un cuerpo perfecto y sea $S = \mathbb{F}[X]$ el anillo de coordenadas de la recta afín; denotemos por $K = \mathbb{F}(X)$ el cuerpo de cocientes de S. Consideremos una extensión finita y separable $L = \mathbb{F}(X, Y)$ de K de grado m como el cuerpo de funciones racionales de la curva afín plana C dada por un polinomio separable y absolutamente irreducible $f(X, Y)$ de grado m sobre el anillo S, y sea $R = \mathbb{F}[X, Y]/(f)$ el anillo de coordenadas afines de la curva C. R es un subanillo del cuerpo de funciones racionales L, es íntegramente cerrado sobre el anillo S y contiene una base de L sobre K; lo que nos interesa en lo que sigue es calcular el cierre íntegro $\overline{R}$ de R en L (nótese que R es A y por tanto $\overline{R}$ es $\overline{A}$ en la notación de la sección 3.1). Llamaremos *base entera* de R a una base de $\overline{R}$ como S-módulo.

Ambos anillos R y $\overline{R}$ son S-módulos libre de rango m, y $\overline{R}$ es, de hecho, el anillo de coordenadas de la parte afín de un modelo no singular $\tilde{C}$ para la curva C, prescindiendo de los puntos que se encuentren en el infinito.

La función Y es entera sobre el anillo S y la suma o producto de elementos enteros sigue siendo entero, con lo que $R \subseteq \overline{\mathbb{F}[\mathrm{X}]}$ y se tiene $\overline{\mathbb{F}[\mathrm{X}]} = \overline{R}$. Por otro lado, el conjunto $\{1, \mathrm{Y}, \ldots, \mathrm{Y}^{m-1}\}$ es una base de R como S-módulo; partiendo de esta aproximación inicial, cada iteración del algoritmo que vamos a describir producirá un S-módulo cada vez más grande hasta que finalmente se obtiene el cierre íntegro $\overline{R}$. Introduciremos a continuación varios conceptos que se utilizarán en el desarrollo de dicho algoritmo.

Definición 3.5 *Sea $\{\omega_i\}_{i=1}^m$ una base de R como S-módulo; se llama discriminante de la base $\{\omega_i\}_{i=1}^m$, y se denota por $Disc(\{\omega_i\})$, al determinante de la matriz $(Tr(\omega_i \cdot \omega_j))_{1 \leq i,j \leq m}$.*

Definición 3.6 *En las mismas condiciones, se llama discriminante de R con respecto a S al ideal principal de S generado por $Disc(\{\omega_i\})$, y se denota por $\delta_{R/S}$.*

Definición 3.7 *Dado un polinomio f en las condiciones anteriores, se define el discriminante de f con respecto a* X *como la resultante $Res_{\mathrm{X}}(f, \dfrac{\partial f}{\partial \mathrm{X}})$, y se denota por D_f, sobreentendiendo la variable* X.

El siguiente resultado es el fundamento teórico del algoritmo que nos interesa, y se deduce fácilmente de resultados elementales de álgebra conmutativa (ver Zariski-Samuel [112]).

Proposición 3.2 *Una extensión de anillos R' de R es íntegramente cerrada si y sólo si el idealizador del radical del discriminante de R' con respecto a R es el anillo R'.*

Basándonos en este resultado podemos describir ya el llamado *algoritmo de la base entera*; este algoritmo termina en un número finito de pasos y tiene complejidad polinomial en el grado m de la curva (más detalles en [87]):

Paso 1: Se parte inicialmente de la base $\{1, \mathrm{Y}, \ldots, \mathrm{Y}^{m-1}\}$ del anillo $R_0 = R$ sobre S, y se toma β un factor irreducible sobre $\mathbb{F}$ del discriminante D_f.

Paso 2: Se calcula una base del radical $rad(\beta R_0)$ sobre S; esto se efectúa calculando una base de la imagen inversa del conjunto de todos los elementos nilpotentes del anillo cociente $R_0/\beta R_0$ a través del homomorfismo natural ϕ de paso al cociente. Considerando una base de este último anillo como $S/\beta S$-módulo libre (en realidad, es un espacio vectorial sobre el cuerpo $S/\beta S$), imponer a una combinación lineal de elementos de dicha base el hecho ser un elemento nilpotente consiste en resolver un sistema lineal de ecuaciones de dimensión m, donde m es el grado de la curva.

Paso 3: Se calcula una base del idealizador $R_1 = Id(rad(\beta R_0))$; para imponer a los elementos del cuerpo de cocientes $Fr(R_0)$ que estén en R_1 no tenemos más que establecer m condiciones de tipo lineal, siendo m el grado de la curva.

Paso 4: Se calcula la dimensión $dim_{\mathbb{F}} R_1/R_0$; si esta dimensión es igual a la dimensión $dim_{\mathbb{F}} \overline{R_0}/R_0$, la base hallada en el paso 3 es la base buscada y se termina.

Paso 5: En caso contrario, se escribe $R_0 = R_1$ y se repite el proceso desde el paso 2 hasta que la dimensión considerada en el paso 4 alcance la dimensión buscada; el número de repeticiones que se necesitan es a lo más $l \doteq dim_{\mathbb{F}} \overline{R_0}/R_0$. Además, en cada repetición el discriminante queda dividido por β^2, con lo que en la práctica basta considerar los factores cuadráticos del correspondiente discriminante.

Ejemplo 3.3 *Se considera sobre* $\mathbb{F}_2$ *la curva proyectiva* $\mathrm{X}_1^2\mathrm{X}_0^2 + \mathrm{X}_1\mathrm{X}_2\mathrm{X}_0^2 + \mathrm{X}_2^4 = 0$ *con un único punto en el infinito, cuya ecuación afín viene dada por* $f(\mathrm{X},\mathrm{Y}) = \mathrm{Y}^4 + \mathrm{XY} + \mathrm{X}^2 = 0$. *El discriminante de* f *es* $D_f = \mathrm{X}^4$, *con lo que podemos considerar únicamente el factor* $\beta = \mathrm{X}$.

Paso 1: *Se toma la base* $\{1, \mathrm{Y}, \mathrm{Y}^2, \mathrm{Y}^3\}$ *de* R_0 *sobre* S.

Paso 2: *De la ecuación* $f = 0$ *se deduce que* $\mathrm{Y}^4 = \mathrm{X}\,(\mathrm{X} + \mathrm{Y})$, *con lo que la imagen de* Y^4 *es un nilpotente en el cociente* $R_0/(\mathrm{X}\,R_0)$; *en consecuencia, los nilpotentes de* $R_0/(\mathrm{X}\,R_0)$ *son* $\{\overline{\mathrm{Y}}, \overline{\mathrm{Y}}^2, \overline{\mathrm{Y}}^3\}$ *(denotando* $\phi(\mathrm{Y}) = \overline{\mathrm{Y}}$*), lo cual implica que* $\{\mathrm{X}, \mathrm{Y}, \mathrm{Y}^2, \mathrm{Y}^3\}$ *es una base de* $rad(\mathrm{X}\,R_0)$.

Paso 3: *Podemos escribir el idealizador como* $R_1 = \{b \in Fr(R_0) \mid b\mathrm{X} \in rad(\mathrm{X}\, R_0), \quad b\mathrm{Y}^k \in rad(\mathrm{X}\, R_0) \quad \text{para} \quad k = 1, 2, 3\}$*; escribiendo un elemento* b *genérico en la forma* $b = a_0 + a_1\mathrm{Y} + a_2\mathrm{Y}^2 + a_3\mathrm{Y}^3$ *con* $a_i \in Fr(S)$*, las anteriores condiciones para* R_1 *imponen que*

$$a_0 \in S, \;\; a_1 \in S, \;\; a_2 \in S, \;\; a_3\mathrm{X} \in S$$

con lo que $\{1, \mathrm{Y}, \mathrm{Y}^2, \dfrac{\mathrm{Y}^3}{\mathrm{X}}\}$ *es una base de* R_1 *sobre* S*.*

Paso 4: *La dimensión de* R_1/R_0 *sobre* $\mathbb{F}$ *es igual a* 1*, que es exactamente la de* $\overline{R_0}/R_0$*, con lo que la base entera que buscamos es la obtenida en el paso 3 y se termina el algoritmo.*

Existen algunas mejoras de este algoritmo, basadas en la utilización de *series de Puiseux* para comprobar si un elemento de L es entero o no, y que están implementadas para característica cero en las últimas versiones de Maple V y AXIOM (ver [56], [61] y [89]). Dichas mejoras plantean problemas prácticos en el caso de característica positiva si la correspondiente extensión de cuerpos tiene *ramificación salvaje*, pero esta situación no se da si la característica no divide al grado de la curva, que es la condición que nosotros asumiremos en la práctica. En todo caso, podrían sustituirse los desarrollos de Puiseux por los de Hamburger-Noether en la implementación del algoritmo con el fin de evitar tales problemas, puesto que estos desarrollos funcionan mejor en el caso de característica positiva.

El algoritmo de la base entera es una variante del llamado *algoritmo de Coates* que, en particular, permite calcular una base de $\mathcal{L}(G)$ sobre $\mathbb{F}$ para cualquier divisor racional G mediante un método alternativo al del algoritmo de Brill-Noether (ver Davenport [26] o Duval [35]).

Por último, decir que el cálculo de una base entera nos permite resolver la singularidades de la parte afín de la curva considerada, es decir, hallar la parte afín $\tilde{C}$ de un modelo no singular $\tilde{\chi}$ para la curva proyectiva plana χ cuya parte afín es C, según la notación empleada en la sección 3.1 . La idea es que si $\{u_1, \ldots, u_m\}$ es una tal base y llamamos $u_0 = \mathrm{X}$, tomamos una indeterminada Y_i para cada uno de los elementos u_i $(0 \leq i \leq m)$ y consideramos la variedad afín $V \subseteq \mathbb{F}^{m+1}$ definida por el ideal I de $\mathbb{F}[\mathrm{Y}_0, \ldots, \mathrm{Y}_m]$ que generan los polinomios $f_{i,j} = \mathrm{Y}_i\mathrm{Y}_j - \sum_k \alpha_{i,j}^k(\mathrm{Y}_0)\mathrm{Y}_k$, donde $\alpha_{i,j}^k$ se define por las relaciones

$u_i u_j = \sum_{k=0}^{m} \alpha_{i,j}^k(\mathrm{X}) u_k$ para $0 \leq i \leq j \leq m$. Entonces, el homomorfismo natural de $\mathbb{F}$-álgebras

$$\tilde{\phi} \; : \; \mathbb{F}[V] = \mathbb{F}[\mathrm{Y}_0, \ldots, \mathrm{Y}_m]/I \to \overline{R} = \mathbb{F}[\mathrm{X}]\, u_1 + \ldots + \mathbb{F}[\mathrm{X}]\, u_m$$

es un $\mathbb{F}$-isomorfismo, y $\tilde{C} \doteq V$ es el modelo afín no singular buscado. De hecho, podrían encontrarse los puntos infinitamente próximos a uno dado a través del morfismo birracional propio de variedades inducido por el correspondiente $\mathbb{F}$-isomorfismo entre los anillos de coordenadas afines (ver [87]).

3.7 La distancia de Feng y Rao

En esta sección mostraremos cómo calcular la distancia de Feng y Rao del semigrupo de Weierstrass en un punto racional P, suponiendo que éste sea el único punto en el infinito de un modelo plano singular, en las condiciones del teorema de Abhyankar-Moh; este cálculo es de gran interés en la decodificación de códigos álgebro-geométricos sobre un punto mediante el test de mayoría de Feng y Rao, tal y como se vio en el primer capítulo del presente trabajo. De hecho, mostraremos cómo se define y cómo se calcula para semigrupos numéricos arbitrarios siempre que se tenga una sucesión particular de generadores, que son muy fáciles de calcular en el caso del teorema de Abhyankar-Moh, y fáciles de modificar si se añade un número finito de elementos según se hizo en el lema 3.1 . Introduciremos para ello las definiciones y resultados básicos sobre semigrupos de números naturales.

3.7.1 Sistemas de Apéry y distancia de Feng y Rao para semigrupos numéricos

Aunque la distancia de Feng y Rao haya sido definida ya en el capítulo 1 para semigrupos de Weierstrass al hablar del método de decodificación de Feng y Rao para códigos sobre un punto, volvemos ahora a dar la misma definición en un contexto mucho más general como es el marco de la aritmética de semigrupos numéricos arbitrarios.

Definición 3.8 *Sea $S \subseteq \mathbb{N}$ un semigrupo numérico de complemento finito, es decir, tal que $\sharp(\mathbb{N} \setminus S) < \infty$, y supongamos que $0 \in S$; para $n \in S$ se*

define la distancia de Feng y Rao de n relativa a S como

$$\delta_{FR}(n) \doteq mín\,\{N_r \mid r \geq n,\ \ r \in S\}$$

donde $N_r \doteq \sharp\{(a,b) \in S \times S \mid a+b=r\}$.

La siguiente definición nos proporciona un método general para obtener de forma teórica sistemas de generadores para semigrupos numéricos arbitrarios, y constituye la herramienta fundamental para obtener los resultados de esta sección. Dichos resultados podrán aplicarse al caso de semigrupos en el infinito a través del teorema de Abhyankar-Moh, y constituyen otra aportación original en el terreno de la teoría de códigos álgebro-geométricos.

Definición 3.9 *Sea $S \subseteq \mathbb{N}$ un semigrupo con las mismas hipótesis que en la definición anterior; para $m \in S \setminus \{0\}$ se define el conjunto de Apéry de S relativo a m como el conjunto formado por la sucesión de números*

$$a_i \doteq mín\,\{n \in S \mid n \equiv i\ (mod\ \ m)\} \qquad \text{para} \quad 0 \leq i \leq m-1$$

De ahora en adelante, el índice i se identificará con el correspondiente elemento en el anillo $\mathbb{Z}/(m)$. Podríamos eliminar el elemento $a_0 = 0$, puesto que no añade ninguna información sobre el semigrupo; en realidad, se tiene obviamente una unión disjunta del tipo

$$S = \bigcup_{i=0}^{m-1} (a_i + m\mathbb{N})$$

con lo que, en consecuencia, el conjunto $\{a_1, \ldots, a_{m-1}, m\}$ es un sistema de generadores para el semigrupo S, que se denomina *sistema de generadores de Apéry* de S relativo a m (sistema de Apéry, para abreviar, sobreentendiéndose el m fijado). Usualmente se suele tomar m como el mínimo del semigrupo $S \setminus \{0\}$, pero no es necesario; dicho sistema de generadores está lejos de ser minimal, pero es muy útil para hacer cierto tipo de cálculo, como veremos a continuación en el problema que nos interesa en el presente apartado.

Veamos ahora qué tipo de relaciones ligan entre sí a los distintos elementos del conjunto de Apéry; sean $i, j \in \mathbb{Z}/(m) \equiv \mathbb{Z}_m$ y consideremos $i+j \in \mathbb{Z}_m$ (salvo identificación módulo m, según hemos indicado anteriormente); entonces

$$a_i + a_j = a_{i+j} + \alpha_{i,j} m$$

para ciertos $\alpha_{i,j} \geq 0$, por definición de los elementos de Apéry.

Usando esta notación, cada elemento $n \in S$ puede escribirse de manera única como $n = a_i + lm$, con $i \in \mathbb{Z}_m$ y $l \geq 0$; de esta manera, podemos asociar a cada elemento n del semigrupo un par de coordenadas $(i, l) \in \mathbb{Z}_m \times \mathbb{N}$, que llamaremos *coordenadas de Apéry relativas a* m.

Veamos cómo se pueden usar las coordenadas de Apéry para calcular el número N_r. Sean $r \equiv (i, l)$, $a \equiv (i_1, l_1)$ y $b \equiv (i_2, l_2)$; puesto que se quiere que

$$r = a + b = a_{i_1+i_2} + (l_1 + l_2 + \alpha_{i_1,i_2})\, m$$

se deduce que $l_1 + l_2 = l - \alpha_{i_1,i_2}$.

Escribiendo $i_1 = k$ y $i_2 = i - k$, si $l < \alpha_{k,i-k}$ la igualdad $r = a + b$ no es posible, con lo que el caso que nos interesa es que se verifique la desigualdad $\alpha_{k,i-k} \leq l$.

Para $0 \leq i \leq m-1$ y $h \geq 0$ definimos ahora el número

$$B_i^{(h)} \doteq \sharp\{\alpha_{k,i-k} \leq h \mid k \in \mathbb{Z}_m\}$$

Establecida esta notación, el siguiente resultado nos da un fórmula para calcular el número N_r.

Proposición 3.3 $\quad N_r = B_i^{(0)} + B_i^{(1)} + \ldots + B_i^{(l)}$.

Demostración:

Supongamos que $\alpha_{k,i-k} = h \leq l$; entonces, en la suma de la derecha de la igualdad $\alpha_{k,i-k}$ ha sido considerado una vez en cada uno de los sumandos $B_{(i)}^h, B_i^{(h+1)}, \ldots, B_i^{(l)}$, es decir $l - h + 1$ veces.

Por otro lado, la igualdad $l_1 + l_2 = l - \alpha_{k,i-k}$ se verifica para $l - h + 1$ posible pares l_1, l_2 , lo cual prueba el resultado.

□

A continuación, si queremos tener una fórmula para calcular la distancia de Feng y Rao $\delta_{FR}(n)$, siendo $n \equiv (i_0, l_0)$, la observación fundamental es que, a causa de la igualdad del resultado anterior, el número N_r es *creciente en la coordenada* l; de esta manera, para calcular dicha distancia es suficiente con hallar el *mínimo en la coordenada* i, lo cual reduce el proceso a un número finito de posibilidades.

De forma más precisa, para cada $j \in \mathbb{Z}_m$ nos interesa encontrar el mínimo $r_j = a_j + t_j m$ tal que $r_j \geq n = a_{i_0} + l_0 m$; sin más que efectuar unas operaciones muy sencillas, se puede probar fácilmente el siguiente resultado.

Teorema 3.3 *En las condiciones anteriores, se tiene que*

$$\delta_{FR}(n) = mín\,\{N_{r_j} \mid j \in \mathbb{Z}_m\}$$

donde $r_j \equiv (j, t_j)$ *y* t_j *es el mínimo entero tal que* $t_j \geq máx\left(\frac{a_{i_0} - a_j}{m} + l_0, 0\right)$.

□

En conclusión, el cálculo de la distancia de Feng y Rao para un semigrupo numérico arbitrario es bastante sencillo si se dispone del sistema de Apéry relativo a un elemento n del semigrupo. Veamos cómo puede hallarse un tal sistema de Apéry en el caso geométrico que nos interesa.

3.7.2 Sistemas de Apéry para semigrupos en el infinito

Veamos en primer lugar cómo calcular un sistema de Apéry para el caso del semigrupo S_P, aunque en realidad como el método y los resultados obtenidos dependen únicamente de las propiedades aritméticas de los generadores dadas por el teorema de Abhyankar-Moh, todo ello será válido igualmente para semigrupos telescópicos arbitrarios. Nótese que, por otra parte, tales semigrupos pueden verse como el semigrupo S_P de alguna curva plana, según los resultados de la sección 3.5 , con lo que ambos puntos de vista son equivalentes.

Para ello, en las condiciones y notaciones del teorema de Abhyankar-Moh, consideraremos el elemento del semigrupo $m = \delta_0 = deg\,\chi$. El hecho fundamental es entonces recordar que cualquier n en el semigrupo S_P puede escribirse de manera única en la forma

$$n = \sum_{k=0}^{h} \lambda_k \delta_k = \lambda_0 m + \sum_{k=1}^{h} \lambda_k \delta_k$$

con $\lambda_0 \geq 0$ y $0 \leq \lambda_k < n_k = d_k/d_{k+1}$ para $1 \leq k \leq h$; esto implica que los elementos de Apéry relativos a $m = \delta_0$ son necesariamente aquéllos tales que $\lambda_0 = 0$.

Por otro lado, el número total de elementos con $\lambda_0 = 0$ es

$$\frac{d_1}{d_2}\frac{d_2}{d_3}\cdots\frac{d_h}{d_{h+1}} = m$$

al ser $d_1 = \delta_0 = m$ y $d_{h+1} = 1$. En consecuencia, los elementos $\sum_{k=1}^{h} \lambda_k \delta_k$ con $0 \leq \lambda_k < n_k = d_k/d_{k+1}$ para $1 \leq k \leq h$ son elementos de S_P diferentes dos a dos módulo $m = \delta_0$, y son mínimos en S_P con esta propiedad; por lo tanto éstos no son otra cosa que elementos del sistema de Apéry de S_P relativos al elemento m.

Por lo tanto, el sistema de Apéry del semigrupo S_P relativo al grado m de la curva (o análogamente de un semigrupo telescópico arbitrario en relación a δ_0) es fácil de obtener a partir de la sucesión de generadores dada por el teorema de Abhyankar-Moh.

De hecho pueden obtenerse fácilmente las coordenadas de Apéry de un elemento cualquiera del semigrupo S_P a partir de dicha sucesión, aunque se pueden calcular directamente a partir del sistema de Apéry con más rapidez. Efectivamente, dado $n \in S_P$ escrito en la forma

$$n = \lambda_0 m + \sum_{k=1}^{h} \lambda_k \delta_k$$

se tiene que $l = \lambda_0$ y que $i \in \mathbb{Z}_m$ es el elemento tal que $i \equiv \sum_{k=1}^{h} \lambda_k \delta_k \ (mod \ \ m)$; en particular, podemos calcular fácilmente los números a_i, $\alpha_{i,j}$, N_r y $\delta_{FR}(n)$ para el semigrupo S_P.

El problema que queda ahora por resolver es el cálculo del sistema Apéry relativo al elemento $m = deg\,\chi$ para el semigrupo de Weierstrass $\Gamma_P = S_P + b_1\mathbb{N} + \ldots + b_l\mathbb{N}$, donde $l = dim_{\mathbb{F}}(\overline{A}/A)$ y b_i son calculados según el procedimiento de triangulación dado por el lema 3.1 .

Dicho problema se reduce a iterar un número finito de veces un algoritmo que resuelva el siguiente problema general para semigrupos numéricos arbitrarios: *calcular el sistema de Apéry relativo a m para un semigrupo del tipo* $\overline{S} = S + b\mathbb{N}$ *modificando el sistema de Apéry del semigrupo S relativo a* $m \in S$.

Supongamos para ello que $\{a_1, \ldots, a_{m-1}\}$ es el sistema de Apéry de S relativo a $m \in S$ y sea $\{\alpha_{i,j}\}$ el conjunto de relaciones para dicho sistema; veamos cómo se calcula $\{\overline{a_1}, \ldots, \overline{a_{m-1}}\}$ el sistema de Apéry de $\overline{S}$ relativo a $m \in \overline{S}$ y en consecuencia las correspondientes relaciones $\{\overline{\alpha_{i,j}}\}$.

En primer lugar, podemos suponer que $b \notin S$, pues en caso contrario el semigrupo no cambia y no hay ninguna modificación que hacer ni en los generadores ni en las relaciones; la comprobación de si un elemento b está o no en el semigrupo S puede hacerse fácilmente en términos del sistema de Apéry de S mediante el procedimiento siguiente:

(i) Se calcula $j \in \mathbb{Z}_m$ tal que $j \equiv b \ (mod \ \ m)$.

(ii) $b \in S$ si y sólo si $l = \dfrac{b - a_j}{m} \geq 0$.

Ahora bien, está claro que los candidatos a ser los elementos del nuevo sistema de Apéry son los números $s_{j,\lambda} = a_j + \lambda\, b$ con $0 \leq j, \lambda \leq m-1$; en definitiva, sólo hay que efectuar un número finito de comprobaciones. De esta manera, el procedimiento a seguir es el que se detalla a continuación:

1. Inicializar $\overline{a_i} = a_i$ para $1 \leq i \leq m-1$ (obviamente se tendrá que $\overline{a_0} = a_0 = 0$).

2. Tomar uno por uno los elementos $s_{j,\lambda}$ y calcular su resto i módulo m.

3. Comparar $s_{j,\lambda}$ con el valor de $\overline{a_i}$; si $\overline{a_i}$ es mayor, tendremos que actualizar su valor y cambiarlo por $\overline{a_i} = s_{j,\lambda}$, continuando así con todos y cada uno de los restantes $s_{j,\lambda}$.

El algoritmo anterior nos da como resultado final el sistema de Apéry para el semigrupo $\overline{S}$.

Nota 3.5 *Los resultados obtenidos en esta sección nos sugieren la utilización sistemática de los sistemas de Apéry y sus correspondientes coordenadas para describir un semigrupo numérico arbitrario y poder efectuar así cierto tipo de cálculos con bastante sencillez. De esta manera, los elementos n de un semigrupo se identifican con pares $(i,l) \in \mathbb{Z}_m \times \mathbb{N}$ si $n = a_i + l\, m$, con lo que el semigrupo no sería otra cosa que el conjunto de datos $\{m;\ \ a_i \ \text{para} \ \ 0 \leq i \leq m-1\}$ junto con las restricciones $\alpha_{i,j} \geq 0$, según la definición que se ha dado en la presente sección. Con esta terminología, añadir un nuevo generador al semigrupo no es más que efectuar ciertas modificaciones en dichos datos.*

Nota 3.6 *Nótese que el cálculo de una función en el anillo afín $\overline{A}$ con un polo en P de orden $n \in \Gamma_P$ es mucho más sencillo con un sistema que Apéry que tal y como lo describimos en el párrafo 3.4.2 ; de forma más precisa, supongamos que tenemos un sistema de Apéry $\{m;\ a_i \text{ para } 0 \leq i \leq m-1\}$ para Γ_P, y sean $f_0, f_1, \ldots, f_{m-1}$ funciones en $\overline{A}$ con un polo en P de orden $a_0, a_1, \ldots, a_{m-1}$ respectivamente. Entonces, dado $n = lm + a_i \in \Gamma_P$, la función $g_n \doteq \mathrm{X}^l f_i$ tiene en P un polo de orden n (nótese que $F_0 \doteq \mathrm{X}$ es la función asociada al valor $\delta_0 = m$, en las condiciones del algoritmo de raíces aproximadas).*

En particular, al aplicar este procedimiento al algoritmo de triangulación del lema 3.1 , el semigrupo de Weierstrass Γ_P, las funciones que alcanzan los valores de dicho semigrupo y la distancia de Feng y Rao pueden irse calculando simultáneamente, mediante las correspondientes modificaciones en cada uno de los pasos del proceso de triangulación.

Como conclusión de lo expuesto en el presente capítulo, podemos enunciar el siguiente teorema que resume los resultados fundamentales del mismo.

Teorema 3.4 *Sea χ una curva algebraica proyectiva plana de grado m con una sola rama racional P en el infinito que está definida sobre el cuerpo perfecto base $\mathbb{F}$. Supongamos que o bien la característica del cuerpo $\mathbb{F}$ es cero, o bien ésta no divide simultáneamente a m y a $e_P(\chi)$. Entonces existe un algoritmo que calcula simultáneamente el semigrupo de Weierstrass Γ_P, funciones con un único polo en P de orden cada uno de los valores del semigrupo y la distancia de Feng y Rao de cada uno de los elementos de dicho semigrupo.*

Más aún, fijado un semigrupo telescópico generado por una sucesión de elementos $\{\delta_i\}_{i=0}^{h}$ que verifican las propiedades (I), (II) y (III) dadas por el teorema de Abhyankar-Moh, se pueden generar explícitamente curvas planas sobre un cuerpo perfecto dado con una sola rama racional en el infinito que está definida sobre dicho cuerpo y cuyo semigrupo en el infinito S_P es el semigrupo prefijado.

□

Bibliography

[1] S.S. Abhyankar, *Lectures on expansion techniques in Algebraic Geometry*, Tata Institute of Fundamental Research, Bombay (1977).

[2] S.S. Abhyankar, *On the semigroup of a meromorphic curve*, Intl. Symp. on Algebraic Geometry, pp. 249-414, Kyoto (1977).

[3] S.S. Abhyankar, *Irreducibility criterion for germs of analytic functions of two complex variables*, Advances in Mathematics **74**, pp. 190-257 (1989).

[4] S.S. Abhyankar, *Desingularization of plane curves*, American Mathematical Society Proc. of the Symp. in Pure Mathematics, pp. 1-45 (1983).

[5] S.S. Abhyankar, *Algebraic Geometry for scientists and engineers*, American Mathematical Society (1990).

[6] S.S. Abhyankar and T.T. Moh, *Newton-Puiseux expansion and generalized Tschirnhausen transformation*, J. Reine Math. **260**, pp. 47-83 and **261**, pp. 29-54 (1973).

[7] G. Angermuller, *Die Wertehalbgruppe einer ebenen irreduziblen algebroiden Kurve*, Math. Zeit. **153**, pp. 267-282 (1977).

[8] R. Apéry, *Sur les branches superlinéaires des courbes algébriques*, C.R. Acad. Sciences Paris **222**, pp. 1198-1200 (1946).

[9] M.F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Pub. Company, Massachusetts (1969).

[10] E.R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York (1968).

[11] E.R. Berlekamp, R.J. McEliece and H.C.A. van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Trans. Inform. Theory **24**, pp. 384-386 (1978).

[12] J. Bertin et P. Carbonne, *Sur la structure des semi-groupes d'entiers et applications aux branches*, C.R. Acad. Sciences Paris, ser. A, vol. 280, pp. 1745-1748 (1975).

[13] G.A. Bliss, *Algebraic functions*, Dover (1966).

[14] N. Bourbaki, *Commutative Algebra*, Addison Wesley (1972).

[15] Von A. Brill und M. Noether, *Die Entwicklung der Theorie der algebraischen Funktionen in älterer und neuerer Zeit*, Jahresberichte der deutschen Mathematiker-Vereinigung III, pp. 111-566 (1892-1893).

[16] A. Campillo, *Algebroid curves in positive characteristic*, Lecture Notes in Math., vol. 813, Springer-Verlag (1980).

[17] A. Campillo and J. Castellanos, *Curve singularities*, Univ. Valladolid, preprint (1997).

[18] A. Campillo and J.I. Farrán, *Computing Weierstrass semigroups from singular plane models*, Univ. Valladolid, preprint (1997).

[19] A. Campillo, G. González-Sprinberg and M. Lejeune-Jalabert, *Clusters of infinitely near points*, Math. Annalen **306**, pp. 169-194 (1996).

[20] E. Casas, *Infinitely near imposed singularities and singularities of polar curves*, Math. Annalen **287**, pp. 429-454 (1990).

[21] E. Casas, *Singularities of polar curves*, Compositio Mathematica, vol. 89, pp. 339-359 (1993).

[22] D. Cox, J. Little and D. O'Shea, *Ideals, varieties and algorithms: an introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag UTM (1992).

[23] B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan and S.M. Watt, *Maple V Language Reference Manual*, Springer-Verlag (1991).

[24] B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan and S.M. Watt, *Maple V Library Reference Manual*, Springer-Verlag (1991).

[25] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Math. Surveys., vol. VI, Amer. Math. Soc. (1951).

[26] J.H. Davenport, *On the integration of algebraic functions*, Lecture Notes in Computer Science **102**, Springer-Verlag, (1981).

[27] F. Delgado, *The semigroup of values of a curve singularity with several branches*, Manuscripta Math. **59**, pp. 347-374 (1987).

[28] F. Delgado, The symmetry of the Weierstrass generalized semigroups and affine embeddings, Proc. of the Amer. Math. Soc. **108**, pp. 627-631 (1990).

[29] Y. Driencourt et J.F. Michon, *Rapport sur les codes géométriques*, Univ. Paris 7, preprint (1986).

[30] V.G. Drinfeld and S.G. Vlăduţ, *Number of points of an algebraic curve*, Funktsional'-nyi Analiz i Ego Prilozhenia **17**, pp. 53-54 (1983).

[31] I.M. Duursma, *Algebraic decoding using special divisors*, IEEE Trans. Inform. Theory **39**, pp. 694-698 (1993).

[32] I.M. Duursma, *Majority coset decoding*, IEEE Trans. Inform. Theory **39**, pp. 1067-1071 (1993).

[33] I.M. Duursma, *Decoding codes from curves and cyclic codes*, Ph.D. thesis, Univ. Eindhoven (1993).

[34] I. Duursma and R. Kötter, *On error locating pairs for cyclic codes*, IEEE Trans. Inform. Theory **40**, pp. 1108-1121 (1994).

[35] D. Duval, *Diverses questions relatives au calcul formel avec des nombres algébriques*, Ph.D. thesis, Univ. Grenoble (1987).

[36] D. Ehrhard, *Über das Dekodieren algebraisch-geometrischer Codes*, Ph.D. thesis, Universität Düsseldorf (1991).

[37] D. Ehrhard, *Decoding algebraic-geometric codes by solving a key equation*, Proceedings AGCT-3, H. Stichtenoth and M.A. Tsfasman (eds.), Luminy 1991, Springer Lect. Notes. **1518**, pp. 18-25 (1992).

[38] D. Ehrhard, *Achieving the designed error capacity in decoding algebraic-geometric codes*, IEEE Trans. Inform. Theory **39**, pp. 743-751 (1993).

[39] F. Enriques e O. Chisini, *Teoria geometrica delle equazioni e delle funzioni algebriche*, Bologna (1918).

[40] J.I. Farrán, *Rational points, genus and asymptotic behaviour in reduced algebraic curves over finite fields*, Univ. Valladolid, preprint (1994).

[41] J.I. Farrán, *Decoding algebraic-geometric codes*, Univ. Valladolid, preprint (1997).

[42] G.L. Feng and T.R.N. Rao, *Decoding algebraic-geometric codes up to the designed minimum distance*, IEEE Trans. Inform. Theory **39**, pp. 37-45 (1993).

[43] G.L. Feng and T.R.N. Rao, *A simple approach for construction of algebraic-geometric codes from affine plane curves*, IEEE Trans. Inform. Theory **40**, pp. 1003-1012 (1994).

[44] G.L. Feng, V. Wei, T.R.N. Rao and K.K. Tzeng *Simplified understanding and efficient decoding of a class of algebraic-geometric codes*, IEEE Trans. Inform. Theory **40**, pp. 981-1002 (1994).

[45] W. Fulton, *Algebraic curves*, W.A. Benjamin, Inc. (1969).

[46] A. García and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound*, Inventiones Mathematicae **121**, pp. 211-222 (1995).

[47] G. van der Geer and J.H. van Lint, *Introduction to Coding Theory and Algebraic Geometry*, DMV seminar, Band 12, Birkhäuser Verlag, Basel (1988).

[48] V.D. Goppa, *Geometry and codes*, Kluwer Academic Publishers (1988).

[49] D. Gorenstein, *An arithmetic theory of adjoint plane curves*, Trans. Amer. Math. Soc., vol. 72, pp. 414-436 (1952).

[50] G. Haché, *Construction effective des codes géométriques*, Ph.D. thesis, Univ. Paris 6 (1996).

[51] G. Haché and D. Le Brigand, *Effective construction of Algebraic Geometry codes*, IEEE Trans. Inform. Theory **41**, pp. 1615-1628 (1995).

[52] J.P. Hansen and H. Stichtenoth, *Group codes on certain algebraic curves with many rational points*, AAECC, vol. 1, pp. 67-77 (1990).

[53] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Math., vol. 52, Springer-Verlag (1977).

[54] J. Herzog, *Generators and relations of abelian semigroups and semigroup rings*, Manuscripta Math. **3**, pp. 175-193 (1970).

[55] J. Herzog und E. Kunz, *Die Wertehalbgruppe eines lokalen Rings der Dimension 1*, Sitz. Ber. Heidelberger Akad. der Wissenschaft 2, Abhandlung (1971).

[56] M. van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*, Maple V Release 4 share library, preprint (1996).

[57] T. Høholdt and R. Pellikaan, *On the decoding of algebraic-geometric codes*, IEEE Trans. Inform. Theory **41**, pp. 1589-1614 (1995).

[58] T. Høholdt, J.H. van Lint and R. Pellikaan, *Algebraic Geometry codes*, Techn. Univ. of Denmark, preprint (1996).

[59] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sciences Tokyo, vol. 28, pp. 721-724 (1981).

[60] H. Imai, *Essentials of error-control coding techniques*, Academic Press, Inc. (1990).

[61] R.D. Jenks and R.S. Sutor, *AXIOM: the scientific computation system*, Springer-Verlag (1992).

[62] J. Justesen, K.J. Larsen, H.E. Jensen, A. Havemose and T. Høholdt, *Construction and decoding of a class of algebraic geometric codes*, IEEE Trans. Inform. Theory **35**, pp. 811-821 (1989).

[63] J. Justesen, K.J. Larsen, H.E. Jensen and T. Høholdt, *Fast decoding of codes from algebraic plane curves*, IEEE Trans. Inform. Theory **38**, pp. 111-119 (1992).

[64] G.L. Katsman, M.A. Tsfasman and S.G. Vlăduţ, *Modular curves and codes with a polynomial construction*, IEEE Trans. Inform. Theory **30**, pp. 353-355 (1984).

[65] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41**, pp. 1720-1732 (1995).

[66] E. Kunz, *Über die Klassifikation numerischer Halbgruppen*, Regensburger Mathematische Schriften, vol. 11, Universität Regensburg (1987).

[67] G. Lachaud, *Les codes géométriques de Goppa*, Sém. Bourbaki, 37Ème année, 1984-85, nº 641, pp. 189-207, Astérisque 133-134 (1986).

[68] D. Le Brigand et J.J. Risler, *Algorithme de Brill-Noether et codes de Goppa*, Bull. Soc. Math. France, pp. 231-253 (1988).

[69] J.H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, New York (1982).

[70] J. Lipman, *On complete ideals in regular local rings*, Algebraic Geometry and Commutative Algebra in honor of M. Nagata, pp. 203-231 (1987).

[71] C.L. Liu, *Elements of Discrete Mathematics*, McGraw-Hill, Inc., New York (1985).

[72] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, vol. 16, Amsterdam (1977).

[73] Y.I. Manin, *What is the maximum number of points on a curve over* $\mathbb{F}_2$*?*, J. Fac. Sciences Univ. Tokyo, I A, vol. 28, pp. 715-720 (1981).

[74] Y.I. Manin et S.G. Vlăduţ, *Codes linéaires et courbes modulaires*, Sovr. Prob. Mat., VINITI, Moscow (1984).

[75] J.L. Massey, *Threshold decoding*, Cambridge, MA – M.I.T. Press (1963).

[76] H. Matsumura, *Commutative Algebra*, Benjamin/Cummings Pub. Company (1980).

[77] R.J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, DSN Progress Report 42-44, JPL, Pasadena, Jan. and Feb. (1978).

[78] R.J. McEliece, *Finite fields for computer scientists and engineers*, Kluwer Academic Publishers (1987).

[79] C. Moreno, *Algebraic curves over finite fields*, Cambridge University Press (1990).

[80] C. Moreno, *Résolution paresseuse de courbes planes*, CALSYF **7** (1988).

[81] C. Munuera and R. Pellikaan, *Equality of geometric Goppa codes and equivalence of divisors*, Journal of Pure and Applied Algebra pp. 229-252 (1993).

[82] R. Pellikaan, *On decoding linear codes by error locating pairs*, Eindhoven Univ. of Techn., preprint (1988).

[83] R. Pellikaan, *On a decoding algorithm for codes on maximal curves*, IEEE Trans. Inform. Theory **35**, pp. 1228-1232 (1989).

[84] R. Pellikaan, *On the efficient decoding of algebraic-geometric codes*, Proc. Eurocode 92, CISM Courses and Lectures, vol. 339, pp. 231-253, Springer-Verlag, New York (1993).

[85] R. Pellikaan, B.-Z. Shen and G.J.M. van Wee, *Which linear codes are algebraic-geometric?*, IEEE Trans. Inform. Theory **37**, pp. 583-602 (1991).

[86] H. Pinkham, *Séminaire sur les singularités des surfaces (Demazure-Pinkham-Teissier)*, Cours donné au Centre de Math. de l'École Polytechnique (1977-1978).

[87] D. Polemi, *The Brill-Noether theorem with applications to algebraic geometric Goppa codes and exponential sums*, Ph.D. thesis, New York (1992).

[88] S.C. Porter, B.-Z. Shen and R. Pellikaan, *On decoding geometric Goppa codes using an extra place*, IEEE Trans. Inform. Theory **38**, pp. 1663-1676 (1992).

[89] D. Redfern, *The Maple handbook*, Springer-Verlag (1993).

[90] A.J. Reguera, *Semigroups and clusters at infinity*, Progress in Mathematics, vol. 134, pp. 339-374, Birkhäuser (1996).

[91] M. Rybowicz, *Sur le calcul des places et des anneaux d'entiers d'un corps de fonctions algébriques*, Ph.D. thesis, Limoges (1990).

[92] I. Rubio, M. Sweedler and C. Heegard, *A Gröbner bases algorithm for the decoding of algebraic-geometric codes*, Cornell University – Ithaka, preprint (1997).

[93] K. Saints and C. Heegard, *Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases*, IEEE Trans. Inform. Theory **41**, pp. 1733-1751 (1995).

[94] S. Sakata, *Extension of the Berlekamp-Massey algorithm to N dimensions*, Information and Computation, vol. 84, pp. 207-239 (1990).

[95] S. Sakata, H.E. Jensen and T. Høholdt, *Generalized Berlekamp-Massey decoding of algebraic-geometric codes up to half the Feng-Rao bound*, IEEE Trans. Inform. Theory **41**, pp. 1762-1768 (1995).

[96] A. Sathaye, *On planar curves*, Amer. J. Math. **99**, pp. 1105-1135 (1977).

[97] J.P. Serre, *Groupes algébriques et corps de classes*, Hermann et cie., Paris (1959).

[98] J.P. Serre, *Sur le nombre des points rationnels d'un courbe algébrique sur un corps fini*, C.R. Acad. Sc. Paris **296**, pp. 397-402 (1983).

[99] C.E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J., pp. 379-423 and 623-656 (1948).

[100] B.-Z. Shen, *Solving a congruence on a graded algebra by a subresultant sequence and its application*, J. Symbolic Comput., vol. 14, pp. 505-522 (1992).

[101] B.-Z. Shen, *Algebraic-geometric codes and their decoding algorithm*, Ph.D. thesis, Univ. Eindhoven (1992).

[102] A.N. Skorobogatov and S.G. Vlăduţ, *On the decoding of algebraic-geometric codes*, IEEE Trans. Inform. Theory **36**, pp. 1051-1060 (1990).

[103] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag (1993).

[104] B.M. Trager, *Integration of algebraic functions*, Ph.D. thesis, Dept. of EECS, Massachusetts Institute of Technology (1984).

[105] M.A. Tsfasman, *Goppa codes that are better than Varshamov-Gilbert bound*, Prob. Peredachi Inform. **18**, pp. 3-6 (1982).

[106] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic-geometric codes*, Math. and its Appl., vol. 58, Kluwer Academic Pub., Amsterdam (1991).

[107] M.A. Tsfasman, S.G. Vlăduţ and Th. Zink, *Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109**, pp. 21-28 (1982).

[108] S.G. Vlăduţ, *On the decoding of algebraic-geometric codes over $GF(q)$ for $q \geq 16$*, IEEE Trans. Inform. Theory **36**, pp. 1461-1463 (1990).

[109] Van der Waerden, *Modern Algebra*, N.Y. Ungar (1949).

[110] A. Weil, *Basic Number Theory*, Grund. der Math. Wiss., Bd. 144, Springer, New York (1974).

[111] D. Welsh, *Codes and Cryptography*, Clarendon Press, Oxford (1988).

[112] O. Zariski and P. Samuel, *Commutative Algebra*, vols. I and II, Van Nostrand Pub. Company, Princeton (1960).