Universidad de Sevilla

Álgebras de semigrupos y aplicaciones

Alberto Vignerón Tenorio

Tesis de Doctorado

Facultad de Matemáticas

Directora: Dra. Dña. Pilar Pisón Casares

2004

Álgebras de Semigrupos y Aplicaciones

Alberto Vigneron Tenorio

5 de octubre de 2004

Quiero expresar mi más sincero agradecimiento a Dña. Pilar Pisón Casares por su inestimable ayuda y enseñanzas recibidas a lo largo de los últimos años. Sin su ayuda esta memoria no sería hoy una realidad.

A mis padres.

ÍNDICE GENERAL

Índice de cuadros

Índice de figuras

INTRODUCCIÓN

Dado S un semigrupo conmutativo, finitamente generado, cancelativo y con elemento neutro, y dado un cuerpo k, podemos considerar la k–álgebra asociada al semigrupo, $k[S] = \oplus_{m\in S} km$, entendiendo m como un símbolo. El producto en esta álgebra se define como $m \cdot m' = m + m'$, es decir, el producto de símbolos es el símbolo de la suma. El estudio de esta álgebra tiene un gran interés dentro de la Geometría Algebraica por su relación con la Geometría Tórica. De hecho, estudiar este álgebra es equivalente a estudiar las relaciones entre los generadores de ideales definidos por variedades monomiales, es decir, variedades afines parametrizadas por ecuaciones monomiales. En [STU95]y [CP] aparece un interesante estudio sobre los distintos enfoques que se dan en la actualidad al estudio de las variedades tóricas.

Dados unos generadores del semigrupo S, $\{n_1, \dots, n_r\}$, y el anillo de polinomios $R = k[X_1, \dots, X_r]$, definimos el ideal del semigrupo como el núcleo del morfismo de k–álgebras dado por

$$\begin{gathered}\varphi : R \longrightarrow k[S]\\ \varphi(X_i) = n_i\end{gathered}$$

Es conocido (ver [HER70]) que este ideal es binomial y homogéneo respecto de la graduación $grado(X_i) = n_i$. Existen algoritmos para calcular estos ideales si el semigrupo S es libre de torsión. Casi todos ellos emplean bases de Gröbner.

El caso de la torsión fue abordado por primera vez en [BCMP98b] para semigrupos verificando $S\cap(-S) = 0$. Las técnicas utilizadas en este artículo se basan en el estudio de ciertos complejos simpliciales que fueron definidos por primera vez en [CM91] y cuyos grafos subyacentes aparecen en [ROS91]. Estas técnicas son computacionalmente poco *eficientes*, aunque no es la eficiencia lo que se busca con estos métodos, sino un mejor conocimiento del porqué de los resultados.

En cualquier caso, con torsión o no, casi todos ellos solucionan el problema de calcular el ideal recurriendo a introducir nuevas variables. El problema de aumentar el número de variables es que la complejidad del cálculo de ideales de semigrupos es simplemente exponencial en el número de variables (ver [STU91]), con lo cual, usar algoritmos que utilicen más variables de las estrictamente necesarias, provocan una gran reducción en la eficiencia de los métodos.

Nosotros resolvemos este problema en I–D.2 recurriendo a los ideales de retículo:

$$I_{\mathcal{L}} := < X^u - X^v : u, v \in \mathbb{N}^r,\ u - v \in \mathcal{L} >,$$

donde $\mathcal{L}$ es un retículo. Dado un semigrupo, le asociamos el retículo dado por las soluciones del sistema

$$(n_1| \dots |n_r) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0.$$

A este retículo será al que le calculemos su ideal asociado. Mediante este paso, sólo calculamos bases de Gröbner con el número mínimo posible de variables.

Si el semigrupo de partida, S, verifica la condición $S \cap (-S) = 0$, podemos enunciar el lema de Nakayama (III–A.1) para módulos S–graduados, y, por lo tanto, podemos hablar de la resolución libre minimal del álgebra $k[S]$ y de sistemas minimales de generadores del i–ésimo módulo de sicigias del mismo álgebra. Para calcular un sistema de generadores del i–ésimo módulo de sicigias, vamos a recurrir a resultados que ligan dichos generadores con unos complejos simpliciales de naturaleza combinatoria asociados a los elementos $m \in S$:

$$\Delta_m := \{F \subset \Lambda | m - n_F \in S\},$$

donde Λ es el conjunto $\{1, 2, \ldots, r\}$. Dichos resultados nos relacionan los generadores minimales de grado $m \in S$ del i–ésimo módulo de sicigias con las homologías reducidas, $\tilde{H}_i(\Delta_m)$. En primer lugar, veremos que en un sistema minimal de generadores del i–ésimo módulo de sicigias hay un elemento de grado m si y solo si $\tilde{H}_i(\Delta_m) \neq 0$ (III–A.4). A partir de las homologías no nulas podremos calcular directamente los generadores (III–A.5). Ésta es la filosofía que se desprende de [CM91], y es la que seguiremos en gran parte de esta memoria. De hecho, vamos a dedicar gran parte de ella a resolver el primer paso de este problema: calcular

$$C_i := \{m \in S \mid \tilde{H}_i(\Delta_m) \neq 0\}.$$

En [CG00], los autores definen nuevos complejos que permiten calcular este conjunto en situaciones concretas, pero no en el caso general. Más referencias con respecto a la relación entre las resoluciones libres y los complejos simpliciales aparecen en [PS98], [BS98], [HOC95], [STA96] y [BH97].

Al estudiar los elementos relacionados con los semigrupos, se llega de manera natural a los sistemas diofánticos y a sus $\mathbb{N}$–soluciones, es decir, soluciones enteras positivas. El simple problema de decidir si un elemento está o no en un semigrupo, se traduce en saber si un cierto sistema diofántico tiene o no una $\mathbb{N}$–solución. Por lo tanto, es muy importante conocer las estructuras de las $\mathbb{N}$–soluciones de un sistema diofántico, así como conocer algoritmos que calculen dichas soluciones.

Las estructuras de las $\mathbb{N}$–soluciones son conocidas desde finales del siglo XIX: las $\mathbb{N}$–soluciones de un sistema homogéneo forman un semigrupo, $\mathcal{G}$, generado por sus elementos minimales respecto del orden natural en $\mathbb{N}$ (II–A.1). Las de un sistema no homogéneo, vienen dadas por uniones de conjuntos formados a partir de ciertas $\mathbb{N}$–soluciones particulares y su suma con el semigrupo $\mathcal{G}$ (II–A.2). En II–D.1 generalizamos estas estructuras a sistemas diofánticos en congruencias, concluyendo que para estos sistemas, las estructuras anteriores se repiten. Un sistema diofántico en congruencias es un sistema diofántico donde al menos una de sus ecuaciones está formulada sobre $\mathbb{Z}/c\mathbb{Z}$, donde c es un entero no nulo.

Como ya hemos dicho, el conocimiento de las estructuras de las $\mathbb{N}$–soluciones datan de muy *antiguo*. Lo que, sorprendentemente, no es tan clásico, es el estudio de los algoritmos *eficientes* ligados a obtener estas $\mathbb{N}$–soluciones. De hecho, los estudios más relevantes en este sentido pertenecen a la última década del siglo XX. Los primeros métodos aplicados, los cuales no eran *eficientes*, se basaban en realizar una búsqueda exhaustiva o en la reducción a una única ecuación, cuyas soluciones eran *más fáciles* de calcular (II–B). Nosotros, en II–B, damos un nuevo algoritmo para calcular la $\mathbb{N}$–solución general a un sistema diofántico basado en una versión constructiva (para ciertos conjuntos) del lema de Dickson (II–B.7). Gracias a este algoritmo se reduce el cálculo de la $\mathbb{N}$–solución general a calcular $\mathbb{N}$–soluciones particulares a distintos sistemas diofánticos.

Entre los algoritmos existentes para calcular una $\mathbb{N}$–solución particular, caso de que exista, a un sistema homogéneo, cabe destacar, por su velocidad de cómputo, el algoritmo II–C.3, basado en el lema de Farkas (II–C.1). Guiados por la alta velocidad de este algoritmo, generalizamos en la sección II–C dicho algoritmo para aplicarlo a sistemas no homogéneos. En esta sección damos además una condición necesaria y suficiente para saber si un sistema diofántico no homogéneo tiene alguna $\mathbb{N}$–solución en función de una única ecuación que construimos.

Aplicando los resultados obtenidos en el capítulo I, damos un nuevo algoritmo basado en ideales de semigrupos para la obtención de $\mathbb{N}$–soluciones particulares a sistemas diofánticos (II–D.5). La clave de dicho algoritmo radica en asociar a un sistema diofántico un semigrupo, probando que son equivalentes:

- El sistema tiene alguna $\mathbb{N}$–solución.
- En el ideal asociado al semigrupo existe un binomio de una

forma determinada.

Gracias a esto, el algoritmo II–D.5 se puede aplicar a sistemas diofánticos en congruencias sin necesidad de añadir nuevas variables, algo completamente novedoso. De hecho, en II–D.6, damos un nuevo algoritmo para calcular la $\mathbb{N}$–solución general a un sistema diofántico en congruencias sin añadir ninguna nueva variable.

Nuestra obsesión por no aumentar el número de variables radica en que la complejidad teórica de resolver el cálculo de $\mathbb{N}$–soluciones es $\mathcal{NP}$–completo ([SCH96, corolario 18.1a]). En la práctica, la complejidad aumenta con el número de variables, por lo que tenemos que tratar de realizar los cálculos con el número mínimo de incógnitas posible. Hablar de algoritmos *eficientes*, de velocidad de cálculo y rapidez, debe ser entendido dentro de este contexto.

Una vez concluido el estudio de las $\mathbb{N}$–soluciones de un sistema, aplicamos estos resultados al cálculo de los módulos de sicigias de la resolución libre minimal de $k[S]$ en el caso más general, es decir, S abeliano, finitamente generado, con elemento neutro, cancelativo y Nakayama.

La *forma* de un complejo simplicial determina si su i–ésima homología asociada es o no nula. Basándonos en esto, definimos unas estructuras que aparecen en todo complejo simplicial con i–ésima homología no nula. A partir de ellas, construimos subconjuntos finitos del semigrupo S que contienen los grados de los elementos que aparecen en un sistema minimal de generadores del i–ésimo módulo de sicigias. La finitud de estos conjuntos se deduce, en último término, de la finitud de las bases de Hilbert de un número finito de sistemas lineales diofánticos asociados a estas estructuras.

En primer lugar, para el primer módulo de sicigias, definimos el concepto de F–hueco (IV–A.1) y probamos en IV–A.3 que si $\tilde{H}_1(\Delta_m) \neq 0$, entonces existe un F–hueco asociado al complejo simplicial Δ_m. A cada uno de estos F–huecos le asociamos un sistema diofántico construido a partir de los generadores de S. Además, damos un método basado en las $\mathbb{N}$–soluciones de estos sistemas, para obtener un conjunto finito que contenga a los elementos $m \in S$, tales que $\tilde{H}_1(\Delta_m) \neq 0$ (IV–A.8).

Una vez resuelto el primer módulo de sicigias, pasamos a estudiar el caso general, es decir, a estudiar el i–ésimo módulo. Para ello generalizamos el concepto de F–hueco de Δ_m al de j–triangulación de F en Δ_m (V–A.2). Con ello, usando también las técnicas de programación lineal del capítulo II, damos un algoritmo para calcular los grados de los elementos que aparecen en un sistema minimal de generadores del i–ésimo módulo de sicigias de $k[S]$. De aquí deducimos un procedimiento de cálculo de un sistema minimal.

Debido a la naturaleza de las relaciones obtenidas entre los elementos de S con homología no nula, y las $\mathbb{N}$–soluciones a sistemas diofánticos, podemos, además de calcular, acotar los grados de un sistema minimal de generadores del i–ésimo módulo de sicigias. En V–B.2 damos una cota para las sicigias de cualquier orden, y en V–B.3 mejoramos esa cota para el primer módulo. En cualquier caso, las cotas obtenidas son simplemente exponenciales en el número de generadores del semigrupo.

Las cotas y construcciones sobre los grados de las sicigias las aplicamos a acotar (V–C.1) y determinar (V–C.2) la regularidad de una variedad tórica proyectiva. Dado un ideal homogéneo, I, se define la regularidad de I, $reg(I)$, al menor entero p tal que el i–ésimo módulo de sicigias de I está generado por elementos de grados menores o iguales a $p + i$, para $\forall i \geq 0$ (ver [BM93]).

El objetivo principal de esta memoria es tener un mejor conocimiento del álgebra de un semigrupo, así como tener herramientas efectivas que nos permitan calcular los elementos asociados a dicha álgebra a partir de unos generadores del semigrupo. Con este propósito fuimos resolviendo de manera escalonada y satisfactoria distintos problemas que surgían al profundizar nuestro estudio. El primer problema fue dar un método efectivo y *eficiente* para calcular un sistema de generadores del ideal de un semigrupo con torsión. Es más, hasta ahora no había forma de construir de manera efectiva el ideal de un semigrupo genérico con torsión. El siguiente problema fue encontrar algoritmos para resolver sistemas diofánticos en congruencias, problema que surge de manera natural al tratar con semigrupos cancelativos con torsión. Esta fue la clave para poder dar un algoritmo que calcula los grados de los sistemas minimales de generadores de los distintos módulos que aparecen en una resolución libre de $k[S]$, convirtiendo en método efectivo el método dado en [BCMP98a] para calcular sistemas minimales de generadores de estos módulos.

En el capítulo I, estudiamos la estructura de los ideales asociados a semigrupos abelianos, cancelativos, finitamente generados y con elemento neutro, determinando que éstos se corresponden con ideales de retículo (I–B.1). Este estudio revela una *dualidad* entre los semigrupos y los retículos. También analizamos distintos algoritmos conocidos de cálculo de ideales de retículo basados en el uso de bases de Gröbner, y, apoyándonos en los resultados obtenidos, damos algoritmos que nos permiten calcular sistemas irreducibles de generadores del ideal de un semigrupo con torsión (I–D.2 y I–D.4). Este capítulo recoge básicamente el contenido publicado en el artículo [VT99].

El capítulo II está dedicado al estudio de las estructuras de las soluciones enteras positivas de un sistema diofántico en congruencias. En primer lugar vemos distintos métodos basados en técnicas muy dispares que resuelven sistemas diofánticos sin congruencias, dando sistemas de generadores minimales de dichas soluciones, así como soluciones particulares. Después generalizamos los resultados sobre las estructuras de las $\mathbb{N}$–soluciones de esos sistemas a sistemas en congruencias. Por último damos algoritmos basados en bases de Gröbner (II–D.5) y en el lema de Dickson (II–D.6), para resolver sistemas diofánticos en congruencias sin añadir nuevas variables. El contenido de este capítulo amplía y generaliza al caso de sistemas en congruencias los resultados obtenidos en [PCVT98].

En el capítulo III comenzamos a estudiar la resolución libre minimal de la k–álgebra de un semigrupo Nakayama. Vemos como se pueden caracterizar los grados de los sistemas minimales de generadores del i–ésimo módulo de sicigias de $k[S]$, a través de estructuras combinatorias. En particular resolvemos este problema para el 0–módulo (ideal del semigrupo) mediante un algoritmo (III–B.6). También vemos como, conocidos los grados que aparecen en los sistemas de generadores minimales, podemos calcular los propios generadores. Los resultados presentados en este capítulo constituyen una revisión de los aparecidos en [BCMP98b] y [BCMP98a].

El capítulo IV lo dedicamos a dar un método efectivo, basado en el cálculo de $\mathbb{N}$–soluciones de sistemas diofánticos en congruencias, para calcular los grados que aparecen en el primer módulo de sicigias de $k[S]$ (IV–A.8). Básicamente, este capítulo recoge los resultados publicados en [PCVTer].

En el capítulo V generalizamos los métodos del capítulo IV a toda la resolución del álgebra $k[S]$ (V–A.9). Además, damos cotas para los grados que aparecen en un sistema minimal de generadores del i–ésimo módulo de sicigias de $k[S]$, en función solamente de los generadores considerados para el semigrupo. Terminamos el capítulo explicitando una cota para la regularidad de una variedad tórica (V–C.1), así como un algoritmo para hallar dicha regularidad (V–C.2). Los resultados de este capítulo están recogidos en [BMPCVT99].

En el capítulo VI, vemos una serie de ejemplos numéricos que ilustran los algoritmos más importantes dados en esta memoria.

CAPÍTULO I

Cálculo de Ideales de Retículos y Semigrupos

I–A. INTRODUCCIÓN

Sea S un semigrupo conmutativo, finitamente generado y con elemento neutro, k un cuerpo, y $\{n_1, \ldots, n_r\}$ un sistema de generadores de S. Denotaremos por R al anillo en r indeterminadas sobre el cuerpo k, $k[X_1, \ldots, X_r]$.

Recordemos que se puede asociar un ideal I (dependiente del sistema de generadores considerado en S) al semigrupo S. Dicho ideal es el núcleo del morfismo de k–álgebras

$$\begin{aligned} \varphi : R &\longrightarrow k[S], \\ \varphi(X_i) &= n_i, \end{aligned} \tag{I–A.1}$$

donde $k[S]$ es el álgebra asociada a S. Además, es conocido (ver [HER70]) que I está generado por el conjunto

$$\{X^{\alpha} - X^{\beta} : \sum_{i=1}^{r} \alpha_i n_i = \sum_{i=1}^{r} \beta_i n_i, \ \ \alpha, \beta \in \mathbb{N}^r\},$$

luego es un ideal binomial.

Diremos que S es Nakayama si verifica la condición $S \cap (-S) = \{0\}$. Esta propiedad es fundamental para poder hablar de sistemas minimales de generadores de I. Un semigrupo es cancelativo si dados m, n, $n' \in S$ con $m + n' = m + n$, se tiene $n = n'$. En capítulos posteriores nos encargaremos de profundizar más en el aspecto teórico de los resultados que necesitaremos sobre el álgebra de un semigrupo.

De manera parecida al caso del semigrupo, dado un retículo $\mathcal{L}$ de $\mathbb{Z}^r$, le podemos asociar un ideal binomial en R,

$$I_{\mathcal{L}} := < X^u - X^v : u, v \in \mathbb{N}^r,\ u - v \in \mathcal{L} > .$$

A estos ideales los llamaremos de manera genérica ideales de retículo.

Para fijar notación, dado $u \in \mathbb{Z}^r$, denotamos por u^+, u^- a los únicos elementos de $\mathbb{N}^r$ tales que $u = u^+ - u^-$ y $supp(u^+) \cap supp(u^-) = \emptyset$.

Diremos que un retículo $\mathcal{L}$ es Nakayama si verifica la condición $\mathcal{L} \cap \mathbb{N}^r = (0)$. Y diremos que es saturado si dado cualquier upla $u \in \mathbb{Z}^r$ y cualquier $\alpha \in \mathbb{Z}$ no nulo verificando $\alpha u \in \mathcal{L}$, se tiene $u \in \mathcal{L}$. Entonces, si un retículo es saturado, existe una matriz, A, con coeficientes enteros tal que $\mathcal{L} = \ker(A)$. Es conocido que dado un retículo saturado, su ideal asociado es primo (ver [ES96]).

En este capítulo veremos en primer lugar que los ideales de retículo son, en realidad, un caso particular de ideales de semigrupos: los semigrupos conmutativos, finitamente generados, con elemento neutro y cancelativos (lema I–B.1), dando distintos algoritmos para calcular un sistema de generadores del ideal I.

Además analizaremos diferentes métodos para calcular unos generadores del ideal $I_{\mathcal{L}}$ a partir de un sistema de generadores de $\mathcal{L}$.

I–B. IDEALES DE RETÍCULO E IDEALES DE SEMIGRUPO

De nuevo consideremos S un semigrupo abeliano, con elemento neutro, cancelativo y finitamente generado. Por el Teorema de Estructura (ver [BCMP98b]) podemos suponer, sin perdida de generalidad, que

$$S \subset \mathbb{Z}^h \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z},$$

donde $a_1, \ldots, a_s$ son enteros no nulos. Consideremos $\{n_1, \ldots, n_r\}$ un conjunto de generadores del semigrupo S anterior, y sea $I \subset k[X_1 \ldots, X_r]$ el ideal asociado a S.

El ideal anterior lo podemos identificar con el ideal de retículo $I_{\ker(S)}$, donde $\ker(S)$ es el retículo formado por las soluciones enteras del sistema

$$(n_1| \ldots |n_r)\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0,$$

como puede verse en el siguiente resultado.

Lema I–B.1 ■ *I es un ideal de un semigrupo S cancelativo, finitamente generado, abeliano y con elemento neutro, si y sólo si I es un ideal de retículo.*

Demostración. Sea $S =< n_1, \ldots, n_r >$ un semigrupo y sea I su ideal en R. Por [HER70] sabemos que I está generado por

$$\mathcal{B} = \{X^\alpha - X^\beta : \sum_{i=1}^r \alpha_i n_i = \sum_{i=1}^r \beta_i n_i,\ \alpha_i, \beta_i \geq 0\}.$$

Además, por ser S cancelativo, podemos asegurar que I está generado por

$$\mathcal{B}' = \{X^{\alpha^+} - X^{\alpha^-} : \sum_{i=1}^r \alpha_i n_i = 0,\ \alpha_i \in \mathbb{Z}\}.$$

Por tanto, tomando el retículo $\mathcal{L}$ generado por las r–uplas $\alpha^+ - \alpha^-$ del conjunto $\mathcal{B}'$, tenemos que

$$I =< X^{\alpha^+} - X^{\alpha^-} : \alpha^+ - \alpha^- \in \mathcal{L} >,$$

luego I es un ideal de retículo.

Recíprocamente, sea $\mathcal{L}$ un retículo en $\mathbb{Z}^r$. Consideramos la aplicación

$$\pi : \mathbb{N}^r \to \mathbb{Z}^r/\mathcal{L}$$
$$e_i \mapsto e_i + \mathcal{L},$$

donde los e_i forman la base canónica de $\mathbb{N}^r$.
Sea S el semigrupo $< e_1+\mathcal{L}, \dots, e_r+\mathcal{L} >$ ([CG00]). Es fácil ver que su ideal asociado coincide con $I_{\mathcal{L}}$. ■

Este resultado nos indica que existe una dualidad entre los semigrupos cancelativos, conmutativos, finitamente generados y con elemento neutro, y los retículos. Dado un semigrupo, S, le asociamos un retículo ker(S), y dado un retículo $\mathcal{L}$, podemos asociarle un semigrupo, $\mathbf{S} =< e_1+\mathcal{L}, \dots, e_r+\mathcal{L} >$. Respecto a las propiedades, es fácil ver que si partimos de un semigrupo S, S es Nakayama si y sólo si ker(S) lo es, y S es libre de torsión si y sólo si ker(S) es saturado. Equivalentemente, si partimos de un retículo $\mathcal{L}$, $\mathcal{L}$ es Nakayama si y sólo si $\mathbf{S}$ lo es, y $\mathcal{L}$ es saturado si y sólo si $\mathbf{S}$ es libre de torsión.

El ejemplo siguiente pone de manifiesto que los sistemas de generadores irreducibles de I pueden tener distinto cardinal.

Ejemplo I–B.2 ■ Sea el semigrupo incluido en $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$,

$$S =< (0, \overline{0}, \overline{1}), (2, \overline{1}, \overline{1}), (1, \overline{0}, \overline{3}), (-2, -\overline{1}, \overline{3}) >,$$

que no es Nakayama ($-n_2 = n_4$). Entonces se tiene que el ideal de S está generado por

$$I =< x_4^2x_3^4 - x_1^2, x_2 - x_4^3x_3^8, x_4^4x_3^8 - 1 >=< x_4x_2 - 1, 1 - x_1^4, x_3^8 - x_1^8x_2^4, x_3^{12} - x_1^{10}x_2^6 >,$$

donde ambos sistemas son irreducibles.

Sin embargo si el semigrupo de partida cumple la condición:

$$S \cap (-S) = \{0\},$$

i.e. es Nakayama, tiene sentido hablar de *sistemas minimales de generadores* de I, ya que todos los sistemas irreducibles de generadores tienen el mismo cardinal (ver [BCMP98b], aunque en capítulos posteriores entraremos con más detalle en este tema). Al ser ésta una propiedad que afecta tanto al resultado que se obtiene, es interesante poder detectar con qué tipo de semigrupo nos estamos enfrentando. Para ello usaremos la siguiente caracterización.

Lema I–B.3 ■ Sea S un semigrupo, y sea I su ideal en $k[X_1,\ldots,X_r]$. El semigrupo S no es Nakayama si y sólo si existe en su ideal I un binomio de la forma $\mathcal{M}-1$, siendo $\mathcal{M}$ un monomio en $k[X_1,\ldots,X_r]$.

Demostración. Sean $n_1,\ldots,n_r$ unos generadores de S, y supongamos que existe un binomio $X^\alpha-1$ perteneciente a I, con $\alpha=(\alpha_1,\ldots,\alpha_r)\in\mathbb{N}^r$. En ese caso tenemos que

$$\sum_{i=1}^{r}\alpha_i n_i=\overline{0},$$

con lo cual S no es Nakayama.

Análogamente, si S no es Nakayama, existe una r–upla $\alpha=(\alpha_1,\ldots,\alpha_r)\in\mathbb{N}^r$, tal que $\sum_{i=1}^{r}\alpha_i n_i=\overline{0}$, y por lo tanto el binomio $X^\alpha-1$ pertenece a I. ■

Nota I–B.4 ■ Para ver entonces si S es o no Nakayama sólo habrá que buscar, en cualquier sistema de generadores binomiales con coeficientes 1 y −1 de I, si hay o no un elemento de la forma $\pm(\mathcal{M}-1)$, con $\mathcal{M}$ un monomio.

Pasemos ahora a ver distintos algoritmos para calcular un ideal de retículo y, a partir de ellos, distintos algoritmos para calcular ideales de semigrupos conmutativos, cancelativos, finitamente generados y con elemento neutro.

I–C. ALGORITMOS CLÁSICOS DE CÁLCULO DE $I_\mathcal{L}$

Con la notación anterior, el problema que nos planteamos es cómo calcular unos generadores del ideal $I_\mathcal{L}$ a partir de un conjunto de generadores C de $\mathcal{L}$.

En adelante vamos a suponer, sin pérdida de generalidad, que para toda coordenada $i = 1, \ldots, r$ de los elementos de $\mathcal{L}$, existe al menos un elemento $u \in \mathcal{L}$ tal que $u_i \neq 0$. Gracias a ello podemos considerar equivalentes los sistemas de generadores C de $\mathcal{L}$ tales que $C \subset \mathbb{N}^r$ y aquellos en los que existe un elemento con todas las coordenadas estrictamente positivas, ya que podremos pasar de unos a otros con operaciones elementales. Además, uno de estos sistemas de generadores existe si y sólo si existe el otro.

Una propiedad de los ideales de retículo que nos será muy útil en lo sucesivo es la siguiente.

Lema I–C.1 ■ $X^u - X^v \in I_{\mathcal{L}}$ si y sólo si $u - v \in \mathcal{L}$ con $u, v \in \mathbb{N}^r$.

Demostración. Por definición de $I_{\mathcal{L}}$, si $u - v \in \mathcal{L}$, tenemos que $X^u - X^v \in I_{\mathcal{L}}$. Luego es la otra implicación la que tenemos que probar.

Al retículo $\mathcal{L}$ podemos asociarle (I–B.1) un semigrupo S generado por unos ciertos $n_1, \ldots, n_r \in S$ tales que $\mathcal{L} = \ker(S)$ e $I_{\mathcal{L}} = I$.

Entonces, dado un binomio $X^u - X^v \in I_{\mathcal{L}} = I$, tenemos que (I–A.1)

$$0 = \varphi(X^u - X^v) = \sum u_i n_i - \sum v_i n_i$$

y por lo tanto $\sum (u_i - v_i) n_i = 0$. Llegamos entonces a que $u - v \in \ker(S) = \mathcal{L}$, concluyendo la demostración. ■

Si J es un ideal de R, y $f \in R$ un polinomio, también son ideales los conjuntos

$$(J : f) = \{g \in k[X_1, \ldots, X_r] : fg \in J\},$$

$$(J : f^\infty) = \{g \in k[X_1, \ldots, X_r] : f^s g \in J, \text{ para algún } s \in \mathbb{N}\}.$$

A estos ideales los llamaremos ideales cocientes de J sobre f ó f^∞ respectivamente. Por ser R noetheriano, sabemos que existe $s \in \mathbb{N}$ tal que $(J : f^\infty) = (J : f^s)$. Estos ideales serán binomiales si J es binomial y f es un monomio (ver [ES96]).

El porqué de haber introducido los ideales anteriores queda claramente respondido en el siguiente lema, el cual los liga a los ideales de retículo.

Lema I–C.2 ■ Sea $C = \{u_1, \ldots, u_s\} \subset \mathcal{L}$. Entonces C es un conjunto de generadores del retículo $\mathcal{L}$ si y sólo si

$$(J_C : (X_1 \ldots X_r)^\infty) = I_{\mathcal{L}},$$

donde

$$J_C :=< X^{u^+} - X^{u^-} : u = u^+ - u^- \in C > .$$

Demostración. Veamos en primer lugar la implicación *sólo si*. Para ello vamos a probar por doble inclusión la igualdad

$$(J_C : (X_1 \ldots X_r)^\infty) = I_{\mathcal{L}}.$$

Sea $u = u^+ - u^- \in \mathcal{L}$. Si C genera $\mathcal{L}$, se tiene que existen $\alpha_1, \ldots, \alpha_s \in \mathbb{Z}$ tales que $u = \sum_{i=1}^s \alpha_i u_i$. Entonces

$$\frac{X^{u^+}}{X^{u^-}} - 1 = \prod_{i=1}^s \left(\frac{X^{u_i^+}}{X^{u_i^-}}\right)^{\alpha_i} - 1.$$

Por comodidad de notación, denotaremos por v_i a la upla u_i si $\alpha_i \geq 0$ ó $-u_i$ en otro caso, quedando la expresión anterior como sigue

$$\frac{X^{u^+}}{X^{u^-}} - 1 = \prod_{i=1}^s \left(\frac{X^{v_i^+}}{X^{v_i^-}}\right)^{\alpha_i'} - 1,$$

con $\alpha_i' \geq 0$. Vamos a suponer por comodidad de notación que $\alpha_i' = \alpha_i$.

Reduciendo los denominadores, llegamos a que existe un cierto monomio X^a tal que

$$X^a(X^{u^+} - X^{u^-}) = X^{u^-}(X^{\sum \alpha_i v_i^+} - X^{\sum \alpha_i v_i^-}).$$

Veamos que $X^{\sum \alpha_i v_i^+} - X^{\sum \alpha_i v_i^-} \in J_C$.

Si suponemos que $\alpha_1 > 0$, podemos considerar $X^{\sum \alpha_i v_i^+} - X^{\sum \alpha_i v_i^-} = X^{w_1^1} X^{v_1^+} - X^{w_1^2} X^{v_1^-}$, con $w_1^1 = (\alpha_1 - 1)v_1^+ + \sum_{i=2}^s \alpha_i v_i^+$ y $w_1^2 = (\alpha_1 - 1)v_1^- + \sum_{i=2}^s \alpha_i v_i^-$. Por lo tanto

$$\begin{aligned} X^{\sum \alpha_i v_i^+} - X^{\sum \alpha_i v_i^-} &= X^{w_1^1} X^{v_1^+} - X^{w_1^2} X^{v_1^-} \\ &= X^{w_1^1} X^{v_1^+} - X^{w_1^1} X^{v_1^-} + X^{w_1^1} X^{v_1^-} - X^{w_1^2} X^{v_1^-} \\ &= X^{w_1^1} \underbrace{(X^{v_1^+} - X^{v_1^-})}_{\in J_C} + X^{v_1^-} (X^{w_1^1} - X^{w_1^2}) \end{aligned}$$

Si operamos de manera inductiva con $X^{w_1^1} - X^{w_1^2}$, obtenemos que $X^{\sum \alpha_i v_i^+} - X^{\sum \alpha_i v_i^-} \in J_C$, y ya hemos demostrado $I_{\mathcal{L}} \subset (J_C : (X_1 \ldots X_r)^\infty)$.

La otra inclusión es trivial, basta con recordar que el ideal cociente es binomial y probar la inclusión para binomios usando I–C.1.

Para probar la implicación recíproca, tomemos $u \in \mathcal{L}$ y su binomio asociado en $I_{\mathcal{L}}$, $X^{u^+} - X^{u^-}$. Entonces, existirá un monomio, X^a, de manera que $X^a(X^{u^+} - X^{u^-}) \in J_C$. Aplicando ahora I–C.1 tenemos $u = a + u^+ - a - u^- \in < C >$. Por lo tanto, C es un sistema de generadores de $\mathcal{L}$.

■

Centrémonos en los algoritmos de cálculo del ideal

$$(J_C : (X_1 \ldots X_r)^\infty),$$

ya que así obtenemos $I_{\mathcal{L}}$.

■ Teoría de Eliminación

El primero que referimos se basa en la Teoría de Eliminación.

Proposición I–C.3 ■ Sea $I = < f_1, \ldots, f_l >$ un ideal de R, sea $f \in R$ un polinomio no nulo, y sea $J = < f_1, \ldots, f_l, 1 - Yf >$ ideal en $k[X_1, \ldots, X_r, Y]$. Entonces, $(I : f^\infty)$ es el ideal de eliminación $J_X = J \cap R$. Además, si $\{g_1, \ldots, g_m\}$ es una base de J_X con

$$g_i = h_i(1 - Yf) + \sum_{j=1}^{l} h_{ij} f_j, \ \ (1 \leq i \leq m, h_i, h_{ij} \in k[X_1, \ldots, X_r, Y]),$$

el número

$$s = máx\{deg_Y(h_{ij}) | 1 \leq i \leq m, 1 \leq j \leq l\}$$

satisface $(I : f^\infty) = (I : f^s)$.

Demostración. Ver [BW93, pág. 266]. ∎

Para calcular el ideal $(J_C : (X_1 \dots X_r)^\infty)$, habrá pues que calcular el ideal de eliminación de $< f_1, \dots, f_l, 1 - X_1 \cdot \cdot \cdot X_r Y >$, donde $\{f_1, \dots, f_l\}$ es un sistema generador de J_C. Este cálculo se realiza mediante bases de Gröbner (ver [BW93]). Nótese que hemos pasado de trabajar en un anillo R con r variables a otro con $r+1$ variables, $k[X_1, \dots, X_r, Y]$, lo cual hace que el coste computacional aumente (eterno problema cuando tratamos de realizar cálculos usando bases de Gröbner).

Existen otros métodos basados en calcular bases de Gröbner con un menor número de variables, lo que, en general, acelera el proceso computacional.

■ Método de Sturmfels-Hosten-Shapiro

El primero que estudiamos aparece en [STU95] y puede aplicarse al caso en el cual la graduación que consideremos en el anillo R sea positiva. Esto, a nivel del retículo, se traduce en que se verifica

$$\mathcal{L} \cap \mathbb{N}^r = \{0\},$$

es decir, es Nakayama. Dicho algoritmo se basa en el siguiente lema.

Lema I–C.4 ■ Sea J un ideal homogéneo para una graduación positiva, entonces, fijado el orden reverso lexicográfico inducido por $X_1 > \cdot \cdot \cdot > X_r$, y denotando por $\mathcal{G}$ a la base de Gröbner reducida de J, se tiene que el conjunto formado por los polinomios que resultan de dividir cada elemento $f \in \mathcal{G}$ por la mayor potencia de X_r que divide a f, es una base de Gröbner de $(J : X_r^\infty)$.

Demostración. Ver [STU95, lema 12.1]. ∎

Este lema nos permite calcular el cociente respecto de una variable, pudiéndose ampliar al ideal cociente que nos interesa con el siguiente método recurrente:

$$(J : (X_1 \dots X_r)^\infty) = ((\cdots ((J : X_1^\infty) : X_2^\infty) \cdots) : X_r^\infty).$$

Esto nos obligaría a computar r bases de Gröbner para poder obtener un algoritmo que resuelva nuestro problema. Aplicando trabajos más recientes ([HS]) vemos que se puede establecer una sustancial mejora en el algoritmo recurrente anterior, ya que para computar el ideal $(J : (X_1 \dots X_r)^\infty)$ no es necesario aplicarlo r veces.

Teorema I–C.5 ■ Existe un conjunto de variables $T = \{X_{i_1}, \dots, X_{i_k}\}$ tales que

$$I_{\mathcal{L}} = ((\cdots ((J_C : X_{i_1}^\infty) : X_{i_2}^\infty) \cdots) : X_{i_k}^\infty),$$

con $k \leq \lfloor r/2 \rfloor$.

El método que se propone en [HS] para calcular el anterior conjunto T es el siguiente: sea M la matriz cuyas filas son los elementos de una base de $\mathcal{L}$, y comencemos con $T = \emptyset$. Supongamos por comodidad de notación que los primeros k_1 elementos de la primera fila de M son no nulos y el resto ceros. Además supongamos que los s_1 primeros son los positivos. Podemos suponer que $s_1 \leq \lfloor k_1/2 \rfloor$, ya que en caso contrario multiplicaríamos esta fila por menos uno. Sea $T = T \cup \{X_1, \dots, X_{s_1}\}$. Eliminamos entonces la primera fila de M y sus primeras k_1 columnas. Si la matriz resultante tiene en cada fila elementos del mismo signo, paramos. En caso contrario, asumimos que los k_2 primeros elementos de la primera fila son los no nulos, y suponemos que hay s_2 positivos colocados en las primeras columnas. De nuevo podemos considerar que $s_2 \leq \lfloor k_2/2 \rfloor$. Sea $T = T \cup \{X_{k_1+1}, \dots, X_{k_1+s_2}\}$ y repetimos el proceso. Al final tendremos un conjunto T de cardinal $s_1 + s_2 + \cdots + s_p \leq \lfloor k_1/2 \rfloor + \lfloor k_2/2 \rfloor + \cdots + \lfloor k_p/2 \rfloor \leq \lfloor r/2 \rfloor$. Este conjunto T es el que buscamos. Con las suposiciones que hemos considerado, se llega a que la matriz M es de la forma

$$\begin{pmatrix} B & 0 \\ C & D \end{pmatrix},$$

donde B es una $p \times (\sum_{j=1}^{p} k_j)$–matriz con la estructura

$$\begin{pmatrix} + & \cdots & + & - & \cdots & - & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ * & \cdots & * & * & \cdots & * & + & \cdots & + & - & \cdots & - & 0 & \cdots & 0 & 0 & \cdots & 0 \\ & \vdots & & & \vdots & & & \vdots & & & \ddots & & & \ddots & & & \ddots & \\ * & \cdots & * & * & \cdots & * & * & \cdots & * & * & \cdots & * & + & \cdots & + & - & \cdots & - \end{pmatrix},$$

y D es una matriz tal que en cada una de sus filas no hay elementos de signos distintos.

El algoritmo resultante es,

Algoritmo I–C.6 ■ Con las notaciones anteriores.

Entrada: Un conjunto de generadores C de un retículo $\mathcal{L}$ Nakayama.

Salida: Un conjunto de generadores del ideal $I_{\mathcal{L}}$.

1. Opcionalmente, reemplazar la base C por una reducida en el sentido de Lovász (ver [COH93]).
2. Sea $J_0 =< X^{u^+} - X^{u^-} : u \in C >$.
3. Computamos el conjunto de variables $T = \{X_{j_1}, \ldots, X_{j_k}\}$ (teorema I–C.5).
4. Para $i = 1, \ldots, k$, computamos $J_i = (J_{i-1} : X_{j_i}^{\infty})$ considerando el orden reverso lexicográfico siendo la variable $X_{j_i} \in T$ la menor.
5. $J_k = I_{\mathcal{L}}$.

Para aplicar este algoritmo a retículos que no verifiquen la condición $\mathcal{L} \cap \mathbb{N}^r = \{0\}$ y saturados, tenemos que usar la elevación de Lawrence (ver [BLVS$^+$93]). Para ello, consideremos una $\mathbb{Z}$–matriz $\mathcal{A}$ de manera que $\mathcal{L}$ sea el retículo asociado al sistema $\mathcal{A}x = 0$ (i.e. $\mathcal{L} = \ker(\mathcal{A})$, de ahí la necesidad de que $\mathcal{L}$ sea saturado). Llamaremos elevación de

Lawrence de $\mathcal{A}$ a la matriz

$$\mathcal{A}' := \begin{pmatrix} \mathcal{A} & 0 \\ 1 & 1 \end{pmatrix}.$$

Si una matriz tiene la forma anterior, diremos que es de Lawrence.

Las matrices $\mathcal{A}$ y $\mathcal{A}'$ tienen núcleos isomorfos verificando

$$\ker(\mathcal{A}') = \{(u, -u) \ : \ u \in \mathcal{L}\}.$$

Por lo tanto, el ideal asociado a $\ker(\mathcal{A}')$ es

$$I_{\ker(\mathcal{A}')} = < X^{u^+} Y^{u^-} - X^{u^-} Y^{u^+} \ : \ u \in \mathcal{L} >$$

en el anillo $k[X_1, \ldots, X_r, Y_1, \ldots, Y_r]$. Nótese que $\ker(\mathcal{A}')$ es un retículo Nakayama.

Por lo tanto, tenemos un algoritmo para el cálculo de un sistema de generadores del ideal de un retículo no Nakayama y saturado basado en I–C.6,

---

Algoritmo I–C.7 ■ *Entrada:* Un retículo no Nakayama y saturado $\mathcal{L}$.
Salida: Un sistema de generadores del ideal $I_{\mathcal{A}}$.

1. Calculamos $\mathcal{A}$ tal que su retículo asociado sea $\mathcal{L}$.
2. Calculamos $\mathcal{A}'$ (elevación de Lawrence de $\mathcal{A}$) y computamos un sistema de generadores $\mathcal{G}'$ de $I_{\ker(\mathcal{A}')}$ usando I–C.6.
3. Sea

$$\mathcal{G} := \{\text{binomios de } \mathcal{G}' \text{ con las variables } Y \text{ iguales a uno}\}.$$

Este conjunto es un sistema de generadores de $I_{\mathcal{L}}$.

■ Método de Di Biase-Urbanke

El último método que presentamos para el cálculo de un ideal de retículo se basa en [DBU95].

Definición I–C.8 ■ Diremos que un conjunto de vectores C' es ortogonal si para todo $u, v \in C'$: o bien $supp(u^-) = supp(v^-)$, o si existe $i_0 \in supp(u^-)$ pero $i_0 \notin supp(v^-)$, entonces $v_{i_0} = 0$.

La clave para el algoritmo que vamos a presentar está en el siguiente resultado sobre ideales de retículo.

Lema I–C.9 ■ Dado un conjunto C de generadores del retículo $\mathcal{L}$, si $C \subset \mathbb{N}^r$ o posee un elemento con todas sus coordenadas estrictamente positivas, se tiene que $I_{\mathcal{L}} = J_C$.

Demostración. Si el conjunto C verifica las hipótesis del lema, tenemos que todas las variables son inversibles módulo J_C, y por lo tanto $J_C = (J_C : (X_1 \cdot \cdot \cdot X_r)^\infty)$. ■

El algoritmo se basa en dos pasos principales:

1. **P.** Construir recursivamente a partir de $\mathcal{L}$ un serie de retículos
$$\mathcal{L}_1, \ldots, \mathcal{L}_t$$
tal que $\mathcal{L}_t$ verifique el lema I–C.9.

2. **P.** Deshacer los cambios, a nivel de los ideales asociados, a través de bases de Gröbner para llegar a obtener $I_{\mathcal{L}}$.

Un resultado muy importante para la construcción de la cadena de retículos (1. **P.**) es el siguiente.

Lema I–C.10 ■ Dado $C = \{u_1, \ldots, u_m\}$ un conjunto de generadores de $\mathcal{L}$, existe otro C' ortogonal que genera el mismo retículo.

Demostración. Un conjunto ortogonal C', viene dado por $C' := \{v_1, \ldots, v_m\}$, con $v_1 := u_1$, $v_2 := u_2 + (1 + ||u_1||_\infty)v_1$, y $v_i := u_i + (1 + ||u_{i-1}||_\infty)v_{i-1}$, $m \geq i \geq 3$. Por definición, $||u||_\infty = \text{máx}_i\{|u_i|\}$■

Realizando una serie de cambios en un sistema de generadores ortogonal de $\mathcal{L}$ (de signo en este caso), podemos construir una sucesión finita de retículos de manera que del último tengamos un sistema de generadores verificando el lema I–C.9. Los cambios de signo citados se harán mediante la aplicación,

$$\begin{array}{rccc} \phi_i : & \mathbb{Z}^r & \longrightarrow & \mathbb{Z}^r \\ & (a_1, \ldots, a_r) & \longmapsto & (a_1, \ldots, -a_i, \ldots, a_r) \end{array}$$

y los retículos y sus sistemas de generadores van a quedar definidos así: $C_i := \phi_{z_i}(C_{i-1})$ y $\mathcal{L}_i$ es el retículo generado por C_i, para ciertos $z_i \in \{1, \ldots, r\}$ que ya determinaremos más adelante.

Con las definiciones anteriores y denotando por $\mathbf{X}$ a los monomios sin la variable X_{z_i}, se tiene que un binomio $X_{z_i}^r \mathbf{X^u} - \mathbf{X^v}$ está en $I_{\mathcal{L}_i}$ si y sólo si $\mathbf{X^u} - \mathbf{X^v} X_{z_i}^r$ está en $I_{\mathcal{L}_{i-1}}$.

El paso 2. **P.** citado antes se basa en la siguiente proposición.

Proposición I–C.11 ■ Sea

$$G_i = \{X_{z_i}^{r_j} \mathbf{X^{u_j}} - \mathbf{X^{v_j}} : j = 1, \ldots, m\}$$

una base de Gröbner de $I_{\mathcal{L}_i}$ respecto a cualquier orden de eliminación para la variable X_{z_i}. Entonces,

$$G = \{\mathbf{X^{u_j}} - \mathbf{X^{v_j}} X_{z_i}^{r_j} : j = 1, \ldots, m\}$$

es un sistema de generadores de $I_{\mathcal{L}_{i-1}}$.

Demostración. Ver [STU95, proposición 12.5].

■

Para *cambiar la variable X_{z_i} de lado* como en la proposición anterior, y llegar a conseguir unos generadores del ideal retículo $I_{\mathcal{L}_{i-1}}$ que buscamos, usamos la aplicación T_{z_i}

$$T_{z_i}(X_{z_i}^r \mathbf{X^u} - \mathbf{X^v}) = \mathbf{X^u} - \mathbf{X^v} X_{z_i}^r.$$

Vistos los pasos más importantes del algoritmo, pasaremos a explicitarlo.

Algoritmo I–C.12 ■ Con las notaciones anteriores.

Entrada: Un conjunto C de generadores de $\mathcal{L}$.

Salida: Un sistema de generadores de $I_{\mathcal{L}}$.

1. Opcionalmente, reemplazar la base C por una reducida en el sentido de Lovász (ver [COH93]).
2. Construyamos C' un conjunto de generadores de $\mathcal{L}$ ortogonal.
3. Consideremos
$$A = \{a_1, \dots, a_l\} = \{supp(\nu^-) | \nu \in C'\},$$
$$C_A = \phi_{a_1}(\phi_{a_2}(\cdots(\phi_{a_l}(C')))) \subset \mathbb{N}^r,$$
y sea
$$G_A = \{X^{\nu^+} - X^{\nu^-} : \nu \in C_A\}.$$
4. Hasta que $A = \emptyset$: elegimos $a \in A$ y tomamos $G_{A \setminus \{a\}}$ el resultado de aplicar T_a a los elementos de la base de Gröbner reducida para G_A respecto del orden $X_a > \cdots$. Ahora, $A = A \setminus \{a\}$.
5. El resultado G_A es un conjunto de generadores de $I_{\mathcal{L}}$.

I–D. CÁLCULO DE IDEALES DE SEMIGRUPOS

Volvamos sobre nuestro semigrupo

$$S \subset \mathbb{Z}^h \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z},$$

donde $a_1, \dots, a_s$ son enteros no nulos. Consideremos $\{n_1, \dots, n_r\}$ un conjunto de generadores del semigrupo.

El lema I–B.1 es una pieza clave para aplicar las técnicas de las secciones anteriores al cálculo de ideales de semigrupos con torsión. Para eliminar la torsión construimos un nuevo semigrupo $S' \subset \mathbb{Z}^{h+s}$ asociado a S.

Sean $n'_i = n_i$, $\forall i \in \{1, \ldots, r\}$ (considerando los generadores de S en $\mathbb{Z}^{h+s}$), y sean también

$$n'_i = (\underbrace{0, \ldots, 0}_{h}, \underbrace{0, \ldots, 0, a_{i-r}, 0, \ldots, 0}_{s})$$

para $i \in \{r+1, \ldots, r+s\}$, donde a_{i-r} ocupa la coordenada $j = i - r + h$.

Denotemos S' al semigrupo de $\mathbb{Z}^{h+s}$ generado por $\{n'_1, \ldots, n'_{r+s}\}$.

■ Algoritmo Algebraico

Sea $\ker(S')$ el retículo formado por las soluciones enteras del sistema

$$(n'_1 | \ldots | n'_{r+s}) \begin{pmatrix} x_1 \\ \vdots \\ x_{r+s} \end{pmatrix} = 0.$$

Es evidente el siguiente resultado,

Lema I–D.1 ■ Dado un sistema de generadores C' de $\ker(S') \subset \mathbb{Z}^{r+s}$, el conjunto C que resulta de proyectar C' en las r primeras coordenadas, es un sistema de generadores de $\ker(S) \subset \mathbb{Z}^r$.

Así obtenemos un algoritmo puramente algebraico para calcular el ideal de un semigrupo con torsión.

Algoritmo I–D.2 ■ Con las notaciones anteriores:

Entrada: Un sistema de generadores de S, $\{n_1, \ldots, n_r\}$.

Salida: Un sistema de generadores del ideal de S.

1. Calculamos el semigrupo S'.
2. Calculamos un conjunto de generadores C' del retículo $\ker(S')$.
3. Proyectamos los elementos de C' sobre $\mathbb{Z}^r$, y obtenemos C un sistema de generadores del retículo $\ker(S)$.

4. De C obtenemos un sistema de generadores de $I = I_{\ker(S)}$ mediante algún algoritmo de cálculo de ideales de retículo.

Veamos en la siguiente sección, un algoritmo basado en un resultado geométrico para calcular el ideal de un semigrupo con torsión. Su estudio explica por qué los ideales de semigrupos con torsión no son necesariamente primos.

■ Algoritmo Geométrico

Sean S y S' como en la sección anterior, y sea I' el ideal de S'.

Lema I–D.3 ■ Sea B' un conjunto de generadores de I' formado por binomios con coeficientes 1 y -1. Entonces, el conjunto B que resulta de hacer uno las variables $\{X_i\}_{i=r+1}^{r+s}$ en los elementos de B', es un sistema de generadores de I.

Demostración. En primer lugar veamos que B está incluido en I. Sea $f \in B$, entonces, existe $f' \in B'$ tal que $f = f'(X_1, \ldots, X_r, 1, \ldots, 1)$, con $f' = X^{\alpha'} - X^{\beta'}$, donde $\alpha', \beta' \in \mathbb{N}^{r+s}$ y $\sum_{i=1}^{r+s} \alpha'_i n'_i = \sum_{i=1}^{r+s} \beta'_i n'_i$. Es inmediato probar que $\sum_{i=1}^{r} \alpha'_i n_i = \sum_{i=1}^{r} \beta'_i n_i$. Por lo tanto f es un binomio de I.

Ahora probemos que B genera el ideal I. Para ello basta probar que todo binomio con coeficientes ± 1 en I puede ser expresado en función de los elementos de B. Sea $f = X^{\alpha} - X^{\beta}$ un binomio de I, entonces $\sum_{i=1}^{r} \alpha_i n_i = \sum_{i=1}^{r} \beta_i n_i$. Construiremos $f' \in I'$ tal que $f = f'(X_1, \ldots, X_r, 1, \ldots, 1)$, lo cual basta, ya que al ser B' un conjunto generador de I', tenemos que podemos expresar f' en función de los elementos de B', y por lo tanto, al hacer uno las variables $\{X_i\}_{i=r+1}^{r+s}$, tenemos f en función de los elementos de B, lo que probaría que B es un conjunto de generadores de I.

Sabemos que, denotando por n_{ij} a la j–ésima componente de n_i, $\forall j = 1, \ldots, h+s$

$$\sum_{i=1}^{r} \alpha_i n_{ij} = \sum_{i=1}^{r} \beta_i n_{ij}.$$

Si $j \in \{h+1, \ldots, h+s\}$ la igualdad anterior debe entenderse en $\mathbb{Z}/a_{j-h}\mathbb{Z}$, por lo tanto se tiene que

$$\sum_{i=1}^{r} \alpha_i n_{ij} - \sum_{i=1}^{r} \beta_i n_{ij} = l_j a_{j-n}$$

para cierto $l_j \in \mathbb{Z}$.

Definimos $\forall i = 1, \ldots, r$, $\alpha'_i = \alpha_i$ y $\beta'_i = \beta_i$, mientras que si $i = r+1, \ldots, r+s$, definimos

$$\alpha'_i = \begin{cases} -l_{i-r+h} & \text{si } l_{i-r+h} \leq 0 \\ 0 & \text{en otro caso} \end{cases}$$

$$\beta'_i = \begin{cases} l_{i-r+h} & \text{si } l_{i-r+h} > 0 \\ 0 & \text{en otro caso} \end{cases}$$

Es fácil comprobar ahora que $\sum_{i=1}^{r+s} \alpha'_i n'_i = \sum_{i=1}^{r+s} \beta'_i n'_i$ y que con $f' = X^{\alpha'} - X^{\beta'} \in I'$ se tiene que $f = f'(X_1, \ldots, X_r, 1, \ldots, 1)$. ■

Usando este lema podemos trabajar pasando de nuestro semigrupo de partida a uno libre de torsión. La *vuelta* al semigrupo inicial se realizará a nivel del ideal y no del retículo como en el algoritmo I–D.2 haciendo uno las variables introducidas con los nuevos generadores de S'.

Algoritmo I–D.4 ■ Con las notaciones anteriores:

Entrada: Un sistema de generadores de S, $\{n_1, \ldots, n_r\}$.

Salida: Un sistema irreducible de generadores del ideal de S, indicando si S es o no Nakayama.

1. Calculamos el semigrupo S'.
2. Calculamos un conjunto de generadores B' de I' (algoritmo I–C.12).
3. Hacemos uno las variables $\{X_i\}_{i=r+1}^{r+s}$ en B' y obtenemos B un sistema de generadores de I.
4. De B obtenemos un sistema irreducible de generadores de I.

Este algoritmo es computacionalmente menos eficiente que I–D.2 ya que añade nuevas variables al cálculo, pero da una visión más geométrica de la estructura de los ideales de semigrupos con torsión. De hecho, nos da una explicación de por qué los ideales de semigrupos con torsión no son primos en general. Esto se debe a que dicho ideal lo obtenemos a partir de uno primo ($I_{S'}$) mediante intersecciones con hipersuperficies ($\{X_j = 1\}$), lo cual no da necesariamente un ideal primo.

I–E. NOTAS

En este capítulo hemos presentado dos tipos de algoritmos: unos calculan el ideal de un retículo y otros el de un semigrupo.

De entre los primeros, existen estudios que realizan una comparativa sobre ideales de retículos Nakayama y saturados (ver por ejemplo [HS95]). Estas comparaciones son anteriores a la mejora realizada en [HS] (algoritmo I–C.6), y de ellas se deducía que para ese tipo de retículos ambos algoritmos eran de un eficiencia similar. Por lo tanto, cabe pensar ahora que el algoritmo I–C.6 es más eficiente, en cuanto a tiempo de cómputo, que I–C.12. Además, en [BLSR99] (implementado en CoCoA [CoC]) se da un algoritmo paralelizado de I–C.6 el cual optimiza aún más ese algoritmo.

En el caso de un retículo no Nakayama, el más eficiente es I–C.12 debido a que no hay que usar la elevación de Lawrence y por lo tanto siempre estamos trabajando en un anillo de polinomios en r variables, frente a las $2r$ variables necesarias para aplicar I–C.7. El algoritmo I–C.12 es el más recomendable para usar si no conocemos la naturaleza del retículo, es decir, si es o no Nakayama o saturado.

En cuanto a los ideales de semigrupos con torsión, sólo existía hasta la aparición de [PCVT96] una referencia a ese cálculo en [BCMP98b], pero dicho algoritmo usaba métodos combinatorios que en la práctica resultan del todo ineficientes, además de que sólo es aplicable a semigrupos Nakayama. Un algoritmo posterior a [PCVT96] aparece en

[RUB96]. En [RGS98] encontramos otro algoritmo donde se aborda el problema desde el cálculo de $\mathbb{N}$–soluciones de un sistema diofántico. Entre el algoritmo I–D.2 (publicado en [VT99]) y el aparecido en [RGS98] no se han realizado estudios comparativos respecto de la eficacia de ambos.

El algoritmo I–C.12 lo hemos implementado en MapleV3 y puede ser obtenido vía ftp en

`ftp.uca.es/pub/matematicas/semigrou1.zip`

CAPÍTULO II

Sistemas diofánticos: $\mathbb{N}$–soluciones

II–A. INTRODUCCIÓN

En este capítulo vamos a realizar un pequeño recorrido a través de distintos métodos que calculan $\mathbb{N}$–soluciones de un sistema diofántico. Además damos nuevos algoritmos para calcular $\mathbb{N}$–soluciones de sistemas diofánticos en congruencias.

Comencemos considerando el sistema diofántico homogéneo $Gx = 0$, con $G \in \mathcal{M}_{m\times r}(\mathbb{Z})$.

Es conocido desde finales del siglo XIX ([GOR73], [HIL90]) que las soluciones enteras positivas ($\mathbb{N}$–soluciones) de un sistema de ecuaciones homogéneas diofánticas forman un semigrupo S con elemento neutro y finitamente generado, existiendo un único sistema minimal de generadores tal que cualquier $\mathbb{N}$–solución puede ser expresada como una combinación lineal con coeficientes enteros positivos de los elementos de dicho conjunto. A este conjunto se le denomina *base de Hilbert* y se le denota por $\mathcal{H}(S)$ ó $\mathcal{H}S$.

Denotaremos por $\gg$ al orden parcial natural sobre $\mathbb{N}^r$, es decir, dadas dos uplas de números enteros α y α', diremos que α es $\gg$ –mayor que α' ($\alpha \gg \alpha'$) si todos los elementos de $\alpha - \alpha'$ son enteros no negativos y al menos uno es no nulo. Sea $L \subset \mathbb{N}^r$, diremos que $\alpha \in L$ es $\gg$ –minimal en L si $\forall \alpha' \in L \setminus \{\alpha\}$, $\alpha \not\gg \alpha'$. Denotaremos por $\mathcal{H}(L)$ ó $\mathcal{H}L$ al conjunto

- si $L \neq \{0\}$, $\mathcal{H}L$ es el conjunto de elementos $\gg$ –minimales en $L \setminus \{0\}$,
- si $L = \{0\}$, $\mathcal{H}L := \{0\}$.

El lema de Dickson ([BW93, pág. 163]) nos garantiza la finitud de $\mathcal{H}L$. Nosotros damos en II–B.5 una versión constructiva de dicho lema para determinados subconjuntos de $\mathbb{N}^r$ a los que ya nos referiremos.

Considerando esta notación, tenemos el siguiente resultado.

Lema II–A.1 ■ Sea $\mathcal{G} = \{x \in \mathbb{N}^r | \, Gx = 0\}$, entonces $\mathcal{H}\mathcal{G}$ es el sistema minimal de generadores de $\mathcal{G}$ (i.e. $\mathcal{H}\mathcal{G}$ es la base de Hilbert de $\mathcal{G}$).

En el caso de que el sistema sea no homogéneo, $Gx = b$, con $b \in \mathbb{Z}^m$, las $\mathbb{N}$–soluciones pueden ser escritas como la unión finita de subconjuntos de $\mathbb{N}^r$. Estos subconjuntos están formados por la suma de una $\mathbb{N}$–solución $\gg$ –minimal y el conjunto de $\mathbb{N}$–soluciones del sistema homogéneo asociado, como vemos en el lema siguiente.

Lema II–A.2 ■ Sea $\mathcal{G}'$ el conjunto $\{x \in \mathbb{N}^r | \, Gx = b\}$, y sea $\mathcal{G} = \{x \in \mathbb{N}^r | \, Gx = 0\}$. Entonces

$$\mathcal{G}' = \bigcup_{x \in \mathcal{H}\mathcal{G}'} (x + \mathcal{G}).$$

Resolver un sistema no homogéneo se reduce habitualmente a resolver un sistema homogéneo con una incógnita más. Este paso nos lo permite la siguiente nota.

Nota II–A.3 ■ Sistemas no homogéneos.

- $\mathcal{H}\mathcal{G}' = \mathcal{H}\{x \in \mathbb{N}^r \,|\, (G| - b)(x, 1) = 0\}$.
- Si $\mathcal{G}'' = \{x \in \mathbb{N}^{r+1} \,|\, (G| - b)x = 0\}$, entonces

$$\mathcal{H}\mathcal{G}' = \{x \in \mathbb{N}^r \,|\, (x, 1) \in \mathcal{H}\mathcal{G}''\}.$$

En capítulos sucesivos, vamos a necesitar calcular tan solo $\mathbb{N}$–soluciones minimales más grandes que un elemento fijo dado $e \gg 0$. Esto lo haremos mediante la siguiente nota, pasando a resolver el problema calculando $\mathbb{N}$–soluciones de un sistema no homogéneo.

Nota II–A.4 ■ Sea $e \in \mathbb{N}^r$ y sea

$$\mathcal{G}_e := \{x \in \mathbb{N}^r | Gx = 0, x \gg e\}.$$

Para calcular $\mathcal{H}\mathcal{G}_e$, usaremos que $\mathcal{G}_e = \mathcal{G}'_e + e$, y $\mathcal{H}\mathcal{G}_e = \mathcal{H}\mathcal{G}'_e + e$ con

$$\mathcal{G}'_e := \{x \in \mathbb{N}^r | G(x + e) = 0\}.$$

Por lo tanto, una vez obtenido $\mathcal{H}\mathcal{G}'_e$ (soluciones de un sistema no homogéneo), le sumaremos a cada uno de sus elementos la upla e. El resultado de esa suma será $\mathcal{H}\mathcal{G}_e$.

II–B. CÁLCULO DE LA $\mathbb{N}$–SOLUCIÓN GENERAL

Para encontrar un sistema de generadores de las $\mathbb{N}$–soluciones de un sistema diofántico, aparecen en la bibliografía matemática varios métodos. Entre ellos vamos a destacar aquellos que más han influido en la elaboración de esta memoria. Los dividiremos en distintas secciones en función de la filosofía de cada método.

■ Búsqueda Exhaustiva

Este método se basa en la realización de una búsqueda exhaustiva (o barrido) de las $\mathbb{N}$–soluciones en una región del espacio. Dicha región viene determinada por una cota para las coordenadas de los elementos de un sistema de generadores de las $\mathbb{N}$−soluciones. El método consiste en, una vez obtenida una cota, comprobar qué uplas de elementos enteros positivos (determinados por las cotas) verifican las ecuaciones. Después, nos quedamos sólo con los elementos $\gg$ −minimales de ese conjunto. El principal problema de este método es el enorme tamaño de las cotas conocidas hasta el momento. En esta memoria sólo vamos a dar algunos ejemplos de estas cotas (ver [TOM97] si se desea ampliar esta información). Para ello, vamos a considerar los sistemas

$$Gx = b, Gx = 0, \text{ con } G = (g_{ij}) \in \mathcal{M}_{m\times r}(\mathbb{Z}), rg(G) = m \text{ y } r \geq m. \qquad \text{(II–B.1)}$$

Denotamos por $\mathcal{HG}'$ y por $\mathcal{HG}$ a los respectivos conjuntos de $\mathbb{N}$−soluciones minimales. La norma uno ($|| \cdot ||_1$) de un conjunto se define como el máximo de las normas uno de cada elemento del conjunto, siendo la norma uno de una upla la suma de los valores absolutos de sus coordenadas. Para una matriz, $A = (a_{ij})$, definimos su norma uno como $||A||_1 = \text{máx}_i \sum_j |a_{ij}|$.

En [STU91] el autor prueba que

$$||\mathcal{HG}||_1 \leq (m+1)(r-m)\,\text{máx}\{|\text{ menores de orden } m\times m \text{ de } G|\}. \qquad \text{(II–B.2)}$$

Para ello se usan técnicas relacionadas con ideales de retículos y la relación de estos ideales con los sistemas diofánticos.

En [POT91] aparecen varias cotas. Entre ellas consideramos la siguiente

$$||\mathcal{HG}||_1 \leq (1 + \max_{1\leq i\leq m} \sum_{j=1}^{r} |g_{ij}|)^m, \qquad \text{(II–B.3)}$$

y una un poco más pequeña en general,

$$||\mathcal{HG}||_1 \leq \prod_{i=1}^{m}(1 + \sum_{j=1}^{r} |g_{ij}|). \qquad \text{(II–B.4)}$$

Las cotas anteriores (II–B.4) y (II–B.2) no son comparables en general, existiendo ejemplos particulares donde una es mayor que la otra, y viceversa. Por ejemplo, si consideramos la matriz

$$\begin{pmatrix} 8 & 4 & -5 & -5 \\ 3 & -5 & 8 & 5 \end{pmatrix}$$

obtenemos que la cota (II–B.2) vale 474, que (II–B.4) vale 506. Sin embargo, si consideramos la matriz

$$\begin{pmatrix} -1 & 0 & 3 & -4 \\ -5 & -2 & -1 & -9 \end{pmatrix}$$

tenemos que (II–B.2) vale 186 mientras que (II–B.4) vale 162.

■ Método de Clausen-Fortenbacher

En [CF89] aparece un algoritmo para calcular $\mathbb{N}$–soluciones a una única ecuación diofántica homogénea, abriendo la puerta a una serie de trabajos posteriores que utilizan este algoritmo como punto de partida.

Consideremos una única ecuación diofántica homogénea

$$dx \equiv g_1x_1 + g_2x_2 + \cdots + g_rx_r = 0.$$

La idea que aparece en [CF89] es construir las $\mathbb{N}$–soluciones $\gg$ –minimales de esta ecuación a partir de la base canónica de $\mathbb{N}^r$, $\{e_1, \ldots, e_r\}$. Partiendo de $(0, \ldots, 0)$ podemos ir incrementando las coordenadas hasta llegar a una $\mathbb{N}$–solución o a un vector mayor que una $\mathbb{N}$–solución. Como es de suponer, esta idea tiene que ir acompañada de alguna condición *inteligente* que limite las coordenadas que van a ser incrementadas para obtener un método que, además de efectivo, sea eficiente. Esas condiciones para incrementar una coordenada son:

1. Si $g_1x_1 + g_2x_2 + \cdots + g_rx_r < 0$, entonces incrementamos en 1 alguna coordenada x_i tal que $g_i > 0$,
2. Si $g_1x_1 + g_2x_2 + \cdots + g_rx_r > 0$, entonces incrementamos en 1 alguna coordenada x_i tal que $g_i < 0$.

El método consiste en *dirigir* de forma *inteligente* la búsqueda de las $\mathbb{N}$–soluciones minimales en las *direcciones correctas*.

Algoritmo II–B.1 ■ Algoritmo de Clausen-Fortenbacher.
Entrada: La ecuación $dx \equiv g_1x_1 + g_2x_2 + \cdots + g_rx_r = 0$.
Salida: La base de Hilbert de las soluciones de la ecuación.

1. $P := \{e_1, \ldots, e_r\}$ y $B := \emptyset$.
2. Mientras $P \neq \emptyset$ haz
   a) $B = B \cup \{x \in P | dx = 0\}$.
   b) $L := \{x \in P \setminus B | x$ minimal en $B \cup \{x\}\}$.
   c) $P = \{x + e_i | x \in L,\ dx > 0,\ de_i < 0\} \cup \{x + e_i | x \in L,\ dx < 0,\ de_i > 0\}$.
3. B es la base de Hilbert de las $\mathbb{N}$–soluciones de $dx = 0$.

La prueba de que el algoritmo anterior es correcto aparece en [CF89] y se puede resumir en el siguiente teorema.

Teorema II–B.2 ■ El algoritmo II–B.1 calcula la base de Hilbert de $dx = 0$ en un número finito de pasos.

Demostración. Ver [CF89, lemas 3, 4 y 5]. ■

■ Reducción de número de ecuaciones

Hasta finales de los años ochenta, los estudios sobre la computación de $\mathbb{N}$–soluciones de sistemas diofánticos se centraron en realizar este cálculo sobre una única ecuación. Principalmente las líneas en la computación sobre una ecuación se basaban en la búsqueda exhaustiva siguiendo los trabajos de [HUE78] y [LAM87], y la búsqueda dirigida dada por [CF89]. Hasta ese momento ninguna de estos dos enfoques resolvía el problema para un sistema con más de una ecuación.

La solución que se daba era la siguiente: sea (*Sist*) un sistema de n ecuaciones

$$\begin{cases} Q &= 0 \quad \text{una ecuación} \\ A &= 0 \quad n-1 \text{ ecuaciones} \end{cases}$$

Si consideramos $\mathcal{HB} = \{u_1, \ldots, u_k\}$ el conjunto de Hilbert de $Q = 0$, todas las soluciones de (*Sist*) pueden escribirse como una combinación lineal con coeficientes enteros positivos, $c_1u_1 + \cdots + c_ku_k$. Sustituyendo esta combinación en $A = 0$, obtenemos un nuevo sistema $A' = 0$ con $n - 1$ ecuaciones cuyas variables son $c_1, \ldots, c_k$. Si tenemos una base de Hilbert del sistema $A' = 0$, sustituimos en $c_1u_1 + \cdots + c_ku_k$ y obtenemos un sistema de generadores de las $\mathbb{N}$–soluciones de (*Sist*). Como este sistema incluye una base de Hilbert de (*Sist*), tan sólo tenemos que considerar los elementos $\gg$ –minimales para obtener dicha base. Este método se usa de manera recurrente hasta que el sistema se haya reducido a una única ecuación, caso en el cual se podían usar los métodos existentes para una ecuación.

Método de Contejean-Devie

En [CD94], los autores generalizan el algoritmo II–B.1 de una ecuación a cualquier sistema de ecuaciones diofánticas.

Sea $Gx = 0$ el sistema diofántico con $G \in \mathcal{M}_{m\times r}(\mathbb{Z})$. Denotaremos por $G(x)$ al vector Gx y por $G(x + e_i)$ a $Gx + Ge_i$, lo que equivale a incrementar en uno la coordenada i–ésima de x y multiplicar el nuevo vector por G.

Vamos a aplicar aquí la idea de la *dirección correcta* de Clausen-Fortenbacher para encontrar una $\mathbb{N}$–solución del sistema. En este caso, partiendo de la solución trivial, vamos a ir incrementando las coordenadas en la dirección e_i tal que $G(x + e_i)$ esté en el semiespacio que contiene al origen, está determinado por el hiperplano afín ortogonal con $G(x)$ y contiene a dicho punto. Esta condición queda escrita como sigue:

- incrementar la coordenada x_i en 1 si $G(x) \cdot G(e_i) < 0$.

Esto nos permite restringir el espacio de búsqueda de las $\mathbb{N}$–soluciones minimales sin perder ninguna. Nótese que en el caso de una sola ecuación, obtenemos la condición dada por Clausen-Fortenbacher.

Mediante esta condición obtenemos un algoritmo para calcular la base de Hilbert de un sistema diofántico homogéneo.

Algoritmo II–B.3 ■ Algoritmo de Contejean-Devie.
Entrada: Un sistema homogéneo $Gx = 0$.
Salida: La base de Hilbert $\mathcal{G}$.

1. $P := \{e_1, \ldots, e_r\}$ y $B := \varnothing$.
2. **Mientras** $P \neq \varnothing$:
   a) $B = B \cup \{x \in P | G(x) = 0\}$.
   b) $L := \{x \in P \setminus B | \forall s \in B \; x \not\gg s\}$.
   c) $P = \{x + e_i | x \in L, \; G(x) \cdot G(e_i) < 0\}$.
3. B es la base de Hilbert de las $\mathbb{N}$–soluciones de $Gx = 0$.

La prueba de que el algoritmo anterior es correcto aparece en [CD94] y se puede resumir en el siguiente teorema.

Teorema II–B.4 ■ El algoritmo II–B.3 calcula la base de Hilbert de $Gx = 0$ en un número finito de pasos.

Demostración. Ver [CD94, proposiciones 1 y 2]. ■

Para resolver un sistema no homogéneo los autores recurren a resolver un sistema homogéneo ampliado con el término independiente, y después toman sólo las $\mathbb{N}$–soluciones con la última coordenada igual a uno (II–A.3).

Además en [CD94] los autores dan una revisión de este algoritmo usando las estructuras de pilas, de lo cual resulta un algoritmo más eficiente en espacio y tiempo, aunque de la misma naturaleza.

■ $\mathbb{N}$–solución general mediante el Lema de Dickson

En esta sección vamos a dar un método que usa el lema de Dickson para calcular de forma recurrente el conjunto de generadores minimales de un subconjunto de $\mathbb{N}^r$ que verifique ciertas propiedades. Dicho resultado lo aplicaremos a obtener la $\mathbb{N}$–solución general a un sistema diofántico.

Dado $L \subset \mathbb{N}^r$ denotaremos por $L(i, \alpha) := \{\beta \in L | \beta_i = \alpha\}$.

Lema II–B.5 ■ (Lema de Dickson) Sea $L \subset \mathbb{N}^r$, $s = (s_1, \ldots, s_r) \in L$, y sea F el conjunto

$$F = \{s\} \cup \bigcup_{i=1}^{r} \bigcup_{\alpha=0}^{s_i-1} \mathcal{H}L(i, \alpha).$$

Entonces, $\mathcal{H}L = \mathcal{H}F$.

Demostración. Es suficiente probar que

$$\forall \delta \in L, \exists \gamma \in F \text{ con } \delta \gg \gamma,$$

ya que trivialmente $F \subset L$.

Sea $\delta \in L$, si $\delta \gg s$ no hay nada que probar. En otro caso, existe un índice i tal que $\delta_i < s_i$. Entonces para $\alpha = \delta_i$, $\delta \in L(i, \alpha)$ y por lo tanto existe $\gamma \in \mathcal{H}L(i, \alpha)$ con $\gamma \ll \delta$. ■

Podemos considerar $L(i, \alpha)$ como un subconjunto de $\mathbb{N}^{r-1}$ y aplicar de nuevo el lema anterior para obtener así $\mathcal{H}L(i, \alpha)$. En los distintos pasos de la recurrencia, llegamos a que tenemos que obtener distintos conjuntos $\mathcal{H}L'$ con

$$L' = L(i_1, \alpha_1)(i_2, \alpha_2) \cdot \cdot \cdot (i_k, \alpha_k) \subset \mathbb{N}^{r-k},$$

para determinados $\alpha_j \in \mathbb{N}$, $1 \leq i_j \leq r$ y $1 \leq j \leq k \leq r$.

Corolario II–B.6 ■ $\mathcal{H}L$ es finito.

Demostración. En el último paso de la recurrencia llegamos a un subconjunto L' de $\mathbb{N}$. Como $\mathbb{N}$ es un conjunto bien ordenado, $\mathcal{H}L'$ es vacío o tiene un único elemento, en particular es finito. Trivialmente, por la recurrencia de II–B.5, tenemos que $\mathcal{H}L$ es finito, por ser una unión finita de conjuntos finitos. ■

El lema II–B.5 será constructivo si son decidibles dos aspectos:

- si L y los distintos L' son vacíos o no;
- si un elemento pertenece a L o a algún L'.

Un subconjunto de $\mathbb{N}^k$ diremos que es constructible si en él son decidibles las dos cuestiones anteriores. Si un conjunto es constructible, podemos ir tomando los elementos s que nos hacen falta para aplicar de forma recurrente el lema anterior, sólo hay que usar la numerabilidad de $\mathbb{N}^k$.

En nuestro caso, tenemos que aplicar este resultado a las $\mathbb{N}$–soluciones de un sistema diofántico. En este contexto, todos los conjuntos que empleamos son constructibles, y la manera de saber si son vacíos o no, y de encontrar un elemento que pertenezca a ellos, se traduce en calcular $\mathbb{N}$–soluciones particulares a sistemas diofánticos.

En el siguiente algoritmo, el cálculo de las $\mathbb{N}$–soluciones particulares se pueden realizar mediante cualquier método.

Algoritmo II–B.7 ■ $\mathbb{N}$–soluciones minimales de un sistema diofántico.

Entrada: La matriz de coeficientes y el término independiente $Gx = b$. Sea r el número de columnas de G.
Salida: $\mathcal{HG}'$, con $\mathcal{G}' = \{\alpha \in \mathbb{N}^r | G\alpha = b\}$.

1. Si $r = 1$, tenemos sólo una incógnita y la solución es trivial.
2. Si $r \geq 2$, determinamos si $\mathcal{G}'$ es vacío o no usando el algoritmo que queramos.
3. Si $\mathcal{G}'$ es vacío, devolvemos $\mathcal{HG}' = \emptyset$ y terminamos.
4. En otro caso, sea $s = (s_1, \ldots, s_r) \in \mathcal{G}'$.
5. Para $i = 1, \ldots, r$ y $\alpha = 0, \ldots, s_i - 1$, calculamos $\mathcal{HG}'(i, \alpha)$ usando de manera recurrente el algoritmo II–B.7.

6. Calculamos el conjunto $\mathcal{H}F$, con

$$F = \{s\} \cup \bigcup_{i=1}^{r} \bigcup_{\alpha=0}^{s_i-1} \mathcal{H}\mathcal{G}'(i, \alpha).$$

7. Devolvemos $\mathcal{H}\mathcal{G}' = \mathcal{H}F$.

Aplicando el algoritmo anterior a un sistema diofántico no homogéneo y a su sistema homogéneo asociado, obtenemos un algoritmo que nos calcula la $\mathbb{N}$–solución general a un sistema diofántico no homogéneo.

Algoritmo II–B.8 ■ $\mathbb{N}$–solución general a un sistema diofántico.
Entrada: El sistema $Gx = b$.
Salida: El conjunto, $\mathcal{G}'$, de las $\mathbb{N}$–soluciones de $Gx = b$.

1. Determinamos $\mathcal{G} = \{\alpha \in \mathbb{N}^r | G\alpha = 0\}$, usando II–B.7.
2. Determinamos $\mathcal{H}\mathcal{G}'$, con $\mathcal{G}' = \{\alpha \in \mathbb{N}^r | G\alpha = b\}$, usando II–B.7.
3. La salida es

$$\mathcal{G}' = \bigcup_{\alpha \in \mathcal{H}\mathcal{G}'} (\alpha + \mathcal{G}).$$

Los algoritmos II–B.7 y II–B.8 pueden ser paralelizados al ser independientes los cálculos de los distintos conjuntos que aparecen en las uniones, con lo que su tiempo de cómputo podría ser mejorado en un ordenador con múltiples procesadores.

II–C. CÁLCULO DE UNA $\mathbb{N}$–SOLUCIÓN PARTICULAR

Los anteriores métodos calculan la $\mathbb{N}$–solución general de un sistema de ecuaciones diofánticas. En particular, también son capaces de detectar si un sistema tiene o no $\mathbb{N}$–solución, y dar una.

Existen métodos dedicados estrictamente a resolver este problema y que pasamos a describir a continuación.

■ Lema de Farkas para sistemas homogéneos

El método que vamos a presentar a continuación nos permite saber de manera rápida si un sistema diofántico homogéneo tiene o no alguna $\mathbb{N}$–solución.

Si el sistema de partida es homogéneo (como es el caso), es equivalente estudiar la existencia de $\mathbb{N}$–soluciones que estudiar la existencia de soluciones en $\mathbb{Q}^+$. Supongamos entonces que L es el $\mathbb{Q}$–espacio vectorial de las soluciones del sistema homogéneo (II–B.1). Supongamos también que $\{c_1, \cdots, c_q\} \subset \mathbb{Q}^r$ es una base de L, y denotemos por C a la $(q \times r)$-matriz cuyas filas son $\{c_1, \ldots, c_q\}$. Llamemos $v_1, \ldots, v_r \in \mathbb{Q}^q$ a las columnas de C. Nótese que existe $u \in L \cap (\mathbb{Q}^+)^r$ no nulo si y sólo si existe $w = (w_1, \ldots, w_q) \in \mathbb{Q}^q$ con $w \cdot v_i \geq 0$, y al menos uno de estos productos es estrictamente positivo. La relación entre $u \in L \subset \mathbb{Q}^r$ y $w \in \mathbb{Q}^q$ es la siguiente

$$u = w_1 c_1 + \cdots + w_q c_q = (w \cdot v_1, \ldots, w \cdot v_r).$$

Una vez colocados en este punto, nos basta con aplicar la siguiente versión constructiva del lema de Farkas.

Proposición II–C.1 ■ Sean $v_1, \ldots, v_r \in \mathbb{Q}^q$. Existe un algoritmo para decidir si existe o no un vector $w \in \mathbb{Q}^q$ tal que $w \cdot v_1 > 0$ y $w \cdot v_i \geq 0$, $\forall i = 2, \ldots, r$. En el caso de existencia, dicho algoritmo nos da un tal vector w.

Demostración. La prueba la haremos de manera recurrente sobre r.

Supongamos que $r = 1$. Si $v_1 = 0$, no existe solución. En otro caso, $v_{1i} \neq 0$, para algún i. Tomando $w \in \mathbb{Q}^q$ con todas las coordenadas nulas salvo la i–ésima igual a $\frac{v_{1i}}{|v_{1i}|}$, ya hemos encontrado el w que buscamos.

Supongamos que $r \geq 2$.

Si no existe $p \in \mathbb{Q}^q$ tal que $p \cdot v_1 > 0$ y $p \cdot v_i \geq 0$, $\forall i = 2, \ldots, r-1$, no existe w y por lo tanto no existe solución. Caso de que sí exista p, y $p \cdot v_r \geq 0$, tomamos $w = p$, y habríamos terminado.

Consideremos entonces que existe p pero $p \cdot v_r < 0$. Definimos unos nuevos vectores v'_i de la manera siguiente:

$$v'_i = v_i - \frac{p \cdot v_i}{p \cdot v_r} v_r, \ \ \forall i = 1, \ldots, r-1. \qquad \text{(II–C.1)}$$

Si existe $p' \in \mathbb{Q}^q$ tal que $p' \cdot v'_1 > 0$, y $p' \cdot v'_i \geq 0$, $\forall i = 2, \ldots, r-1$, es suficiente considerar

$$w = p' - \frac{p' \cdot v_r}{p \cdot v_r} p,$$

ya que $w \cdot v_i = p' \cdot v'_i$, $\forall i = 1, \ldots, r{-}1$ y $w \cdot v_r = 0$. En cualquier caso, hemos probado que existe un vector w verificando la proposición. Veamos que en otro caso ($\nexists p'$) no existe w.

Supongamos que $r = 2$, como no existe p', tenemos que $v'_1 = 0$. Entonces $v_1 = \lambda v_2$, con $\lambda = \frac{p \cdot v_1}{p \cdot v_2} < 0$ y por lo tanto no existe w (de existir, $0 < w \cdot v_1 = \lambda w \cdot v_2 \leq 0$, lo cual es imposible).

Vamos a suponer el resultado cierto para cualquier entero menor que r. Si no existe p', existirá l, un entero entre 1 y $r-1$, tal que para cualquier $j = 1, \ldots, l-1$, existe $l_j > l_{j-1}$ y una colección de vectores $p_j, v_1^{(j)}, \ldots, v_{l_j}^{(j)} \in \mathbb{Q}^q$ verificando:

1. $v_i^{(1)} = v'_i$, $\forall i = 1, \ldots, r-1$.
2. $p_j \cdot v_1^{(j)} > 0$, $p_j \cdot v_i^{(j)} \geq 0$, $p_j \cdot v_{l_j}^{(j)} < 0$, $\forall i = 2, \ldots, l_j - 1$.
3. $v_i^{(j+1)} = v_i^{(j)} - \frac{p_j \cdot v_i^{(j)}}{p_j \cdot v_{l_j}^{(j)}} v_{l_j}^{(j)}$, $1 \leq i \leq l_j - 1$.
4. $v_1^{(l)} = 0$.

Denotemos

$$\lambda_i^{(1)} = -\frac{p \cdot v_i}{p \cdot v_r}, \ \ i = 1, \ldots, r-1,$$

y

$$\lambda_i^{(j+1)} = -\frac{p_j \cdot v_i^{(j)}}{p_j \cdot v_{l_j}^{(j)}}, \ \ j = 1, \ldots, l-1, \ \ i = 1, \ldots, l_j - 1.$$

($\lambda_i^{(j)} \geq 0, \lambda_1^{(j)} > 0, \ \ \forall i \neq 1, \forall j.$)

Vamos a probar que

$$v_i^{(j)} = v_i + \sum_{h=i+1}^{r} \mu_{ih}^{(j)} v_h, \text{ con } \mu_{ih}^{(j)} \geq 0 \ \forall h = i+1, \ldots, r,$$

$\forall j = 1, \ldots, l, \ \forall i = 1, \ldots, l_j$.

Veámoslo por inducción en j. Para $j = 1$, es suficiente ver que de (II–C.1) se tiene:

$$v_i^{(1)} = v_i' = v_i + \lambda_i^{(1)} v_r.$$

Supongámoslo cierto para j, y probémoslo para $j+1$. Sabemos, por la definición de $v_i^{(j+1)}$, que

$$v_i^{(j+1)} = v_i^{(j)} + \lambda_i^{(j+1)} v_{l_j}^{(j)}, \ 1 \leq i \leq l_j - 1.$$

Usando la hipótesis de inducción, podemos escribir

$$v_i^{(j)} = v_i + \sum_{h=i+1}^{r} \mu_{ih}^{(j)} v_h,$$

y

$$v_{l_j}^{(j)} = v_{l_j} + \sum_{h=l_j+1}^{r} \mu_{l_j h}^{(j)} v_h,$$

y obtenemos el resultado.

Ahora como $v_1^{(l)} = 0$, tenemos

$$v_1 = -\sum_{h=2}^{r} \mu_{1h}^{(l)} v_h, \text{ con } \mu_{1h}^{(l)} \geq 0.$$

De aquí se deduce trivialmente que no existe w. ∎

De la propia demostración, obtenemos un algoritmo.

Algoritmo II–C.2 ∎ Algoritmo de Farkas ([ROS95]).
Entrada: Unos vectores $v_1, \ldots, v_r \in \mathbb{Q}^q$.
Salida: Un vector, si existe, $w \in \mathbb{Q}^q$, tal que $w \cdot v_1 > 0$, y $w \cdot v_i \geq 0, \ i = 2, \ldots, r$. Caso de no existir w, devuelve $\emptyset$.

1. Si $r = 1$:

   a) Si $v_1 = 0$, devolver $\emptyset$.

b) En otro caso, devolver $w \in \mathbb{Q}^q$ un vector con todas las coordenadas nulas salvo la i–ésima con v_{1i}, y $v_{1i} \neq 0$.

2. Si $r \geq 2$: determina si existe $p \in \mathbb{Q}^q$ tal que $p \cdot v_1 > 0$ y $p \cdot v_i \geq 0$ para i desde 2 hasta $r-1$, para ello usar de manera recurrente el algoritmo II–C.2.

3. Si no existe p, devolver $\emptyset$ y parar.

4. Si $p \cdot v_r \geq 0$, devolver $w = p$ y parar.

5. Sea
$$v_i' = v_i - \frac{p \cdot v_i}{p \cdot v_r} v_r, \ \forall i = 1, \ldots, r-1.$$
Determinar si existe $p' \in \mathbb{Q}^q$ tal que $p' \cdot v_1' > 0$ y $p' \cdot v_i' \geq 0$, $i = 2, \ldots, r-1$ usando de manera recurrente el algoritmo II–C.2.

6. Si existe p', devolver
$$w = p' - \frac{p' \cdot v_r}{p \cdot v_r} p$$
y parar.

7. Devolver $\emptyset$.

Ahora podemos usar este algoritmo para encontrar, caso de que exista, una $\mathbb{N}$–solución particular de un sistema diofántico homogéneo.

Algoritmo II–C.3 ■ $\mathbb{N}$–solución particular de un sistema homogéneo.
Entrada: La matriz del sistema diofántico $Gx = 0$.
Salida: Una $\mathbb{N}$–solución no trivial, u, del sistema caso de que exista, o la solución trivial si es la única.

1. Si $r = 1$, tenemos una única incógnita, luego la solución es trivial.

2. Si $r \geq 2$, sea C la matriz cuyas filas son una base del $\mathbb{Q}$–espacio vectorial dado por $Gx = 0$. Tomamos $v_1, \ldots, v_r$ las columnas de C.

3. Para $i = 1, \ldots, r$:

   a) Determinar usando el algoritmo II–C.2 si existe un vector w tal que $w \cdot v_i > 0$ y $w \cdot v_j \geq 0$, para $j \neq i, j = 1, \ldots, r$.

   b) Si existe w, sea $u' = (w \cdot v_1, \ldots, w \cdot v_r) \in \mathbb{Q}^r$. Devuelve $\frac{m}{n}u' \in \mathbb{N}^r$, con m el mínimo común múltiplo de los denominadores de u', y n el máximo común divisor de las coordenadas de mu'. Parar.

4. Devuelve $u = 0$.

Lema de Farkas para sistemas no homogéneos

En [PCVT98], generalizamos el uso del lema de Farkas para encontrar $\mathbb{N}$–soluciones particulares a sistemas diofánticos no homogéneos.

Supongamos fijado el sistema diofántico no homogéneo (II–B.1). Para encontrar una $\mathbb{N}$–solución particular a dicho sistema, consideramos el sistema homogeneizado $(-b|G)x = 0$. Si sobre este sistema homogéneo, consideramos las notaciones dadas en II–C, tenemos que el sistema no homogéneo tiene una $\mathbb{N}$–solución, u, si y sólo si

$$\exists (1, u) \in L \text{ con } u \in \mathbb{N}^r,$$

y si y sólo si

$$\exists w \in \mathbb{Q}^q \text{ con } w \cdot v_1 = 1 \text{ y } w \cdot v_i \in \mathbb{N} \ \forall i = 2, \ldots, r + 1.$$

De manera análoga al caso homogéneo, la relación entre la $\mathbb{N}$–solución y w es

$$(1, u) = w_1 c_1 + \cdots + w_q c_q = (w \cdot v_1, \ldots, w \cdot v_{r+1}).$$

Por lo tanto, para poder generalizar el método basado en el lema de Farkas a sistemas no homogéneos, tenemos que resolver el siguiente problema: dados $v_1, \ldots, v_{r+1} \in \mathbb{Q}^q$, determinar si existe $w \in \mathbb{Q}^q$ tal que $w \cdot v_1 = 1$ y $w \cdot v_i \in \mathbb{N} \ \forall i = 2, \ldots, r+1$. Veamos como podemos resolverlo.

Denotaremos por W al $\mathbb{Q}$–espacio vectorial generado por $v_2, \ldots, v_{r+1}$.

Si $v_1 \notin W$, denotamos por $\hat{v}_1$ a la proyección ortogonal de v_1 en $W^\perp$. Es claro que $\hat{v}_1 \neq 0$ y $v_1 \cdot \hat{v}_1 > 0$. En este caso, es suficiente tomar

$$w = \frac{\hat{v}_1}{v_1 \cdot \hat{v}_1},$$

porque $w \cdot v_1 = 1$ y $w \cdot v_i = 0$, $\forall i = 2, \ldots, r+1$.

Si $v_1 \in W$, podemos distinguir dos subcasos:

- Si $v_1 = \sum_{i=2}^{r+1} \mu_i v_i$ con $\mu_i \leq 0$, entonces no existe w (como vimos en la demostración de II–C.1).
- En otro caso, tomamos $v_1 = \sum_{i=2}^{r+1} \mu_i v_i$. Sea A la matriz cuyas filas corresponden a los vectores $v_2, \ldots, v_{r+1}$, y denotemos por $L_1 \subset \mathbb{Q}^r$ el $\mathbb{Q}$–espacio vectorial generado por las columnas de A. Suponemos que $Cx = 0$ son unas ecuaciones implícitas de L_1, y definimos
$$S_1 = \{s \in \mathbb{N}^r | Cs = 0\}.$$
Nótese que el sistema que nos define al semigrupo S_1 es homogéneo. Sea $\{s_1, \ldots, s_h\}$ un sistema de generadores de S_1. Denotamos por D, a la matriz $(s_1 | \cdots | s_h)$, y por
$$m = (m_1, \ldots, m_h) := (\mu_2, \ldots, \mu_{r+1})D.$$

Con estas notaciones tenemos el siguiente resultado.

Proposición II–C.4 ■ Son equivalentes:

1. $\exists w \in \mathbb{Q}^q$ con $w \cdot v_1 = 1$ y $w \cdot v_i \in \mathbb{N}$, $\forall i = 2, \ldots, r+1$.
2. $\exists y \in \mathbb{N}^h$ tal que $m_1 y_1 + \cdots + m_h y_h = 1$.

En este caso, es suficiente tomar w como una solución particular de $Ax = z$, con $z = Dy$.

Demostración. $1 \Rightarrow 2$. Sea $z = Aw$. Es claro que $z \in S_1$, y entonces existe $y \in \mathbb{N}^h$ tal que $z = Dy$. De la combinación lineal $v_1 = \sum_{i=2}^{r+1} \mu_i v_i$ y la igualdad $w \cdot v_1 = 1$, tenemos que $(\mu_2, \ldots, \mu_{r+1}) \cdot z = 1$. Entonces

$$m_1 y_1 + \cdots + m_h y_h = 1.$$

$2 \Rightarrow 1$. Sea $z = Dy$. Como $z \in S_1 \subset L_1$, deducimos que los rangos de A y de $(A|z)$ son iguales, luego el sistema es compatible. Sea w una solución. Para finalizar la demostración, basta señalar que la combinación lineal $v_1 = \sum_{i=2}^{r+1} \mu_i v_i$ implica que

$$w \cdot v_1 = (\mu_2, \ldots, \mu_{r+1})Aw = (\mu_2, \ldots, \mu_{r+1})Dy = 1.$$

■

Como corolario de la proposición anterior, tenemos que un sistema diofántico admite una $\mathbb{N}$–solución si y sólo si la admite una ecuación construida a partir de él: $m_1 y_1 + \cdots + m_h y_h = 1$. Al ser la proposición anterior constructiva y teniendo distintos métodos efectivos para resolver en $\mathbb{N}$ una ecuación diofántica, vamos a tener, a partir del siguiente algoritmo, un nuevo algoritmo para calcular una $\mathbb{N}$–solución a un sistema diofántico.

Algoritmo II–C.5 ■ Algoritmo de Farkas generalizado ([PCVT98]).
Entrada: Un conjunto de vectores $v_1, \ldots, v_{r+1} \in \mathbb{Q}^q$, con $r \geq 1$.
Salida: Un vector, caso de existir, $w \in \mathbb{Q}^q$ tal que $w \cdot v_1 = 1$ y $w \cdot v_i \in \mathbb{N}$, $\forall i = 2, \ldots, r+1$.

1. Consideramos W el $\mathbb{Q}$–espacio vectorial generado por $v_2, \ldots, v_{r+1}$.
2. Si $v_1 \notin W$, tomamos $\hat{v}_1$ la proyección ortogonal de v_1 en $W^\perp$. Devolvemos $w = \frac{\hat{v}_1}{v_1 \cdot \hat{v}_1}$ y paramos.
3. En otro caso, aplicamos el algoritmo II–C.2:
   - Si $v_1 = \sum_{i=2}^{r+1} \mu_i v_i$ con $\mu_i \leq 0$, entonces no hay solución y paramos.
   - En otro caso continuamos.
4. Tomamos una combinación $v_1 = \sum_{i=2}^{r+1} \mu_i v_i$.
5. Sea A la matriz cuyas filas corresponden a los vectores $v_2, \ldots, v_{r+1}$. Consideramos $Cx = 0$ unas ecuaciones implícitas del $\mathbb{Q}$–espa-

cio vectorial generado por las columnas de A, $L_1 \subset \mathbb{Q}^r$. Computamos $\{s_1, \ldots, s_h\}$ un sistema de generadores de

$$S_1 = \{s \in \mathbb{N}^r | Cs = 0\}$$

usando el algoritmo II–B.7. En este algoritmo usaremos II–C.6 para calcular una $\mathbb{N}$–solución particular.

6. Sea $(m_1, \ldots, m_h) = (\mu_2, \ldots, \mu_{r+1})D$, con $D = (s_1 | \cdots | s_h)$.
   - Si existe $y \in \mathbb{N}^h$ tal que $m_1 y_1 + \cdots + m_h y_h = 1$, devolvemos w una solución particular de $Ax = z$ con $z = Dy$, y paramos.
   - En otro caso no hay solución, luego paramos.

De este algoritmo podemos obtener otro que nos da una $\mathbb{N}$–solución particular de un sistema diofántico no homogéneo.

Algoritmo II–C.6 ■ $\mathbb{N}$–solución particular usando el lema de Farkas para sistemas no homogéneos.
Entrada: Un sistema $Gx = b$ como (II–B.1).
Salida: Una $\mathbb{N}$–solución particular si existe.

1. Si $b = 0$, usamos al algoritmo II–C.3.
2. Si $r = 1$, tenemos una única incógnita, luego detectar una $\mathbb{N}$–solución es trivial.
3. Si $r \geq 2$, sea $M = (-b|G)$. Sea $c_1, \ldots, c_q$ una base del $\mathbb{Q}$–espacio vectorial dado por las soluciones de $Mx = 0$.
4. Sean $v_1, \ldots, v_{r+1} \in \mathbb{Q}^q$ los vectores correspondientes a las columnas de la matriz cuyas filas son los $c_1, \ldots, c_q$. A estos vectores les aplicamos el algoritmo II–C.5.
   - Si existe $w \in \mathbb{Q}^q$ tal que $w \cdot v_1 = 1$ y $w \cdot v_i \in \mathbb{N}$, entonces la salida es u donde

$$(1, u) = w_1 c_1 + \cdots + w_q c_q = (w \cdot v_1, \ldots, w \cdot v_{r+1})$$

y paramos.

- En otro caso, no hay solución, luego paramos.

Es de destacar que los algoritmos enlazados anteriores no son cíclicos ya que tanto en II–C.5 como en II–B.7 se va reduciendo el número de variables hasta llegar a una sola. En ese caso es trivial dar una $\mathbb{N}$–solución.

■ Método usando Bases de Gröbner

Tanto en [POT91] como en [CT91], los autores usan las bases de Gröbner y la Teoría de Eliminación para resolver el problema del cálculo de $\mathbb{N}$–soluciones de un sistema diofántico.

Dado un sistema diofántico como (II–B.1), consideramos el anillo de polinomios $k[Z_1, \ldots, Z_r, Y_1, \ldots, Y_m, T]$ y el ideal definido por

$$I = < Y_1 \cdots Y_m T - 1, Y^{G(e_1)^+} - Y^{G(e_1)^-} Z_1, Y^{G(e_2)^+} - Y^{G(e_2)^-} Z_2, \ldots, Y^{G(e_r)^+} - Y^{G(e_r)^-} Z_r > .$$

Teorema II–C.7 ■ Con las notaciones anteriores:

1. $Gx = 0$ tiene una $\mathbb{N}$–solución si y sólo si existe en I un binomio de la forma $Z^\gamma - 1$. En tal caso, γ es una $\mathbb{N}$–solución.
2. $Gx = b$ tiene una $\mathbb{N}$–solución si y sólo si $Y^c T^d = Z^\gamma$ mód I, con $d \in \mathbb{N}$ tal que $c = b - d(-1, -1, \ldots, -1) \in \mathbb{N}^r$. En tal caso, γ es una $\mathbb{N}$–solución.

Demostración. Ver [POT91] y [CT91]. ■

Del anterior teorema se obtiene un algoritmo para saber si un sistema diofántico, tanto homogéneo como no homogéneo, posee una $\mathbb{N}$–solución.

Este algoritmo pasa, en el caso no homogéneo, por calcular una base de Gröbner de I respecto a un orden de eliminación de T e Y y reducir $Y^c T^d$ respecto de ella ([CT91]). Si el resultado de esta reducción es Z^γ, tenemos una ℕ–solución. En otro caso, el sistema no tiene ℕ–soluciones.

En el caso homogéneo, hay que comprobar si tenemos algún binomio de la forma $Z^\gamma - 1$ en una base de Gröbner reducida de I respecto del orden por el cual comparamos primero lexicográficamente las Z_i, y en caso de igualdad miramos el grado, y finalmente el orden lexicográfico ([POT91]). Si en esa base de Gröbner hay un binomio de la forma $Z^\gamma - 1$, tenemos una ℕ–solución. En otro caso, el sistema no tiene ℕ–soluciones.

Si la matriz del sistema estuviese formada por elementos enteros no negativos ($G(e_i) \gg 0$), podría eliminarse la variable T y el ideal I que tomaríamos sería

$$I = < Y^{G(e_1)} - Z_1, Y^{G(e_2)} - Z_2, \ldots, Y^{G(e_r)} - Z_r > .$$

Con este supuesto trabajaríamos con $r + m$ variables. Aunque como hemos visto, en general trabajamos con $r + m + 1$ variables.

En II–D.5 veremos una optimización y generalización de este cálculo usando ideales de semigrupos.

II–D. SISTEMAS DIOFÁNTICOS EN CONGRUENCIAS

Un tema apenas tratado en la literatura y que es la base de algunas partes de esta memoria, es el estudio y cálculo de las ℕ–soluciones de sistemas diofánticos en congruencias. Es decir, sistemas del tipo

$$(Sist) \equiv \left\{ \begin{array}{ccccccc} n_{11}x_1 + n_{12}x_2 + & \cdots & +n_{1r}x_r & = & b_1 & \\ n_{21}x_1 + n_{22}x_2 + & \cdots & +n_{2r}x_r & = & b_2 & \\ \vdots & \vdots & \vdots & & & \\ n_{h1}x_1 + n_{h2}x_2 + & \cdots & +n_{hr}x_r & = & b_h & \\ n_{(h+1)1}x_1 + n_{(h+1)2}x_2 + & \cdots & +n_{(h+1)r}x_r & = & b_{h+1} & \text{mód} a_1 \\ \vdots & \vdots & \vdots & & \vdots & \\ n_{(h+s)1}x_1 + n_{(h+s)2}x_2 + & \cdots & +n_{(h+s)r}x_r & = & b_{h+s} & \text{mód} a_s \end{array} \right.$$

donde n_{ij}, a_l y b_i son números enteros, y $n_i = (n_{1i}, \dots, n_{(h+s)i})$. Es fácil extender los resultados sobre la estructura de las $\mathbb{N}$–soluciones de la anterior sección a un sistema en congruencias como podemos apreciar en la siguiente nota.

Nota II–D.1 ■ Los lemas II–A.1 y II–A.2 son ciertos si el sistema diofántico es en congruencias.

Pero, en matemáticas, una cosa son las estructuras, y otra los métodos de cálculo. El método natural y clásico para calcular las $\mathbb{N}$–soluciones de un sistema diofántico en congruencias pasa por añadir al sistema nuevas variables que *absorban las congruencias*, resolviendo

$$(Sist') \equiv \left\{ \begin{array}{ccccccc} n_{11}x_1 + n_{12}x_2 + & \cdots & +n_{1r}x_r & & & = & b_1 \\ n_{21}x_1 + n_{22}x_2 + & \cdots & +n_{2r}x_r & & & = & b_2 \\ \vdots & \vdots & \vdots & & & & \\ n_{h1}x_1 + n_{h2}x_2 + & \cdots & +n_{hr}x_r & & & = & b_h \\ n_{(h+1)1}x_1 + n_{(h+1)2}x_2 + & \cdots & +n_{(h+1)r}x_r & +t_{11}a_1 & -t_{12}a_1 & = & b_{h+1} \\ \vdots & \vdots & \vdots & & \vdots & & \\ n_{(h+s)1}x_1 + n_{(h+s)2}x_2 + & \cdots & +n_{(h+s)r}x_r & +t_{s1}a_s & -t_{s2}a_s & = & b_{h+s} \end{array} \right.$$

Si consideramos la matriz

$$T := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ a_1 & -a_1 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & a_2 & -a_2 & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & & a_s & -a_s \end{pmatrix} \in \mathcal{M}(\mathbb{Z})_{(h+s)\times 2s},$$

y denotamos por

$$L := \{x \in \mathbb{N}^r \mid Gx = b \mod a\},$$

y

$$L' := \{x' \in \mathbb{N}^{r+2s} \mid (G|T)x' = b\},$$

se satisface la siguiente propiedad.

Propiedad II–D.2 ■

$$L = \pi(L'), \text{ y } \mathcal{H}L \subset \pi(\mathcal{H}L'),$$

donde $\pi : \mathbb{N}^{r+2s} \longrightarrow \mathbb{N}^r$ es la proyección sobre las primeras r coordenadas.

Introducir nuevas variables sobre un objeto matemático al que se va a aplicar un algoritmo de alta complejidad, no olvidemos que el calculo de $\mathbb{N}$–soluciones es $\mathcal{NP}$–completo, no es una política *computacionalmente correcta.* Y es algo que debemos evitar si realizamos algún cálculo de manera efectiva y pretendemos que sea *eficiente.*

Si lo que queremos es encontrar, caso de que exista, una $\mathbb{N}$–solución, podemos aplicar un método similar a los explicados en II–C junto a la propiedad II–D.2. En este caso, introducimos nuevas variables, ya que el ideal asociado al semigrupo generado por el sistema $(Sist)'$ es calculado en un anillo de polinomios con $r + m + 1 + 2s$ variables.

Para calcular la $\mathbb{N}$–solución general de un sistema en congruencias se ha usado clásicamente un método basado en II–D.2 y que aparece en [RGS98]. Además en [RGS98], se da una cota de las $\mathbb{N}$–soluciones de estos sistemas, por lo que podría aplicarse también la búsqueda exhaustiva. De todas formas, seguimos teniendo el problema computacional de añadir variables.

Los métodos que enunciamos a continuación pueden evitar ese problema manteniendo en r o, a lo más, $r + 1$ (caso de sistemas no homogéneos) el número de variables con las que realizaremos los cálculos de complejidad alta.

■ $\mathbb{N}$–solución particular mediante ideales de semigrupos

Este algoritmo es de naturaleza similar a los algoritmos explicados en II–C. La principal diferencia en cuanto a la velocidad de cómputo viene dada por el cálculo del ideal del semigrupo asociado al sistema

(*Sist*) que se realizará usando el algoritmo I–D.2 (ver [VT99]). Necesitamos además los siguientes resultados.

Teorema II–D.3 ■ El sistema (*Sist*) admite una $\mathbb{N}$–solución si y sólo si existe un binomio de la forma $X_{r+1} - \mathbf{X}^{\beta}$ en el ideal asociado al semigrupo

$$S =< n_1, \ldots, n_r, b > \subset \mathbb{Z}^h \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z},$$

con $r + 1 \notin supp(\mathbf{X})$. En tal caso, β es una $\mathbb{N}$–solución de (*Sist*).

Demostración. Ver [VT99]. ■

Para ver si un binomio como el del teorema anterior pertenece o no al ideal asociado a S usaremos el siguiente lema.

Lema II–D.4 ■ Fijemos en $k[X_1, \ldots, X_{r+1}]$ un orden monomial verificando $X_{r+1} > \cdots$, y sea $\mathbf{X}$ tal que $r+1 \notin supp(\mathbf{X})$. Sea I el ideal asociado al semigrupo S del teorema anterior y sea B la base de Gröbner reducida de I. Entonces:

$$\exists X_{r+1} - \mathbf{X}^{\beta} \in I \Leftrightarrow \exists \pm (X_{r+1} - \mathbf{X}^{\beta'}) \in B.$$

Además, si S es un semigrupo Nakayama y B un conjunto de generadores binomiales de I con coeficientes ± 1 (no necesariamente base de Gröbner), también es cierto el resultado.

Demostración. Ver [VT99]. ■

Ya estamos en condiciones de explicitar nuestro algoritmo.

Algoritmo II–D.5 ■ Cálculo de $\mathbb{N}$–solución particular para sistemas en congruencias.
Entrada: Un conjunto de ecuaciones como (*Sist*) con $n_i \neq 0$.
Salida: Sabremos si el sistema admite, o no, una $\mathbb{N}$–solución en $\mathbb{N}^r$. En caso afirmativo, tendremos una $\mathbb{N}$–solución.

1. Si $b = 0$:

   a) Sea el semigrupo $S =< n_1, \ldots, n_r >$.

b) Calculamos $I_S \subset k[X_1, \ldots, X_r]$, ideal de S, usando el algoritmo I–D.2. Sea C, un sistema de generadores binomiales con coeficientes ± 1 de I_S.

c) Si S no es Nakayama, i.e. $\exists \pm (X^\alpha - 1) \in C$, (*Sist*) admite una $\mathbb{N}$–solución y α es una tal $\mathbb{N}$–solución. En otro caso, (*Sist*) no tiene $\mathbb{N}$–solución.

2. Si $b \neq 0$:

   a) Sea el semigrupo $S =< n_1, \ldots, n_r, b >$.

   b) Calculamos $I_S \subset k[X_1, \ldots, X_r, X_{r+1}]$, ideal de S, usando el algoritmo I–D.2.

   c) Si S es Nakayama, sea C un conjunto de generadores de I_S. En otro caso, fijamos un orden monomial dando prioridad a la última variable X_{r+1}, y calculamos una base de Gröbner de I_S, C.

   d) Si existe un binomio $\pm(X_{r+1} - \mathbf{X}^\beta)$ en C, entonces (*Sist*) admite una $\mathbb{N}$–solución y β es una tal $\mathbb{N}$–solución. En otro caso, (*Sist*) no admite $\mathbb{N}$–solución.

Como puede apreciarse, el anterior algoritmo añade s variables para resolver sistemas de ecuaciones sobre $\mathbb{Z}$, mientras que los cálculos de alta complejidad (bases de Gröbner) se realizan en los anillos de polinomios en r ó $r + 1$ variables según sea el caso. Este algoritmo generaliza a los de la sección II–C, ya que los extiende a sistemas en congruencias, y también los optimiza al no usar Teoría de Eliminación para calcular los ideales de los semigrupos.

■ $\mathbb{N}$–solución general mediante el Lema de Dickson

En esta sección vamos a generalizar a sistemas en congruencias el método dado en II–B.7. En el siguiente algoritmo, nosotros proponemos el cálculo de las $\mathbb{N}$–soluciones particulares mediante el algoritmo II–D.5 para no aumentar el número de incógnitas en la computación.

Algoritmo II–D.6 ■ $\mathbb{N}$–soluciones minimales de un sistema diofántico en congruencias.
Entrada: La matriz de coeficientes, el término independiente y la congruencia del sistema $Gx = b$ mód a. Sea r el número de columnas de G.
Salida: $\mathcal{H}\mathcal{G}'$, con $\mathcal{G}' = \{\alpha \in \mathbb{N}^r | G\alpha = b \text{ mód } a\}$.

1. Si $r = 1$, tenemos sólo una incógnita y la solución es trivial.
2. Si $r \geq 2$, determinamos si $\mathcal{G}'$ es vacío o no usando el algoritmo II–D.5.
3. Si $\mathcal{G}'$ es vacío, devolvemos $\mathcal{H}\mathcal{G}' = \emptyset$ y terminamos.
4. En otro caso, sea $s = (s_1, \ldots, s_r) \in \mathcal{G}'$.
5. Mediante el algoritmo II–B.7 calculamos el conjunto $\mathcal{H}\mathcal{F}$, con
$$F = \{s\} \cup \bigcup_{i=1}^{r} \bigcup_{\alpha=0}^{s_i-1} \mathcal{H}\mathcal{G}'(i, \alpha).$$
En el algoritmo II–B.7 usaremos II–D.5 al calcular las distintas $\mathbb{N}$–soluciones particulares para no aumentar el número de variables.
6. Devolvemos $\mathcal{H}\mathcal{G}' = \mathcal{H}\mathcal{F}$.

Al igual que en el caso sin congruencias, podemos aplicar este algoritmo para calcular la $\mathbb{N}$–solución general a un sistema diofántico no homogéneo en congruencias usando II–B.8.

II–E. NOTAS

Los métodos más tradicionales y que aparecen en los libros de *cabecera* de los estudiosos de la Programación Lineal Entera (por ejemplo [SCH96]) son los basados en la búsqueda exhaustiva. Estos métodos han sido ampliamente superados, en cuanto a velocidad de cómputo, tanto por los basados en la teoría de bases de Gröbner (ver [PCVT98]), como por los basados en la *búsqueda dirigida* de Clausen-Fortenbacher y que llamaremos de *segunda generación*.

Tanto el algoritmo II–D.5 como II–D.6 no han sido comparados computacionalmente con los de *segunda generación*. La tabla II.1 muestra, sobre varios ejemplos, una comparación entre el algoritmo II–B.7 usando II–D.5 y II–C.6 para calcular $\mathbb{N}$–soluciones particulares. De la tabla se *deduce* que el algoritmo II–B.7 tiene un mejor comportamiento computacional si en él usamos bases de Gröbner II–D.5 en vez de los métodos clásicos de programación lineal II–C.6.

Si consideramos sistemas en congruencias, la primera referencia de un algoritmo para calcular una $\mathbb{N}$–solución particular aparece en [VT99]. Es de prever que los algoritmos II–D.5 y II–D.6 tengan mucho que decir, en cuanto a la computación, frente a los de *segunda generación* por no aumentar el número de incógnitas al realizar el cálculo de las $\mathbb{N}$–soluciones. Además, el cálculo de ideales de semigrupos (base de II–D.5) está siendo mejorado día a día, por lo que el avance en el cálculo de $\mathbb{N}$–soluciones por esta vía puede ser amplio. En cualquier caso, es un mundo computacional a explorar.

Entre los algoritmos de *segunda generación*, aunque de naturaleza distinta, cabe destacar también el dado por Domenjoud (ver [DOM91]), el cual es susceptible de ser paralelizado.

Una clara aplicación de los métodos expuestos en este capítulo es el cálculo de identidades de particiones [STU95, capítulo 6].

Los algoritmos II–D.5 y II–D.6 los hemos implementado en MapleV3 y pueden ser obtenidos vía ftp en

`ftp.uca.es/pub/matematicas/nsol.zip`

Cuadro II.1. Algoritmos II–B.7 + II–C.6 versus II–B.7 + II–D.5

Sistemas Homogéneos	Usando bases de Gröbner	Usando lema de Farkas
$\begin{pmatrix} 1 & -3 & 2 & -5 \end{pmatrix}$	2 sec., $s = [1, 1, 1, 0]$	5 sec., $s = [5, 0, 0, 1]$
$\begin{pmatrix} 1 & -2 & 1 & 2 \\ -2 & -1 & -1 & 2 \end{pmatrix}$	4 sec., $s = [0, 4, 2, 3]$	16 sec., $s = [2, 6, 0, 5]$
$\begin{pmatrix} 1 & 2 & 3 & -5 \\ -2 & -1 & 4 & 5 \end{pmatrix}$	5 sec., $s = [7, 0, 1, 2]$	7 sec., $s = [5, 5, 0, 3]$
$\begin{pmatrix} 3 & -1 & -2 & -3 \\ 3 & -7 & 2 & -1 \end{pmatrix}$	7 sec., $s = [2, 1, 1, 1]$	111 sec., $s = [8, 6, 9, 0]$
$\begin{pmatrix} -4 & 1 & 0 & -1 & 0 & -2 \\ 0 & -1 & 0 & 2 & -3 & 1 \end{pmatrix}$	5 sec., $s = [0, 0, 1, 0, 0, 0]$	1961 sec., $s = [1, 8, 0, 4, 0, 0]$
$\begin{pmatrix} -1 & 2 & -3 & 0 & -1 \\ 0 & 1 & 0 & -3 & 0 \\ -1 & -2 & 0 & 0 & 1 \end{pmatrix}$	4 sec., $s = [0, 3, 0, 1, 6]$	9 sec., $s = [0, 3, 0, 1, 6]$
$\begin{pmatrix} -2 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & -3 & 1 \\ 1 & -3 & 0 & 1 & -1 & 0 \\ 2 & 0 & 0 & -2 & 1 & 0 \end{pmatrix}$	17 sec., $s = [1, 0, 2, 3, 4, 8]$	500 sec., $s = [1, 0, 2, 3, 4, 8]$
$\begin{pmatrix} 0 & -1 & 2 & -3 & 0 & 0 \\ 1 & 0 & 1 & 0 & -3 & 0 \\ -1 & 4 & -2 & 0 & 0 & -1 \end{pmatrix}$	102 sec., $s = [2, 2, 1, 0, 1, 4]$	Parado a los 40.000 sec., $s = [18, 6, 3, 0, 7, 0]$
$\begin{pmatrix} 1 & 2 & -3 & -2 & -4 \\ 2 & -1 & -3 & 2 & 5 \end{pmatrix}$	49 sec., $s = [1, 3, 1, 2, 0]$	Parado a los 40.000 sec., $s = [9, 3, 5, 0, 0]$

CAPÍTULO III

Módulos de Sicigias

En este capítulo vamos a estudiar la resolución libre minimal del álgebra de un semigrupo Nakayama con torsión. En particular, comenzaremos definiendo tal resolución y dando el método aparecido en [BCMP98a] para calcular dicha resolución. Este método utiliza la homología reducida de ciertos complejos simpliciales asociados a los elementos del semigrupo.

Empezaremos por explicar los pasos principales del algoritmo aparecido en [BCMP98b] para calcular el 0-módulo de sicigias (ideal del semigrupo). La naturaleza de este algoritmo es completamente distinta a los explicados en el capítulo I, y está basado en combinatoria y en los métodos de programación lineal entera del capítulo II. Es precisamente esta filosofía la que seguiremos en capítulos sucesivos para dar un algoritmo que calcula sistemas minimales de generadores de los módulos de sicigias de orden superior, y por tanto la resolución libre minimal de $k[S]$.

III–A. MÓDULOS DE SICIGIAS

De nuevo vamos a considerar un semigrupo, S, cancelativo, abeliano, finitamente generado y con elemento neutro. En estas condiciones, es conocido, y ya lo hemos empleado con anterioridad, que nuestro semigrupo es isomorfo a un subsemigrupo de un grupo abeliano finitamente generado, $G(S)$ (ver [BCMP98b]). Por ello, podemos suponer sin pérdida de generalidad que,

$$S \subset \mathbb{Z}^h \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z}$$

con $a = (a_1, \ldots, a_s) \in \mathbb{Z}^s$. Sea $\{n_1, \ldots, n_r\}$ un conjunto de generadores de S. Vamos a suponer en lo sucesivo que nuestro semigrupo es Nakayama, es decir, verifica la condición $S \cap (-S) = \{0\}$.

Considerando k un cuerpo, denotamos por R al anillo de polinomios $k[X_1, \ldots, X_r]$, y por $k[S]$ a la k–álgebra asociada a S. Sea $\mathbf{m} = (X_1, \ldots, X_r)$ el ideal maximal irrelevante de R.

La k–álgebra, $k[S]$, es un anillo S–graduado

$$k[S] = \oplus_{m \in S} k[S]_m,$$

donde las componentes homogéneas son $k[S]_m = km$. R es también un anillo S–graduado, dando a cada variables X_i el grado n_i. Por lo tanto podemos escribir

$$R = \oplus_{m \in S} R_m,$$

donde R_m es el k–espacio vectorial generado por los monomios de grado m. Es conocido que estos espacios vectoriales son de generación finita (ver [BCMP98b, nota 1.3]).

La S–graduación anterior nos permite enunciar el lema de Nakayama para módulos S–graduados.

Proposición III–A.1 ■ Sea S un semigrupo cancelativo, abeliano, finitamente generado, con elemento neutro y Nakayama. Si Q es un R–módulo S–graduado tal que $\mathbf{m}Q = Q$, entonces se tiene que $Q = 0$.

Demostración. Ver [BCMP98b, proposición 1.4]. ■

El homomorfismo de k–álgebras (I–A.1) dado por

$$\varphi_0 : R \longrightarrow k[S]$$
$$\varphi(X_i) = n_i,$$

es un homomorfismo graduado de grado cero, y su núcleo es, como ya vimos, un ideal homogéneo, I. Este ideal depende directamente del sistema de generadores de S tomado, pero, consideremos el sistema que consideremos, se tiene que

$$k[S] \cong R/I.$$

Luego conocer el ideal *es* conocer el álgebra del semigrupo.

Denotemos por V_0 al cociente $I/\mathbf{m}I$, y por $V_0(m)$ a los cocientes $I_m/(\mathbf{m}I)_m$, con $m \in S$. Por III–A.1, tenemos que un conjunto finito de elementos de I lo genera si y sólo si las clases de sus elementos en V_0 generan este espacio vectorial. Además, un sistema minimal de generadores de I tiene tantos elementos de grado m como $\dim_k V_0(m)$. Los espacios vectoriales $V_0(m)$ son nulos salvo una cantidad finita por ser R un anillo noetheriano.

Llegados a este punto, si uno escoge un sistema minimal y homogéneo de generadores de I, $\{f_1, \ldots, f_{b_1}\}$, puede construir un nuevo homomorfismo de k–álgebras

$$\varphi_1 : R^{b_1} \longrightarrow R$$
$$\varphi_1(e_j) = f_j$$

con $j = 1, \ldots, b_1$, $b_1 := \sum_{m \in S} \dim_k V_0(m)$ y e_j el j–ésimo generador estándar de R^{b_1}.

De la misma manera podemos construir recurrentemente los morfismos

$$\varphi_{i+1} : R^{b_{i+1}} \longrightarrow R^{b_i}, \tag{III–A.1}$$

que corresponden a tomar un conjunto minimal y homogéneo de generadores en $N_i = \ker(\varphi_i) \subset R^{b_i}$, con $N_0 = I$ y $b_0 = 1$, y hacer que la imagen de cada uno de los generadores estándar de $R^{b_{i+1}}$ sea un generador de

N_i. Si para cada j entre uno y b_i, el grado del j–ésimo generador de N_i es $m_j \in S$, $R^{b_{i+1}}$ tiene como elementos homogéneos las b_{i+1}–uplas cuya j–ésima componente es un elemento homogéneo en R de grado $m - m_j$.

Con este proceso construimos una resolución libre minimal y S–graduada para el R–módulo $k[S]$ dada por

$$\cdots \to R^{b_{i+1}} \xrightarrow{\varphi_{i+1}} R^{b_i} \xrightarrow{\varphi_i} \cdots \to R^{b_2} \xrightarrow{\varphi_2} R^{b_1} \xrightarrow{\varphi_1} R \xrightarrow{\varphi_0} K[S] \to 0,$$

con $b_{i+1} = \sum_{m\in S} \dim_k V_i(m)$, y

$$V_i(m) = \frac{(N_i)_m}{(\mathbf{m}N_i)_m}.$$

El entero b_{i+1} es finito por ser R noetheriano. El número de elementos de grado m en un sistema minimal de generadores del i–ésimo módulo de sicigias N_i es $\dim_k V_i(m)$.

El teorema de Auslander-Buchbaum (ver [VAS98]) nos garantiza que b_i es nulo a partir de un índice i suficientemente grande. Concretamente se tiene el siguiente resultado.

Proposición III–A.2 ■ Con las notaciones anteriores, la resolución libre minimal S–graduada para el álgebra $k[S]$ tiene la forma

$$0 \to R^{b_p} \to \cdots \to R^{b_1} \to R \to K[S] \to 0$$

con $r - rg(G(S)) \leq p \leq r$.

Visto esto, para obtener el i–ésimo paso de la resolución libre minimal de $k[S]$, podemos calcular, en primer lugar, los distintos $m \in S$ tales que los espacios $V_i(m)$ son no nulos, y después una base de cada espacio vectorial. Los espacios $V_i(m)$ los vamos a determinar mediante espacios isomorfos a ellos. Veamos ahora cuáles serán esos espacios.

■ $\tilde{H}_i(\Delta_m) \cong V_i(m)$

Para comenzar, sea Λ el conjunto formado por los subíndices de los generadores de S, i.e. $\Lambda := \{1, 2, \ldots, r\}$. Dado $F \subset \Lambda$, vamos a denotar por n_F al elemento $\sum_{i\in F} n_i$, y por $n_\emptyset$ al cero. Con esta notación, para cada $m \in S$, podemos definir el siguiente complejo simplicial.

Definición III–A.3 ■ Sea $m \in S$, llamaremos complejo asociado a m al complejo simplicial abstracto

$$\Delta_m := \{F \subset \Lambda | m - n_F \in S\}.$$

Fijado un elemento m en S, y escogida una orientación en cada cara de Δ_m, podemos considerar la homología reducida, $\tilde{H}_\bullet(\Delta_m)$, del complejo Δ_m con valores sobre el cuerpo k. Construyámosla.

Sea $\tilde{C}_i(\Delta_m)$ el k–espacio vectorial generado por las caras de dimensión i de Δ_m, donde $\dim F := \sharp F - 1$ ($\dim \emptyset := -1$). Sea también ∂_i la aplicación k–lineal

$$\partial_i : \tilde{C}_i(\Delta_m) \to \tilde{C}_{i-1}(\Delta_m)$$
$$\partial_i(F) = \sum_{F' \in \Delta_m, \dim F' = i-1} \epsilon_{FF'} F'$$

donde $\epsilon_{FF'} = 0$ si $F' \not\subset F$, y $\epsilon_{FF'} = \pm 1$ si $F' \subset F$ ($\epsilon_{FF'}$ será uno si la orientación inducida de F en F' es igual a la escogida en F', en otro caso $\epsilon_{FF'} = -1$). Fijemos nuestra atención sobre las aplicaciones

$$\tilde{C}_{i+1}(\Delta_m) \xrightarrow{\partial_{i+1}} \tilde{C}_i(\Delta_m) \xrightarrow{\partial_i} \tilde{C}_{i-1}(\Delta_m)$$

con $i \geq 0$. Denotaremos por $\tilde{Z}_i(\Delta_m)$ a $\ker(\partial_i)$, y por $\tilde{B}_i(\Delta_m)$ a $Im(\partial_{i+1})$. A los elementos de $\tilde{Z}_i(\Delta_m)$ se les denomina ciclos y a los de $\tilde{B}_i(\Delta_m)$ bordes. Entonces tenemos que

$$\tilde{H}_i(\Delta_m) := \tilde{Z}_i(\Delta_m)/\tilde{B}_i(\Delta_m).$$

Ahora estamos en condiciones de enunciar el resultado que nos va a permitir calcular $V_i(m)$.

Teorema III–A.4 ■ Sea S un semigrupo abeliano, finitamente generado, cancelativo, con elemento neutro y Nakayama. Fijado un conjunto de generadores no nulos de S, $\{n_1, \ldots, n_r\}$, un cuerpo conmutativo k, y considerando la resolución libre minimal S–graduada de $k[S]$ y los complejos Δ_m, se tiene

$$\tilde{H}_i(\Delta_m) \cong V_i(m) \text{ (como } k\text{–espacios vectoriales),}$$

para todo $m \in S$, y $i \geq 0$.

Demostración. Ver [BCMP98a, teorema 2.1]. ■

Además, en [BCMP98a, teorema 3.3], los autores dan de manera explícita el isomorfismo del teorema anterior. El resto de esta memoria consiste fundamentalmente en probar que se tiene un algoritmo, basado en métodos combinatorios, para computar sistemas minimales de los módulos de sicigias de $k[S]$. Concretamente,

---

Algoritmo III–A.5 ■ Con las notaciones anteriores
Entrada: Un conjunto de generadores $\{n_1, \ldots, n_r\}$ de S.
Salida: Un sistema minimal de generadores del i–ésimo módulo de sicigias de $k[S]$.

1. Calcular el conjunto $C_i := \{m \in S \mid \tilde{H}_i(\Delta_m) \neq 0\}$.
2. Calcular, $D(m)$, una base del espacio vectorial $\tilde{H}_i(\Delta_m)$, con $m \in C_i$.
3. Calcular M el conjunto imagen de $\bigcup_{m \in C_i} D(m)$, para distintos i, mediante el isomorfismo III–A.4.
   M es un conjunto minimal de generadores del i–ésimo módulo de sicigias de $k[S]$.

El algoritmo anterior será realmente un algoritmo si todos los pasos se pueden realizar de manera efectiva. En particular, tienen que ser efectivos los métodos que utilicemos para resolver dos problemas: calcular C_i y calcular una base de $\tilde{H}_i(\Delta_m)$. El segundo problema se puede resolver de manera algorítmica mediante álgebra lineal realizando los siguientes pasos:

- Se determina Δ_m usando los métodos de programación lineal entera explicados en el capítulo II.
- Se determina ahora

$$\tilde{H}_i(\Delta_m) := \tilde{Z}_i(\Delta_m)/\tilde{B}_i(\Delta_m)$$

  usando álgebra lineal ordinaria en espacios vectoriales sobre un cuerpo k. De hecho, una vez conocidas las caras de Δ_m y fijada una orientación, las aplicaciones ∂_i se pueden explicitar fácilmente mediante matrices. Un ejemplo de esto lo veremos en el capítulo VI.

En la siguiente sección, vamos a dar un método efectivo para calcular C_0, resolviendo el cálculo de C_i, para cualquier i, en capítulos posteriores.

III–B. 0-MÓDULO DE SICIGIAS

Veamos ahora un algoritmo combinatorio que nos permite, no sólo calcular, sino caracterizar, el conjunto de los grados que aparecen en un conjunto minimal de generadores del ideal de un semigrupo, C_0. Por tratarse de homología reducida, son equivalentes: que $\tilde{H}_0(\Delta_m) \neq 0$ y que el complejo Δ_m es no conexo (ver [BCMP98b]).

Nótese que si $M = X_1^{\alpha_1} \cdots X_r^{\alpha_r}$ es un monomio en R de grado $m \in S$, tenemos que $supp(M) \in \Delta_m$. Además, si $A \in \Delta_m$ es una cara maximal de Δ_m, se tiene que existe un monomio de grado m cuyo soporte es A.

Denotemos por $\mathcal{B}$ al conjunto

$$\mathcal{B} = \{X^\alpha - X^\beta | \sum_{i=1}^r \alpha_i n_i = \sum_{i=1}^r \beta_i n_i,\ \alpha_i, \beta_i \geq 0\}.$$

Sea Δ_m no conexo, y $\mathcal{G}_m \subset \mathcal{B}$ un subconjunto de binomios de grado m. Consideremos el siguiente grafo con vértices las componentes conexas de Δ_m (supondremos que hay s): si $b = M - M' \in \mathcal{G}_m$, tomamos una arista cuyos extremos sean las componentes conexas que contengan a $supp(M)$ y $supp(M')$. Diremos que $\mathcal{G}_m$ es un *árbol generador* para Δ_m si es un grafo conexo con s vértices y $s-1$ aristas, es decir, un árbol en el sentido usual. La relación entre estos árboles y el ideal de S la explicitamos en el siguiente resultado.

Teorema III–B.1 ■ Sea $\mathcal{G} \subset \mathcal{B}$. Son equivalentes:

1. $\mathcal{G} = \bigcup_{m \in S} \mathcal{G}_m$, donde $\mathcal{G}_m$ es un árbol generador para Δ_m si éste es no conexo, y $\mathcal{G}_m = \emptyset$ en otro caso.
2. $\mathcal{G}$ es un conjunto minimal de generadores de I.

Demostración. Ver [BCMP98b, teorema 2.5]. ■

A partir del anterior teorema se obtiene un método para calcular un sistema minimal de generadores de I :

1. Determinar $m \in S$ tales que Δ_m es no conexo (C_0).
2. Si Δ_m es no conexo (i.e. $m \in C_0$), determinamos los monomios M_i de grado m con $supp(M_i) \in C_i$ donde $C_1, \ldots, C_s$ son las componentes conexas de Δ_m. Tomamos

$$\mathcal{G}_m = \{M_1 - M_2, \ldots, M_1 - M_s\}.$$

Este proceso será un algoritmo si podemos calcular de manera algorítmica los $m \in S$ tales que su Δ_m es no conexo, i.e. $\tilde{H}_0(\Delta_m) \neq 0$. Además, necesitamos calcular las componentes conexas. Pues bien, ese algoritmo existe y pasaremos ahora a describirlo.

A partir de aquí consideraremos que el conjunto Λ está ordenado. Comencemos dando alguna nueva notación.

Notación III–B.2 ■ Sea $A = \{i_1, \ldots, i_p\} \subset B \subset \Lambda$ con $A \neq \emptyset$ y $B \neq \Lambda$. Denotaremos:

- $E(A, B)$ al conjunto de los $\gamma = (\gamma_1, \ldots, \gamma_p) \in \mathbb{N}^p$ tal que
    1. $\gamma_{i_j} \neq 0$, para $1 \leq j \leq p$.

2. Es posible escribir

$$\sum_{j=1}^{p} \gamma_{i_j} n_{i_j} = \sum_{t \notin A} \rho_t n_t$$

con $\rho_t \in \mathbb{N}$ y $\rho_t \neq 0$ para al menos un $t \notin B$.

- $\tilde{E}(A, B) = E(A, B) + \mathbb{N}^p$.
- $\mathcal{HE}(A, B) = \{\gamma \in E(A, B) | \gamma \text{ es } \gg -\text{minimal}\}$.

Diremos que los elementos de $\mathcal{HE}(A, B)$ son los vértices de $\tilde{E}(A, B)$.

A partir de estas notaciones podemos considerar la siguiente definición.

Definición III–B.3 ■ Sea $m \in S$, y sea $A = \{i_1, \ldots, i_p\} \subset B \subset \Lambda$ con $A \neq \emptyset$ y $B \neq \Lambda$. Diremos que A está m–aislado de $\Lambda \setminus B$ si se cumple:

1. Es posible escribir

$$m = \sum_{j=1}^{p} \gamma_{i_j} n_{i_j} = \sum_{t \notin B} \rho_t n_t$$

con $\gamma_{i_j}, \rho_t \in \mathbb{N}$, y $\gamma_{i_j} \neq 0$ para todo j.

2. $(\gamma_{i_1}, \ldots, \gamma_{i_p}) \in \mathcal{HE}(A, B)$.
3. $(\gamma_{l_1}, \ldots, \gamma_{l_s}) \notin \tilde{E}(A', B)$, para cada $A' = \{i_1, \ldots, i_s\} \subset A$, y $A' \neq A$.

Para detectar si un conjunto, A, está m–aislado de $\Lambda \setminus B$ podemos ver las siguientes condiciones:

1. Si existe un monomio de grado m con soporte contenido en $\Lambda \setminus B$.
2. Si existe $(\lambda_{i_1}, \ldots, \lambda_{i_p}) \in \mathcal{HE}(A, B)$ tal que $m = \sum_{j=1}^{p} \lambda_{i_j} n_{i_j}$.
3. $\forall A' = \{l_1, \ldots, l_s\} \subsetneq A$, y $\forall (\lambda'_{l_1}, \ldots, \lambda'_{l_s}) \in \mathcal{HE}(A', B)$,

$$(\lambda'_{l_1}, \ldots, \lambda'_{l_s}) \nleq (\lambda_{l_1}, \ldots, \lambda_{l_s}).$$

El problema es determinar $\mathcal{HE}(A', B)$, $\forall A' \subset A$. Esto se resuelve recurriendo a técnicas de programación lineal entera y con los métodos que planteamos en el capítulo II.

El siguiente lema nos clarifica la terminología usada.

Lema III–B.4 ■ Sea $m \in S$, $B \subset \Lambda$, $B \neq \Lambda$ y $A \subset B$ está m–aislado de $\Lambda \setminus B$. Entonces no existe ninguna arista en Δ_m cuyos extremos estén uno en A y el otro en $\Lambda \setminus B$.

Demostración. Ver [BCMP98b, lema 3.5]. ■

Como ya hemos visto, necesitamos ser capaces de calcular las componentes conexas del complejo. Para ello enunciamos el siguiente teorema que las caracteriza.

Teorema III–B.5 ■ Sea $C \subset \Lambda$ con $1 \leq \sharp(C) \leq r-1$, y $m \in S$. Son equivalentes:

1. C es una componente conexa de Δ_m, que es no conexo.
2. Existen unos subconjuntos $T_1, \ldots, T_g \subset \Lambda$ verificando:

   a) $C = \bigcup_{j=1}^{g} T_j$.

   b) T_j está m–aislada de $\Lambda \setminus C$, $\forall j$.

   c) $T_j \cap T_{j+1} \neq \emptyset$ para j con $1 \leq j \leq g-1$.

Demostración. Ver [BCMP98b, teorema 3.11].■

Que los conjuntos T_j anteriores pueden ser encontrados de forma algorítmica, y que por lo tanto el resultado puede ser comprobado mediante un método efectivo basado en la combinatoria, aparece en [BCMP98b].

Visto esto podemos plantear ya el, ahora sí, algoritmo para calcular el ideal de un semigrupo Nakayama.

Algoritmo III–B.6 ■ *Entrada:* Un sistema de generadores de un semigrupo S Nakayama.
Salida: Un sistema minimal de generadores del ideal del semigrupo.

1. Sea $\mathcal{M}$ el conjunto
$$\{m \in S \mid \Delta_m \text{ es no conexo}\} \ (= C_0).$$
2. Si Δ_m es no conexo, determinamos los monomios M_i de grado m con $supp(M_i) \subset C_i$ donde $C_1, \ldots, C_s$ son las componentes conexas de Δ_m. Tomamos
$$\mathcal{G}_m = \{M_1 - M_2, \ldots, M_1 - M_s\}.$$
3. $\mathcal{G} = \bigcup_{m \in \mathcal{M}} \mathcal{G}_m$, es un sistema minimal de generadores de I.

III–C. CÁLCULO PRÁCTICO DE LA RESOLUCIÓN DADOS LOS C_i

En [BCMP98a, nota 3.6], los autores dan un algoritmo recurrente para, dados los conjuntos C_i, obtener conjuntos minimales de generadores de los módulos de sicigias de $k[S]$ mediante el isomorfismo $\tilde{H}_j(\Delta_m) \cong V_j(m)$.

Para ello, sea $D_j(m)$ un conjunto de ciclos de $\tilde{Z}_j(\Delta_m)$ que forman una base de la homología $\tilde{H}_j(\Delta_m)$. Denotaremos por σ_j a la aplicación
$$\sigma_j : \tilde{Z}_j(\Delta_m) \longrightarrow (N_j)_m$$
inducida por el isomorfismo del teorema III–A.4 (ver [BCMP98a, pág. 247]).

Pasemos a continuación a enunciar dicho método recurrente:

1.- Para cada $m \in C_0$, i.e. Δ_m no conexo, $D_0(m)$ puede ser construido tomando, para cada componente ν de Δ_m, un punto P_ν en ella, y entonces $D_0(m)$ puede formarse con las diferencias $P_\nu - P_{\nu'}$, donde (ν, ν') son las aristas de un árbol sobre las componentes.

Ahora, para un ciclo $c = \sum_P \lambda_P P \in \tilde{Z}_0(\Delta_m)$, se tiene un elemento, $\sigma_0(c)$, en $(N_0)_m$ $(= I_m)$ dado por $G = \sum_P \lambda_P X_P M_P$, donde M_P es un monomio de grado $m - n_P$. En particular, a un ciclo $P - P' \in D_0(m)$ se le asocia un binomio $M_P - M_{P'}$ donde M_P y $M_{P'}$ son monomios de grado m cuyo soporte contiene a P y P' respectivamente (está claro que $P - P' \in D_0(m)$).

2.- Supongamos que tenemos un sistema minimal de generadores de N_0, $\{G_1^{(0)}, \ldots, G_{b_1}^{(0)}\}$. Consideremos $m \in C_1$, i.e. $\tilde{H}_1(\Delta_m) \neq 0$, y tomemos $D_1(m)$ un subconjunto de $\tilde{Z}_1(\Delta_m)$ base de $\tilde{H}_1(\Delta_m)$. Para cada $c = \sum_F \lambda_F F \in D_1(m)$, realizamos la siguiente construcción: para cada punto $P \in \Delta_m$ consideramos

$$b_P = \sum_F \lambda_F \epsilon_{PF} \frac{X_F}{X_P} M_F,$$

donde M_F es un monomio de grado $m - n_F$. Ahora, como $b_P \in (N_0)_{m-n_P}$, tomamos $a_P = (a_P^l) \in (R^{b_1})_{m-n_p}$ tal que $b_P = \sum a_P^l G_l^{(0)}$. Entonces, una sicigia $\sigma_1(c) \subset (N_1)_m$ viene dada por

$$b = \sum_P X_P a_P.$$

3.- Por recurrencia, supongamos que tenemos un sistema minimal de generadores de N_i, $\{G_1^{(i)}, \ldots, G_{b_{i+1}}^{(i)}\}$, para $1 \leq i \leq j-1$. De nuevo construimos un sistema de generadores de N_j partiendo de un conjunto $D_j(m)$ con $m \in C_j$, i.e. $\tilde{H}_j(\Delta_m) \neq 0$. Dado $c = \sum_F \lambda_F F \in D_j(m) \subset \tilde{Z}_j(\Delta_m)$, podemos computar la sicigia $\sigma_j(c)$ en j pasos como sigue. Primero, para cualquier $F' \subset \Delta_m$ con $\dim F' = j-1$, consideramos el polinomio

$$b_{F'} = \sum_F \lambda_F \epsilon_{F'F} \frac{X_F}{X_{F'}} M_F$$

donde M_F es un monomio de grado $m - n_F$. Ahora tomamos $a_{F'} = (a_{F'}^l) \in R^{b_1}_{m-n_{F'}}$, con $b_{F'} = \sum a_{F'}^l G_l^{(0)}$, y para cada F'' con $\dim F'' = j-2$, consideramos $b_{F''} \in (N_1)_{m-n_{F''}}$ dado por

$$b_{F''} = \sum_{F'} \epsilon_{F''F'} \frac{X_{F''}}{X_{F'}} a_{F'}.$$

De nuevo se construye $a_{F''} \in (R^{b_2})_{m-n_{F''}}$ con el método anterior y continuamos operando de la misma forma. Para la dimensión -1 obtenemos un elemento de $(N_j)_m$ dado por

$$b = \sum_P X_P a_P,$$

donde $a_P \in (R^{b_j})_{m-n_P}$ corresponde a la cara de dimensión 0. Un elemento, $\sigma_j(c)$, en la sicigia es este último, $b = \sum_P X_P a_P$.

En el capítulo dedicado a los ejemplos, realizaremos el cálculo del primer módulo de sicigias para un semigrupo determinado usando estos métodos.

CAPÍTULO IV

Cálculo del Primer Módulo de Sicigias

En este capítulo, como ya habíamos adelantado, nos centraremos en dar un conjunto finito de chequeo, C, tal que si existe un elemento en un sistema minimal de generadores del primer módulo de sicigia de $k[S]$, su grado pertenece a C. Es decir, $C_1 \subset C$.

IV–A. CONJUNTO FINITO DE CHEQUEO

Fijemos S, semigrupo Nakayama (i.e. $S \cap (-S) = \{0\}$) tal que

$$S \subset \mathbb{Z}^h \oplus \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_s$$

con $a = (a_1, \ldots, a_s) \in \mathbb{Z}^s$, y un conjunto de generadores $\{n_1, \ldots, n_r\}$ de S. Sea $\Lambda = \{1, \ldots, r\}$. Considerando los generadores $n_1, \ldots, n_r$ como elementos en $\mathbb{Z}^{h+s}$, podemos definir la $((h+s) \times r)$–matriz

$$\mathcal{A} := (n_1|n_2| \cdots |n_r) \in \mathcal{M}_{(h+s)\times r}(\mathbb{Z}).$$

Como ya expusimos en III–A.5, para dar un sistema de generadores del primer módulo de sicigias del álgebra del semigrupo, basta tener el conjunto $C_1 = \{m \in S \,|\, \tilde{H}_1(\Delta_m) \neq 0\}$. Vamos a construir un conjunto finito, C, que lo contiene. Para ello necesitamos en primer lugar dar una serie de definiciones y resultados.

Definición IV–A.1 ■ Sea $m \in S$ y $F := \{i_1, \ldots, i_t\} \subset \Lambda$ tal que $t \geq 3$, y sea σ un polígono, no necesariamente plano, cuyo conjunto de vértices es F. Diremos que σ es un F–hueco de Δ_m si se tienen las siguientes condiciones:

1. $F_j \in \Delta_m$, $\forall j = 1, \ldots, t$, siendo

$$F_j := \{i_j, i_{j+1}\}, \ \forall j = 1, \ldots, t-1, \ \text{ y } F_t := \{i_t, i_1\},$$

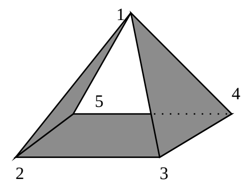
   las caras de σ.

2. Si $F' \subset F$, $\sharp F' \geq 2$, y $F_j \neq F'$ $\forall j = 1, \ldots t$, entonces $F' \notin \Delta_m$.

Aclaremos esta definición mediante el siguiente ejemplo ilustrativo.

Ejemplo IV–A.2 ■ Si consideramos el complejo simplicial Δ_m dado por el gráfico IV.1. es

Figura IV.1. F–hueco



fácil apreciar que el polígono, σ, formado por (1 2 3) es un $\{1, 2, 3\}$–hueco de Δ_m. Sin embargo, el triángulo (1 3 4), no es un $\{1, 3, 4\}$–hueco por estar el propio $\{1, 3, 4\}$ en el complejo.

Nótese que dado un conjunto, F, de vértices de cardinal t, el número de polígonos, σ, distintos sobre él es $\frac{(t-1)!}{2}$.

El primer resultado que planteamos a partir de la definición de F–hueco, nos da una condición necesaria para que el espacio vectorial $\tilde{H}_1(\Delta_m)$ sea no nulo (i.e. $m \in C_1$).

Lema IV–A.3 ■ Sea $m \in S$ tal que $\tilde{H}_1(\Delta_m) \neq 0$. Existen F y σ un F–hueco de Δ_m cuyas caras son F_j, verificando

$$c = \sum_{j=1}^{t} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m),$$

con $\epsilon_j = \pm 1$, $\forall j = 1, \ldots, t$.

Demostración. Por ser $\tilde{H}_1(\Delta_m) \neq 0$, podemos considerar el menor entero t tal que exista

$$d = \sum_{j=1}^{t} \lambda_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m),$$

con $\lambda_j \neq 0$ $\forall j = 1, \ldots, t$. En tal caso, $F_i \neq F_j$ $\forall i \neq j$.

Supongamos como punto de partida que $F_1 = \{i_1, i_2\}$. Entonces, para algún $\epsilon_1 = \pm 1$,

$$\partial_1 d = \lambda_1 \epsilon_1 (\{i_2\} - \{i_1\}) + \cdot \cdot \cdot = 0.$$

En este caso, debe existir un conjunto F_j con $j \neq 1$, y tal que i_2 pertenezca a él. Por comodidad de notación, vamos a suponer que $j = 2$, y que $F_2 = \{i_2, i_3\}$. Es claro que $i_1 \neq i_3$ porque $F_1 \neq F_2$.

Análogamente, existe un conjunto $F_3 = \{i_3, i_4\}$ ($t \geq 3$, primera condición de F–hueco) donde, trivialmente, $i_3 \neq i_4$ y $i_4 \neq i_2$. Veamos las posibilidades de surgen:

- Si $i_4 = i_1$, tenemos

  $$F_1 = \{i_1, i_2\},\ F_2 = \{i_2, i_3\},\ F_3 = \{i_3, i_1\}.$$

  Entonces podemos definir los elementos

  $$d_1 = \lambda_1 F_1 + \epsilon_2 \lambda_1 F_2 + \epsilon_3 \lambda_1 F_3,$$

  $$d_2 = (\lambda_2 - \epsilon_2 \lambda_1) F_2 + (\lambda_3 - \epsilon_3 \lambda_1) F_3 + \sum_{j=4}^{t} \lambda_j F_j,$$

  con $\epsilon_i = \pm 1$, y tales que $\partial_1 d_1 = 0$, y por lo tanto $d_2 = d - d_1 \in Z_1(\Delta_m)$. Si suponemos que $d_2 \neq 0$, se tiene que, por ser t

minimal, $d_2 \in B_1(\Delta_m)$. En este caso, $d_1 \notin B_1(\Delta_m)$, y entonces $t = 3$, luego $d_2 = 0$. Tomando $c = (1/\lambda_1)d_1$ ya habríamos terminado la demostración.

- Si $i_4 \neq i_1$, y sabiendo que $i_4 \neq i_2$, e $i_4 \neq i_3$, tenemos que $t \geq 4$.
  Al igual que antes, obtenemos que existe $F_j = \{i_4, i_5\}$, $i_5 \neq i_3, i_4$. De nuevo vamos a considerar $j = 4$ por comodidad de notación.
  Si tuviésemos el caso $i_5 = i_1$, podemos seguir el razonamiento del punto anterior construyendo un elemento $c = \sum_{j=1}^{4} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m)$, por lo que habríamos terminado.
  Si tuviésemos el caso $i_5 = i_2$, podemos seguir el razonamiento del punto anterior construyendo un elemento $c = \sum_{j=2}^{4} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m)$. Pero esto entra en contradicción con $t \geq 4$.
  Por lo tanto, tomamos $F_5 = \{i_5, i_6\}$ y continuamos con este proceso.

Esta construcción es finita al existir un número finito de posibilidades para i_j. Entonces, podemos concluir que existe

$$c = \sum_{j=1}^{t} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m),$$

con

$$F_1 = \{i_1, i_2\},\ F_2 = \{i_2, i_3\},\ F_3 = \{i_3, i_4\},\ \ldots,\ F_t = \{i_t, i_1\},$$

para unos determinados $\epsilon_j = \pm 1\ \forall j = 1, \ldots, t$. Lo que debemos probar ahora es que el polígono σ definido por $F_1, \ldots, F_t$ es ciertamente un F–hueco de Δ_m, donde F es el conjunto $\bigcup_{j=1}^{t} F_j$. Para esto, sólo nos queda probar sobre σ, la segunda condición de la definición de F–hueco.

Supongamos que existe $F' \subset F$, $F' \neq F_j$, $\sharp F' \geq 2$ y $F' \in \Delta_m$. En ese caso, deben existir a su vez dos enteros $i_p, i_q \in F'$ con $p < q$, tales que $\{i_p, i_q\} \neq F_j \neq \{i_q, i_p\}\ \forall j = 1, \ldots, t$. Supongamos por comodidad que $p = 1$ y consideremos $F'' = \{i_1, i_q\}$. Entonces podemos rescribir c de la manera siguiente

$$\begin{array}{rcl} c & = & \sum_{j=1}^{t} \epsilon_j F_j + \epsilon_{t+1} F'' - \epsilon_{t+1} F'' \\ & = & \underbrace{\epsilon_1 F_1 + \epsilon_2 F_2 + \cdots + \epsilon_{q-1} F_{q-1} - \epsilon_{t+1} F''}_{c_1} \underbrace{+ \epsilon_{t+1} F'' + \epsilon_q F_q + \cdots + \epsilon_t F_t}_{c_2} \; . \end{array}$$

Para un determinado $\epsilon_{t+1} = \pm 1$, se tiene que $c_1, c_2 \in Z_1(\Delta_m)$. Por lo tanto, o bien $c_1 \notin B_1(\Delta_m)$ ó $c_2 \notin B_1(\Delta_m)$ ya que $c \notin B_1(\Delta_m)$. Esto entra en contradicción con que t es minimal. ■

Como aclaración a la demostración anterior, cabe decir que los enteros $\epsilon_i = \pm 1$ dependen directamente de la orientación considerada en Δ_m.

Usando este lema, construir el conjunto finito de chequeo, C, pasa por encontrar una condición sobre los $m \in S$ para que exista un polígono σ F–hueco de Δ_m. Nosotros vamos a dar esta condición a través de las bases de Hilbert de ciertos sistemas de ecuaciones diofánticos.

Comencemos definiendo un orden sobre el semigrupo S.

Definición IV–A.4 ■ Sea $>_S$ el orden parcial sobre S definido por: $m \geq_S m'$ si $m - m' \in S$. Dado un subconjunto H de S, diremos que $m \in H$ es S–minimal en H si

$$m \not>_S m', \ \forall m' \in H.$$

La existencia de elementos S–minimales en un subconjunto $H \subset S$ viene garantizada por ser S Nakayama, ya que esto nos asegura que hay una cantidad finita de escrituras de m en función de los generadores de S ([BCMP98b, proposición 1.2]).

Supongamos que σ es un F–hueco de Δ_m, entonces, existe

$$\beta^{(i)} = (\beta_1^{(i)}, \ldots, \beta_{r-t+2}^{(i)}) \in \mathbb{N}^{(r-t+2)t}$$

verificando

$$\left\{\begin{array}{lcll} m-n_{F_1} & = & \sum_{j\in(\Lambda\setminus F)\cup F_1}\beta_j^{(1)}n_j & mod\ a\\ m-n_{F_2} & = & \sum_{j\in(\Lambda\setminus F)\cup F_2}\beta_j^{(2)}n_j & mod\ a\\ & \vdots & & \\ m-n_{F_{t-1}} & = & \sum_{j\in(\Lambda\setminus F)\cup F_{t-1}}\beta_j^{(t-1)}n_j & mod\ a\\ m-n_{F_t} & = & \sum_{j\in(\Lambda\setminus F)\cup F_t}\beta_j^{(t)}n_j & mod\ a \end{array}\right. \Rightarrow \left\{\begin{array}{lcll} m & = & n_{F_1}+\mathcal{A}_{F_1}\beta^{(1)} & mod\ a\\ m & = & n_{F_2}+\mathcal{A}_{F_2}\beta^{(2)} & mod\ a\\ & \vdots & & \\ m & = & n_{F_{t-1}}+\mathcal{A}_{F_{t-1}}\beta^{(t-1)} & mod\ a\\ m & = & n_{F_t}+\mathcal{A}_{F_t}\beta^{(t)} & mod\ a \end{array}\right.$$

donde $\mathcal{A}_{F_i} \in \mathcal{M}_{(h+s)\times(r-t+2)}(\mathbb{Z})$ es la matriz cuyas columnas son las de $\mathcal{A}$ indicadas por el conjunto $(\Lambda \setminus F) \cup F_i$.

Dada $\{e_1, \ldots, e_r\}$ la base canónica de $\mathbb{N}^r$, definimos

$$e_{F_i} := \pi_i(\sum_{j\in F_i} e_j),$$

con $\pi_i : \mathbb{N}^r \to \mathbb{N}^{r-t+2}$ la proyección que elimina las coordenadas correspondientes al conjunto $F \setminus F_i$, $1 \le i \le t$.

Con las notaciones anteriores, tenemos que existe una upla de uplas

$$\alpha = (\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}) \in \mathbb{N}^{(r-t+2)t}$$

tal que

$$m = \mathcal{A}_{F_1}\alpha^{(1)} = \mathcal{A}_{F_2}\alpha^{(2)} = \cdot\cdot\cdot\cdot = \mathcal{A}_{F_t}\alpha^{(t)}\ mod\ a,$$

y $\alpha \gg e_\sigma$ con $e_\sigma := (e_{F_1}, e_{F_2}, \ldots, e_{F_{t-1}}, e_{F_t}) \in \mathbb{N}^{(r-t+2)t}$.

Entonces, la forma de conseguir elementos $m \in S$ tales que σ sea un F–hueco de Δ_m, será computar algunas $\mathbb{N}$–soluciones, $\alpha \in \mathbb{N}^{(r-t+2)t}$, de los sistemas de ecuaciones diofánticos

$$\begin{pmatrix} \mathcal{A}_{F_1} & -\mathcal{A}_{F_2} & 0 & 0 & 0 & & 0 & 0\\ 0 & \mathcal{A}_{F_2} & -\mathcal{A}_{F_3} & 0 & 0 & \cdots & 0 & 0\\ 0 & 0 & \mathcal{A}_{F_3} & -\mathcal{A}_{F_4} & 0 & & 0 & 0\\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & & \mathcal{A}_{F_{t-1}} & -\mathcal{A}_{F_t} \end{pmatrix} \begin{pmatrix} \alpha^{(1)}\\ \alpha^{(2)}\\ \vdots\\ \alpha^{(t-1)}\\ \alpha^{(t)} \end{pmatrix} = 0,$$

donde cada tramo de $(h+s)$ filas del sistema está en congruencia módulo a ($mod\ a$). Un sistema de la forma anterior lo denotaremos por

$$\mathcal{A}_\sigma\alpha = 0\ \ mod\ \tilde{a},$$

donde

$$\mathcal{A}_\sigma := \begin{pmatrix} \mathcal{A}_{F_1} & -\mathcal{A}_{F_2} & 0 & 0 & 0 & & 0 & 0 \\ 0 & \mathcal{A}_{F_2} & -\mathcal{A}_{F_3} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \mathcal{A}_{F_3} & -\mathcal{A}_{F_4} & 0 & & 0 & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & & \mathcal{A}_{F_{t-1}} & -\mathcal{A}_{F_t} \end{pmatrix} \in \mathcal{M}_{(t-1)(h+s)\times(r-t+2)t}(\mathbb{Z}),$$

y el símbolo $mod\,\tilde{a}$ hace referencia a los tramos en congruencias.

Definimos ahora R_σ al conjunto de $\mathbb{N}$–soluciones

$$R_\sigma := \{\alpha = (\alpha^{(1)}, \ldots, \alpha^{(t)}) \in \mathbb{N}^{(r-t+2)t} | \ \mathcal{A}_\sigma \alpha = 0 \ \ mod\ \tilde{a}, \alpha \gg e_\sigma\}.$$

Sea $\mathcal{H}R_\sigma$ el conjunto de los elementos $\gg$ –minimales de R_σ, y ΣR_σ al subconjunto de S,

$$\Sigma R_\sigma := \{p \in S | \ p = \mathcal{A}_{F_1}\alpha^{(1)} = \cdots = \mathcal{A}_{F_t}\alpha^{(t)}, \ (\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}) \in R_\sigma\}.$$

Sea

$$\mathrm{C}_\sigma := \{p \in S | \ p \text{ es } S\text{–minimal en } \Sigma R_\sigma\}.$$

Relacionemos ahora todas estas definiciones y notaciones con el lema IV–A.3, dando un nuevo resultado mediante el cual vamos a poder *atrapar* los elementos de S con primera homología no nula.

Proposición IV–A.5 ■ Si $\tilde{H}_1(\Delta_m) \neq 0$, entonces existe σ un F–hueco de Δ_m tal que $m \in \mathrm{C}_\sigma$.

Demostración. Por el lema IV–A.3, tenemos que existe σ un F–hueco de Δ_m cuyas caras F_i verifican que

$$c = \sum_{j=1}^{t} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m),$$

para ciertos $\epsilon_j = \pm 1$, $\forall j = 1, \ldots, t$. Visto esto, es claro que $m \in \Sigma R_\sigma$.

Supongamos que $m \in \Sigma R_\sigma \backslash \mathrm{C}_\sigma$. En este caso, debe existir $m' \in \mathrm{C}_\sigma$ y $m'' \in S$, tales que $m = m' + m''$.

Si $m'' = 0$, tendríamos probado que $m \in C_\sigma$, y por lo tanto habríamos concluido.

Supongamos entonces que $m'' \neq 0$, $m'' = \sum_{i=1}^{r} d_i n_i$.

Las posibilidades que se plantean son:

- Si $i \in F$. Tomamos un índice l tal que $i \notin F_l$.

$$\left.\begin{array}{lll} d_i \neq 0 & \Rightarrow & m'' - n_i \in S \\ m' \in C_\sigma & \Rightarrow & m' - n_{F_l} \in S \end{array}\right\} \Rightarrow m - n_{F_l} - n_i \in S \Rightarrow F_l \cup \{i\} \in \Delta_m.$$

Esto entra en contradicción con el hecho de que σ es un F–hueco de Δ_m.

- Si $i \notin F$.

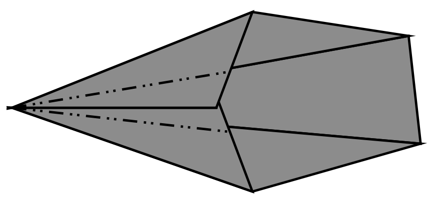
$$\left.\begin{array}{lll} d_i \neq 0 & \Rightarrow & m'' - n_i \in S \\ m' \in C_\sigma & \Rightarrow & m' - n_{F_j} \in S \end{array}\right\} \Rightarrow m - n_{F_j} - n_i \in S,\ \forall j = 1, \ldots, t.$$

Entonces, consideramos $F'_j = F_j \cup \{i\} \in \Delta_m$, $\forall j = 1, \ldots, t$. Es fácil ver que

$$c = \partial_2\left(\sum_{j=1}^{t} \epsilon_j F'_j\right).$$

Esto es una contradicción ya que $c \notin B_1(\Delta_m)$. Gráficamente lo que ocurre es que la figura asociada con el F–hueco es contráctil a un punto, tal y como se aprecia en la figura IV.2.

Figura IV.2. Homología nula



Hemos probado pues que $m \in C_\sigma$. ∎

Relacionados los elementos S–minimales con el lema IV–A.3, nos falta ver que los conjuntos C_σ son finitos y se pueden calcular de manera efectiva. Para hacer esto vamos a considerar el conjunto

$$\Sigma\mathcal{H}R_\sigma := \{p \in S \mid p = \mathcal{A}_{F_1}\alpha^{(1)} = \cdots = \mathcal{A}_{F_t}\alpha^{(t)},\ \alpha = (\alpha^{(1)}, \ldots, \alpha^{(t)}) \in \mathcal{H}R_\sigma\}.$$

Por lo visto en el capítulo II, y en particular por el lema de Dickson, tenemos que $\mathcal{H}R_\sigma$ es un conjunto finito, y por lo tanto también es finito $\Sigma\mathcal{H}R_\sigma$. En el siguiente resultado usamos este hecho para demostrar que C_σ es finito.

Lema IV–A.6 ■ Con las notaciones anteriores, se tiene que

$$\mathrm{C}_\sigma \subset \Sigma\mathcal{H}R_\sigma.$$

En particular, C_σ es finito.

Demostración. Asumamos en un primer momento que $m \in \mathrm{C}_\sigma \setminus \Sigma\mathcal{H}R_\sigma$. En particular tenemos que $m \in \mathrm{C}_\sigma \Rightarrow \exists \alpha = (\alpha^{(1)}, \ldots, \alpha^{(t)}) \in R_\sigma \mid m = \mathcal{A}_{F_1}\alpha^{(1)} = \cdots = \mathcal{A}_{F_t}\alpha^{(t)}$.

Al considerar que $m \notin \Sigma\mathcal{H}R_\sigma$, α no puede ser $\gg$ –minimal en R_σ. Entonces, existen $\alpha' \in \mathcal{H}R_\sigma$ y α'' $\mathbb{N}$–solución de $\mathcal{A}_\sigma\alpha'' = 0$ tal que $\alpha = \alpha' + \alpha''$. Si consideramos el elemento $m' = \mathcal{A}_{F_1}\alpha'^{(1)} \in \Sigma\mathcal{H}R_\sigma$, tenemos que $m - m' \in S$, y por lo tanto m no es S–minimal en ΣR_σ, porque $m \neq m'$. Con ello hemos llegado a una contradicción ya que $m \in \mathrm{C}_\sigma$.

C_σ es un conjunto finito al serlo $\Sigma\mathcal{H}R_\sigma$. ■

Nota IV–A.7 ■ Nótese que el lema IV–A.6 nos relaciona los elementos S–minimales de ΣR_σ con los $\gg$ –minimales de R_σ, $\mathcal{H}R_\sigma$. Esto será una pieza clave a la hora de acotar el grado de las primeras sicigias del álgebra $k[S]$ que veremos en V–B.3. De hecho, en dicha sección acotaremos los grados mediante su pertenencia a $\Sigma\mathcal{H}R_\sigma$ y no por estar en C_σ.

Aplicando ahora el lema IV–A.6, obtenemos un algoritmo para el cálculo de un conjunto finito $\mathrm{C} \subset S$ para chequear los elementos

$m \in S$ tales que $\tilde{H}_1(\Delta_m) \neq 0$.

Algoritmo IV–A.8 ■ Algoritmo de Chequeo

Entrada: un conjunto de generadores $\{n_1, \ldots, n_r\}$ de S.

Salida: C un conjunto finito para chequear los $m \in S$ tales que $\tilde{H}_1(\Delta_m) \neq 0$.

1. $G := \varnothing$ y $\mathcal{F} := \{F \subset \mathcal{P}(\Lambda) | \sharp F \geq 3\}$
2. **Mientras** $\mathcal{F} \neq \varnothing$:
   a) **Para** $F \in \mathcal{F}$ y $\forall\sigma$ polígono cuyo conjunto de vértices es F :
      1) Calcular el subconjunto de $\mathbb{N}$–soluciones, $\mathcal{HR}_\sigma$[1].
      2) Calcular el conjunto C_σ a partir de $\Sigma\mathcal{HR}_\sigma$[2].
      3) $G = G \cup \{(m, \sigma, F) | m \in C_\sigma\}$
   b) $\mathcal{F} = \mathcal{F} \setminus F$.
3. $C := \{m \in S | \sigma\ F$ – hueco de Δ_m y $(m, \sigma, F) \in G\}$

Este algoritmo (IV–A.8) nos permite enunciar el siguiente teorema.

Teorema IV–A.9 ■ El conjunto C_1 de S-grados que aparecen en un sistema minimal de generadores del primer módulo de sicigias de $k[S]$, puede ser calculado de forma efectiva a través de los complejos simpliciales Δ_m, $m \in S$.

Demostración. Inmediata del algoritmo IV–A.8. ■

---

[1] Mediante II–A.4 y los algoritmos de cálculo de $\mathbb{N}$–soluciones del capítulo II , se puede obtener este conjunto calculando las $\mathbb{N}$–soluciones $\gg$ –minimales del sistema

$$\mathcal{A}_\sigma \alpha = -\mathcal{A}_\sigma e_\sigma.$$

[2] Usando el lema IV–A.6, podemos calcular C_σ comprobando si las diferencias de elementos de $\Sigma\mathcal{HR}_\sigma$ están o no en S, i.e. son S–minimales

Usando III–A.4 hemos obtenido un nuevo algoritmo para computar un sistema minimal de generadores de N_1: para todo $m \in C_1$, tomamos una base del espacio $\tilde{H}_1(\Delta_m)$, y a partir de ellos calculamos una base de $V_1(m)$ a través del isomorfismo $\tilde{H}_1(\Delta_m) \cong V_1(m)$.

Corolario IV–A.10 ■ Un conjunto minimal de generadores del primer módulo de sicigias de $k[S]$ puede ser determinado usando el algoritmo IV–A.8.

Con más detalle, para construir a partir del algoritmo IV–A.8 la resolución libre minimal de una variedad tórica, hay que aplicar el algoritmo III–A.5. El primer paso, el cálculo del conjunto C_1, se realiza a partir de un conjunto finito que lo contiene, C, y que es la salida del algoritmo IV–A.8. Una vez obtenido C, eliminamos de este conjunto los elementos $m \in \mathrm{C} \subset S$ tales que la homología reducida asociada a Δ_m es nula. El resultado de esta selección es el conjunto C_1.

IV–B. NOTAS

Aunque el comportamiento computacional de los algoritmos que hemos descrito en este capítulo no es bueno, su importancia radica en que nos permite comprender combinatoriamente el álgebra asociada a un semigrupo. Ésta es la diferencia principal con los algoritmos basados en bases de Gröbner (ver [EIS95, teorema de Schreyer]), ya que estos sólo son una herramienta de cálculo, y no una vía de comprensión.

CAPÍTULO V

Cálculo de la Resolución Libre Minimal

INTRODUCCIÓN

Como en capítulos anteriores, vamos a considerar

$$S = < n_1, \ldots, n_r > \subset \mathbb{Z}^h \oplus \mathbb{Z}/a_1 \oplus \cdots \oplus \mathbb{Z}/a_s$$

con $a = (a_1, \ldots, a_s) \in \mathbb{Z}^s$, y tal que $S \cap (-S) = \{0\}$. Sea $\Lambda = \{1, \ldots, r\}$, y sea C_i el conjunto

$$C_i := \{m \in S \mid \tilde{H}_i(\Delta_m) \neq 0\}.$$

En este capítulo vamos a dar un conjunto finito de chequeo, C'_i, tal que si existe un elemento en un sistema minimal de generadores del i–ésimo módulo de sicigia de $k[S]$, su grado pertenece a C'_i, es decir, $C_i \subset \mathrm{C}'_i$. Para ello generalizaremos los resultados obtenidos para $i = 1$ en el capítulo anterior, sorteando los distintos problemas que surgen al generalizar.

Además, a partir de los conjuntos C'_i anteriores, acotaremos el grado de los elementos que aparecen en un sistema minimal de generadores del i–ésimo módulo de sicigias de nuestra álgebra $k[S]$. Comenzaremos dando una cota para la primera sicigia, y después generalizaremos esta cota a cualquier sicigia. Por último, explicitaremos una cota para la regularidad de una variedad tórica proyectiva, y un algoritmo para calcular la propia regularidad.

V–A. CONJUNTO FINITO DE CHEQUEO

El siguiente lema va a ser una pieza clave en la generalización, ya que al igual que IV–A.3, nos da una aproximación de cómo son los complejos simpliciales cuya i–ésima homología es no nula. Gracias a esta aproximación, podremos dar un método de cálculo de C'_i.

Lema V–A.1 ■ Supongamos que $\tilde{H}_i(\Delta_m)$ es no nula, y sea $c \in \tilde{Z}_i(\Delta_m) \setminus \tilde{B}_i(\Delta_m)$, $c = \sum_{j=1}^{t} \lambda_j F_j$, $\lambda_j \in k \setminus \{0\}$ para cada $j = 1, \ldots, t$, tales que $F_j \neq F_l$ si $j \neq l$. Si $F = \bigcup_{j=1}^{t} F_j$, entonces se tiene que

$$\forall p \in F \quad \exists q, 1 \leq q \leq t \ \mid \ p \notin F_q \text{ y } F_q \cup \{p\} \notin \Delta_m.$$

Demostración. Comencemos probando que $\forall p \in F$, $\exists j$, $1 \leq j \leq t$, tal que $p \notin F_j$. Supongamos para ello lo contrario, es decir, $p \in F$ y $p \in F_j$ para cualquier j, $1 \leq j \leq t$. En ese caso,

$$c' = \sum_{j=1}^{t} \lambda_j \epsilon_{F_j (F_j \setminus \{p\})} (F_j \setminus \{p\}) \in \tilde{C}_{i-1}(\Delta_m).$$

Pero $c' = 0$ porque $\partial_i(c) = 0$, y por lo tanto $\lambda_j = 0$, $\forall j = 1, \ldots, t$. Esto no es posible al ser c no nulo, luego ya hemos probado nuestro primer paso en la demostración.

Fijemos $p \in F$ y supongamos por comodidad que $p \notin F_1$. Si $F_1 \cup \{p\} \notin \Delta_m$ habríamos terminado la prueba. En caso contrario, $F_1 \cup \{p\} \in \Delta_m$, consideramos el número $l := \sharp\{j \mid p \notin F_j\}$ y el conjunto $F'_1 = F_1 \cup \{p\}$.

Tomemos $c_1 := c - \lambda_1 \epsilon_{F'_1 F_1} \partial_{i+1}(F'_1)$. Es claro que $c_1 \in \tilde{Z}_i(\Delta_m) \setminus \tilde{B}_i(\Delta_m)$.

Esta suma queda como sigue,

$$c_1 = \sum_{j=2}^{t} \lambda_j F_j + \sum_{dim(F')=i, F' \neq F_1} \lambda_1 \epsilon_{F_1 F'} F'.$$

Por lo tanto, c_1 se puede reescribir como $c_1 = \sum_{j=1}^{t^{(1)}} \lambda_j^{(1)} F_j^{(1)}$, donde $\lambda_j^{(1)} \in k \setminus \{0\}$ para cualquier $j = 1, \dots, t^{(1)}$, y $F_j^{(1)} \neq F_k^{(1)}$ si $j \neq k$. Sea $l^{(1)} := \sharp\{j \mid p \notin F_j^{(1)}\}$ y sea $F^{(1)} := \bigcup_{j=1}^{t^{(1)}} F_j^{(1)}$. Estos dos elementos satisfacen las siguientes propiedades:

$(*)_1$: $\sharp F^{(1)} \leq \sharp F$.

$(**)_1$: Si $p \notin F_j^{(1)}$, existe q, $2 \leq q \leq t$ tal que $F_j^{(1)} = F_q$.

$(***)_1$: $l^{(1)} < l$.

En realidad, para construir c_1, sólo hemos reemplazado en c, la cara F_1 por varias caras distintas a F_1 que sí contienen a p.

Vamos a continuar con este proceso mediante una inducción en $\sharp F$.

Si $\sharp F$ es mínimo, tenemos la igualdad $\sharp F^{(1)} = \sharp F$. En cualquier caso, nuestro nuevo conjunto $F^{(1)}$ sigue verificando que $p \in F^{(1)}$ y que $l^{(1)} \neq 0$. Por razonamientos análogos al anterior, ahora sobre c_1, sabemos que existe j, $1 \leq j \leq t^{(1)}$, tal que $p \notin F_j^{(1)}$, luego, por $(**)_1$, $F_j^{(1)} = F_q$ para algún q, $2 \leq q \leq t$. Si $F_j^{(1)} \cup \{p\} \notin \Delta_m$, habríamos terminado. En caso contrario, $F_j^{(1)} \cup \{p\} \in \Delta_m$, podemos construir a partir de c_1, y de manera análoga a su obtención, un nuevo elemento $c_2 \in \tilde{Z}_i(\Delta_m) \setminus \tilde{B}_i(\Delta_m)$, $c_2 = \sum_{j=1}^{t^{(2)}} \lambda_j^{(2)} F_j^{(2)}$ donde $\lambda_j^{(2)} \in k \setminus \{0\}$ para cualquier $j = 1, \dots, t^{(2)}$, y tal que $F_j^{(2)} \neq F_k^{(2)}$ si $j \neq k$. Definiendo $l^{(2)} := \sharp\{j \mid p \notin F_j^{(2)}\}$, y $F^{(2)} := \bigcup_{j=1}^{t^{(2)}} F_j^{(2)}$ obtenemos de nuevo:

$(*)_2$: $\sharp F^{(2)} \leq \sharp F^{(1)}$.

$(**)_2$: Si $p \notin F_j^{(2)}$, existe q, $2 \leq q \leq t^{(1)}$ tal que $F_j^{(2)} = F_q^{(1)}$.

$(***)_2$: $l^{(2)} < l^{(1)}$.

De nuevo tenemos en $(*)_2$ la igualdad porque $\sharp F$ es mínimo, y de nuevo $p \in F^{(2)}$ y $l^{(2)} \neq 0$. Nuestro resultado se obtiene por recurrencia ya que este proceso termina en un número finito de pasos gracias a la propiedad $(* * *)$.

Supongamos ahora que nuestro resultado es cierto para cualquier $c' \in \tilde{Z}_i(\Delta_m) \setminus \tilde{B}_i(\Delta_m)$, $c' = \sum_{j=1}^{t'} \lambda'_j F'_j$ donde $\lambda'_j \in k \setminus \{0\}$ para cualquier $j = 1, \dots, t'$, $F'_j \neq F'_l$ si $j \neq l$, y con $\sharp F' < \sharp F$ donde $F' = \bigcup_{j=1}^{t'} F'_j$. Entonces:

- Si en $(*)_1$ no se alcanza la igualdad, es suficiente aplicar la hipótesis de inducción a c_1. Entonces obtenemos que existe $F_j^{(1)}$ tal que $p \notin F_j^{(1)}$ y $F_j^{(1)} \cup \{p\} \notin \Delta_m$. Por $(**)_1$, $F_j^{(1)} = F_q$ con $2 \leq q \leq t$, luego habríamos terminado.
- Si en $(*)_1$ se alcanza la igualdad, repetimos el mismo argumento que en el caso $\sharp F$ mínimo. Si no terminamos, construimos c_2 como antes. De nuevo, obtenemos el resultado por inducción si en $(*)_2$ no se tiene la igualdad. En otro caso continuamos este proceso, el cual es finito ya que la propiedad $(* * *)$ nos lo garantiza.

Con ello ya hemos probado el resultado. ∎

Este lema (V–A.1) asocia a cada $m \in S$ con $\tilde{H}_i(\Delta_m) \neq 0$ un conjunto $F \subset \Lambda$ y una serie de subconjuntos $F_1, \dots, F_t \in \Delta_m$ tales que:

1. $F = \bigcup_{j=1}^{t} F_j$
2. $\dim(F_j) = i, \ \forall j = 1, \dots, t$
3. $F \notin \Delta_m$

Usaremos estas propiedades para dar unas nuevas definiciones sobre subconjuntos de Λ.

Definición V–A.2 ■ Sea el conjunto $F \subset \Lambda$, diremos que $\tau = \{F_1, \dots, F_t\}$ es una i–triangulación de F si se satisfacen las siguientes propiedades:

1. $\dim(F_j) = i, \ \forall j = 1, \dots, t$

2. $F = \bigcup_{j=1}^{t} F_j$

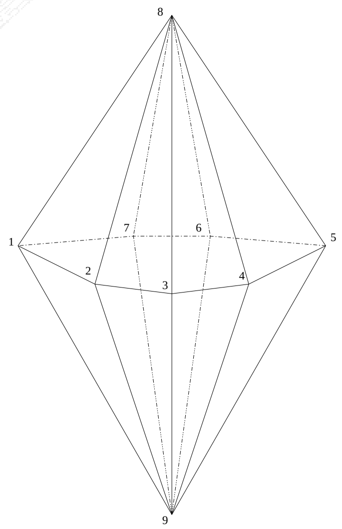
Además, diremos que τ es una i–triangulación de F en Δ_m, con $m \in S$, si $F_j \in \Delta_m$, $\forall j = 1, \ldots, t$, y $F \notin \Delta_m$.

Nótese que $\tau = \{F_1, \ldots, F_t\}$ es una triangulación de F en caras de Δ_m de dimensión i. Esto es una generalización de la definición de F–hueco, ya que un F–hueco es un tipo especial de 1–triangulación de F en Δ_m.

En el siguiente ejemplo tenemos una 2–triangulación de un complejo simplicial.

Ejemplo V–A.3 ■ Fijado $F = \{1, \ldots, 9\}$, y el complejo Δ_m dado por la figura V.1 podemos

Figura V.1. i–triangulación



definir τ como una 2–triangulación de F en Δ_m,

$$\begin{array}{ll} F_1 = \{1,2,8\} & F_2 = \{1,2,9\} \\ F_3 = \{2,3,8\} & F_4 = \{2,3,9\} \\ F_5 = \{3,4,8\} & F_6 = \{3,4,9\} \\ F_7 = \{4,5,8\} & F_8 = \{4,5,9\} \\ F_9 = \{5,6,8\} & F_{10} = \{5,6,9\} \\ F_{11} = \{6,7,8\} & F_{12} = \{6,7,9\} \\ F_{13} = \{7,1,8\} & F_{14} = \{7,1,9\} \end{array}$$
$$\tau = \{F_1, \cdots, F_{14}\}$$

Tenemos un resultado, análogo al lema IV–A.3, que nos relaciona las triangulaciones con los elementos en S tales que su i–ésima homología es no nula.

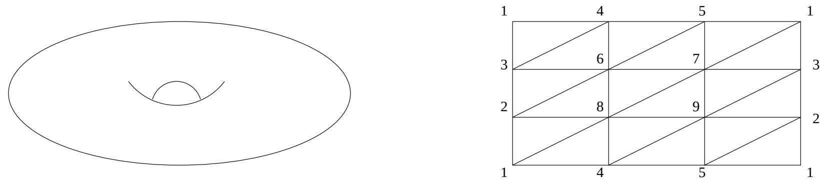
Lema V–A.4 ■ Si $\tilde{H}_i(\Delta_m)$ es no nula, entonces existe un conjunto $F \subset \Lambda$ y τ una i–triangulación de F en Δ_m.

Demostración. Es suficiente tomar el elemento $c \in \tilde{Z}_i(\Delta_m) \setminus \tilde{B}_i(\Delta_m)$ y los conjuntos $F, F_1, \ldots, F_t$ como en el lema V–A.1. ■

Nótese que dado un elemento del semigrupo, $m \in S$, ni el conjunto F ni la triangulación τ anteriores son únicos en general. Veamos mediante el siguiente ejemplo que, dado un conjunto F, pueden existir triangulaciones de distinta forma.

Ejemplo V–A.5 ■ Dado el mismo conjunto $F = \{1, \ldots, 9\}$ del ejemplo V–A.3, podemos considerar sobre él una 2–triangulación correspondiente a la figura V.2 dada por

Figura V.2. Triangulación del Toro



$$
\begin{array}{lll}
F_1 = \{1,3,4\} & F_2 = \{3,4,6\} & F_3 = \{3,6,2\} \\
F_4 = \{2,6,8\} & F_5 = \{2,8,1\} & F_6 = \{1,8,4\} \\
F_7 = \{4,6,5\} & F_8 = \{6,5,7\} & F_9 = \{6,7,8\} \\
F_{10} = \{7,8,9\} & F_{11} = \{8,9,4\} & F_{12} = \{9,4,5\} \\
F_{13} = \{5,1,7\} & F_{14} = \{1,7,3\} & F_{15} = \{7,3,9\} \\
F_{16} = \{3,9,2\} & F_{17} = \{9,2,5\} & F_{18} = \{2,5,1\}
\end{array}
$$

$$\tau = \{F_1, \cdots, F_{18}\}$$

Supongamos que $\tau = \{F_1, \ldots, F_t\}$ es una i–triangulación de F en Δ_m. De manera similar a lo que hicimos con los F–huecos, vamos a buscar nuestras triangulaciones a través de unos determinados sistemas diofánticos que pasamos a construir.

Recordemos que la propiedad $F_i \in \Delta_m$, es equivalente a $m - n_{F_i} \in S$. Esto significa que existen $\alpha_j \in \mathbb{N}$ tales que $m = \sum_{j=1}^{r} \alpha_j n_j$, con $\alpha_j \geq 1$ para cualquier $j \in F_i$. Recordemos también que $\mathcal{A}$ es la matriz cuyas columnas son los generadores de S, considerados sus elementos sin congruencias, i.e. $\mathcal{A} := (n_1 | \ldots | n_r) \in \mathcal{M}_{(h+s)\times r}(\mathbb{Z})$.

Denotaremos por $e_{F_l} \in \mathbb{N}^r$ al vector con todas sus coordenadas nulas salvo la j–ésima que vale 1 para todo $j \in F_l$. Nótese que esta definición de e_{F_l} es distinta de la aparecida en el capítulo IV.

Consideremos la matriz con coeficientes enteros

$$\mathcal{A}(t) := \begin{pmatrix} \mathcal{A} & -\mathcal{A} & 0 & 0 & 0 & & 0 & 0 \\ 0 & \mathcal{A} & -\mathcal{A} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \mathcal{A} & -\mathcal{A} & 0 & & 0 & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & & \mathcal{A} & -\mathcal{A} \end{pmatrix} \in \mathcal{M}_{(h+s)(t-1)\times rt}(\mathbb{Z})$$

y $e_\tau := (e_{F_1}, \ldots, e_{F_t}) \in \mathbb{N}^{rt}$.

Entonces de cada τ i–triangulación de F en Δ_m, se obtiene un vector $\alpha = (\alpha^{(1)}, \ldots, \alpha^{(t)}) \in \mathbb{N}^{rt}$ verificando:

1. $\mathcal{A}(t)\alpha = 0 \mod \tilde{a}$.
2. $\alpha \gg e_\tau$
3. $m = \mathcal{A}\alpha^{(1)} = \ldots = \mathcal{A}\alpha^{(t)}$.

Como ya vimos en el capítulo dedicado al cálculo de C_1, estamos buscando los elementos $m \in S$ tal que $\tilde{H}_i(\Delta_m) \neq 0$, luego tenemos que proceder de manera inversa.

Fijemos $F \subset \Lambda$ y $\tau = \{F_1, \ldots, F_t\}$ una i–triangulación de F, y consideremos ahora que m no está fijada. Vamos a buscar entonces los elementos $m \in S$ tales que τ es una i-triangulación de F en Δ_m. De manera análoga al capítulo IV, definimos los conjuntos:

$$R_\tau := \{\alpha = (\alpha^{(1)}, \ldots, \alpha^{(t)}) \in \mathbb{N}^{rt} \;\mid\; \mathcal{A}(t)\alpha = 0 \mod \tilde{a}, \alpha \gg e_\tau\},$$

$$\Sigma R_\tau := \{m \in S \;\mid\; m = \mathcal{A}\alpha^{(1)}, \alpha = (\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}) \in R_\tau\}.$$

Gracias al lema V–A.1, sabemos que si $m \in S$ verifica que $\tilde{H}_i(\Delta_m) \neq 0$, podemos encontrar un conjunto de vértices F y una τ i–triangulación de F, tal que $m \in \Sigma R_\tau$. Tenemos pues que

$$C_i \subset \bigcup_F \bigcup_\tau \Sigma R_\tau,$$

donde la unión es sobre todas las τ i–triangulaciones de F, y $F \subset \Lambda$ con $\sharp F \geq i+2$ (F proviene del lema V–A.1).

Como ya vimos, los conjuntos ΣR_τ no son, en general, finitos, pero si lo son los conjuntos formados por sus elementos $\gg$ –minimales $\mathcal{H}R_\tau := \{\alpha \in R_\tau \mid \alpha \text{ es minimal para } \gg\}$. A partir de estos, definimos en S una serie de subconjuntos finitos con los que vamos a calcular C_i,

$$\Sigma\mathcal{H}R_\tau := \{m \in S \mid m = \mathcal{A}\alpha^{(1)}, \alpha = (\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}) \in \mathcal{H}R_\tau\}$$

y

$$C_\tau := \{m \in S \mid m \text{ es } S\text{–minimal en } \Sigma R_\tau\}.$$

El conjunto $\Sigma\mathcal{H}R_\tau$ es finito por serlo $\mathcal{H}R_\tau$, y C_τ es también finito por estar contenido en $\Sigma\mathcal{H}R_\tau$ como nos prueba el siguiente lema.

Lema V–A.6 ■ En las condiciones anteriores,

$$C_\tau \subset \Sigma\mathcal{H}R_\tau.$$

En particular, C_τ es finito.

Demostración. Esta demostración es análoga a la del lema IV–A.6. ■

Estamos ya en condiciones de dar, al igual que para el caso de la primera sicigia IV–A.5, un resultado que nos *atrape* los elementos de S cuya i–ésima homología es no nula.

Proposición V–A.7 ■ Si $m \in S$ y $\tilde{H}_i(\Delta_m) \neq 0$, entonces existe un conjunto de vértices, $F \subset \Lambda$ con $\sharp F \geq i+2$, y una τ i-triangulación de F en Δ_m, tal que $m \in C_\tau$.

Demostración. Al suponer que $\tilde{H}_i(\Delta_m) \neq 0$, existe un elemento no nulo en este conjunto, $c \in \tilde{Z}_i(\Delta_m) \setminus \tilde{B}_i(\Delta_m)$, verificando que $c = \sum_{j=1}^{t} \lambda_j F_j$, con $\lambda_j \in k \setminus \{0\}$ para cualquier $j = 1, \ldots, t$, y con $F_j \neq F_l$ si $j \neq l$. Por V–A.1, tomando $F = \bigcup_{j=1}^{t} F_j$ y $\tau = \{F_1, \ldots, F_t\}$, tenemos que τ es una i–triangulación de F en Δ_m y que $m \in \Sigma R_\tau$. Falta probar que, efectivamente, $m \in C_\tau$.

Al estar $m \in \Sigma R_\tau$, tenemos que es suma de un elemento S–minimal en ΣR_τ, $m' \in C_\tau$, y de un elemento $m'' \in S : m = m' + m''$. Si $m'' = 0$, tendríamos que $m = m' \in C_\tau$ y habríamos terminado la demostración.

Supongamos que $m'' \neq 0$. $m'' \in S$ implica directamente que admite una escritura del tipo $m'' = \sum_{j=1}^{r} \beta_j n_j$ con $\beta_j \in \mathbb{N}$ para cualquier j, $1 \leq j \leq r$. Por comodidad en la demostración, supongamos que $\beta_1 \neq 0$. Si $1 \in F$, aplicamos el lema V–A.1 para $p = 1$. Entonces, existirá q, $1 \leq q \leq t$, tal que $1 \notin F_q$ y $F_q \cup \{1\} \notin \Delta_m$. En cualquier caso, $m' - n_{F_q} \in S$ porque $m' \in C_\tau$, y $m'' - n_1 \in S$ porque $\beta_1 \neq 0$. Tenemos entonces que $m - n_{F_q} - n_1 = m' + m'' - n_{F_q} - n_1 \in S$. Este hecho contradice que $F_q \cup \{1\} \notin \Delta_m$ y por lo tanto se deduce que $1 \notin F$.

Al no estar 1 en F y ser $m = m' + m''$, tenemos que $m - n_{F_j} - n_1 \in S$, para cualquier j. Sea $F'_j = F_j \cup \{1\} \in \Delta_m$ y sea

$$c' = \sum_{j=1}^{t} \lambda_j F'_j \in \tilde{C}_{i+1}(\Delta_m).$$

Vamos a probar que $\partial_{i+1} c' = c$. Para simplificar los cálculos vamos a considerar la orientación natural sobre las caras de Δ_m.

Como $\partial_i c = 0$, tenemos que

$$\sum_{j=1}^{t} \lambda_j \epsilon_{F_j F'} = 0, \text{ para todo } F' \text{ con } \dim(F') = i - 1. \qquad \text{(V–A.1)}$$

Por otro lado

$$\partial_{i+1}(c') = \sum_{dim(F'')=i} \left(\sum_{j=1}^{t} \lambda_j \epsilon_{F'_j F''} \right) F''.$$

Vamos a probar que

$$c = \sum_{1 \notin F''} \left(\sum_{j=1}^{t} \lambda_j \epsilon_{F'_j F''} \right) F'' \qquad \text{(V–A.2)}$$

y

$$0 = \sum_{1 \in F''} \left(\sum_{j=1}^{t} \lambda_j \epsilon_{F'_j F''} \right) F''. \qquad \text{(V–A.3)}$$

Si $1 \notin F''$ y $\epsilon_{F'_l F''} \neq 0$, para algún $1 \leq l \leq t$, tenemos que $1 \notin F'' \subset F'_l = F_l \cup \{1\}$, y entonces $F'' = F_l$. En cualquier caso, l es única y tenemos

$$\sum_{j=1}^{t} \lambda_j \epsilon_{F'_j F''} = \lambda_l \epsilon_{F'_l F''} = \lambda_l.$$

Esto prueba (V–A.2).

Para probar (V–A.3), supongamos que $1 \in F''$ y que $\epsilon_{F'_l F''} \neq 0$, para algún $1 \leq l \leq t$. Como $1 \in F'' \subset F'_l$, tenemos que $F'' = \{1\} \cup F'$ con $F' \subset F'_l$ y $\dim(F') = i - 1$. Además como $\epsilon_{F'_j F''} = -\epsilon_{F_j F'}$ y usando (V–A.1), tenemos (V–A.3).

Esto prueba que $\partial_{i+1} c' = c$, y por lo tanto $c \in \tilde{B}_i(\Delta_m)$, llegando a una contradicción. La contradicción surge de suponer que $m'' \neq 0$, luego m'' es realmente el elemento neutro de S, probándose así nuestro resultado. ∎

Por la proposición anterior (V–A.7) tenemos la inclusión

$$C_i \subset \bigcup_F \bigcup_\tau C_\tau,$$

donde $F \subset \Lambda$, $\sharp F \geq i + 2$, y τ es una i–triangulación de F. Al ser cada C_τ finito (lema V–A.6), hemos encontrado un conjunto finito conteniendo a C_i. Podríamos considerar ya este conjunto como C'_i, pero aún podemos afinar un poco más el resultado mediante el siguiente hecho: si $m \in C_\tau$ con $\tau = \{F_1, \ldots, F_t\}$ i–triangulación de F, tenemos la garantía de que $F_j \in \Delta_m$, $\forall j$, $1 \leq j \leq t$, pero puede ocurrir que $F \in \Delta_m$, es decir, τ sea una i–triangulación de F, pero no una i–triangulación de F en Δ_m. Para descartar ese caso, definimos los conjuntos

$$C'_\tau := \{m \in C_\tau \mid F \notin \Delta_m\},$$

que lo excluyen, y sus uniones

$$C_i(F) := \bigcup_\tau C'_\tau.$$

El siguiente teorema nos da, para cada i, un conjunto finito que contiene a los grados que aparecen en un sistema minimal de generadores del i–ésimo módulo de sicigias de $k[S]$.

Teorema V–A.8 ■ El conjunto, C_i, de los S–grados de las i–ésimas sicigias minimales de $k[S]$, está contenido en el conjunto finito

$$C_i' := \bigcup_{F\subset\Lambda,\, \sharp F\geq i+2} C_i(F).$$

Al igual que ocurría en el capítulo IV, la construcción de C_i' puede realizarse de manera efectiva, ya que estamos calculando $\mathbb{N}$–soluciones a sistemas diofánticos. Por lo tanto, tenemos un algoritmo para construir un conjunto de grados que contienen al conjunto formado por los grados de un sistema minimal de generadores del i–ésimo módulo de sicigias del álgebra $k[S]$.

Algoritmo V–A.9 ■ Algoritmo de Chequeo
Entrada: un conjunto de generadores $\{n_1, \ldots, n_r\}$ de S.
Salida: C_i' un conjunto finito para chequear los $m \in S$ tales que $\tilde{H}_i(\Delta_m) \neq 0$.

1. $G := \emptyset$ y $\mathcal{F} := \{F \subset \mathcal{P}(\Lambda) \mid \sharp F \geq i+2\}$
2. **Mientras** $\mathcal{F} \neq \emptyset$:
   a) **Para** $F \in \mathcal{F}$ y $\forall \tau$ i–triangulación de F :
      1) Calcular el subconjunto de $\mathbb{N}$–soluciones, $\mathcal{HR}_\tau$[1].
      2) Calcular el conjunto C_τ a partir de $\mathcal{HR}_\tau$[2].
      3) $G = G \cup \{(m, \tau, F) \mid m \in \mathrm{C}_\tau\}$
   b) $\mathcal{F} = \mathcal{F} \setminus F$.
3. $\mathrm{C}_i' := \{m \in S \mid (m, \tau, F) \in G, F \notin \Delta_m\}$

Este algoritmo (V–A.9) nos permite enunciar el siguiente teorema análogo a IV–A.9.

[1] Cálculo análogo a IV–A.8.
[2] Cálculo análogo a IV–A.8.

Teorema V–A.10 ■ El conjunto C_i de S-grados que aparecen en un sistema minimal de generadores del i–ésimo módulo de sicigias de $k[S]$, puede ser calculado de forma efectiva a través de los complejos simpliciales Δ_m, $m \in S$.

Demostración. Inmediata del algoritmo V–A.9. ■

Este teorema, junto con el algoritmo III–A.5, nos permiten enunciar el siguiente corolario.

Corolario V–A.11 ■ Un conjunto minimal de generadores del i–ésimo módulo de sicigias de la resolución libre minimal de una variedad tórica puede ser determinado usando el algoritmo V–A.9.

La forma de obtener el conjunto minimal de generadores que nos refiere el corolario anterior pasa por aplicar III–A.5. Una vez obtenido un superconjunto finito C_i' que contiene a C_i, hay que eliminar de C_i' los elementos cuya homología asociada a su complejo simplicial sea nula. Así obtenemos el conjunto C_i. Con esto queda justificado que III–A.5 es un algoritmo.

V–B. COTAS DE LOS S–GRADOS

Como ya hemos visto, nuestros conjuntos de chequeo, ya sean para la primera como para la i–ésima sicigia, se obtienen a través de una serie de subconjuntos de ciertas $\mathbb{N}$–soluciones minimales de ecuaciones diofánticas. Vamos a usar este hecho para dar una cota de los grados que aparecen en un sistema minimal de generadores del i–ésimo módulo de sicigias de $k[S]$. Nuestras cotas sólo dependerán de los generadores del semigrupo.

Para obtener estas cotas, vamos a recurrir a las cotas sobre las $\mathbb{N}$–soluciones que hemos dado en la sección II–B, y en particular usaremos la dada por Pottier, (II–B.3).

Sea

$$T := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ a_1 & -a_1 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & a_2 & -a_2 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & a_3 & -a_3 & 0 & & 0 & 0 \\ & & & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & & a_s & -a_s \end{pmatrix} \in \mathcal{M}(\mathbb{Z})_{(h+s)\times 2s}.$$

Denotaremos por $\tilde{T}$ a la matriz

$$\begin{pmatrix} T & 0 & 0 & & 0 \\ 0 & T & 0 & \cdots & 0 \\ 0 & 0 & T & & 0 \\ & \ddots & \ddots & & \\ 0 & 0 & 0 & & T \end{pmatrix} \in \mathcal{M}(\mathbb{Z})_{(t-1)(h+s)\times 2s(t-1)}.$$

Fijemos $m \in C_i$. Aplicando la proposición V–A.7, sabemos que existe un conjunto $F \subset \Lambda$, con $\sharp F \geq i+2$, y existe τ una i–triangulación de F en Δ_m, tal que $m \in C_\tau$. Hemos visto también que por el lema V–A.6, $m \in \Sigma\mathcal{HR}_\tau$. Y entonces existe $\alpha \in \mathcal{HR}_\tau$ tal que $m = \mathcal{A}\alpha^{(1)}$, donde $\alpha = (\alpha^{(1)}, \ldots, \alpha^{(t)})$.

Tenemos que $\alpha \in \mathcal{HR}_\tau$ si y sólo si

$$\alpha - e_\tau \in \mathcal{H}\{\beta \in \mathbb{N}^{rt} \mid \mathcal{A}(t)(\beta + e_\tau) = 0 \text{ mód } \tilde{a}\}$$

y si y sólo si existe $\lambda \in \mathbb{N}^{2s}$ tal que

$$(\alpha - e_\tau, \lambda, 1) \in \mathcal{H}\{\beta \in \mathbb{N}^{rt+2s} | \mathcal{A}_\tau \beta = 0\},$$

con $\mathcal{A}_\tau := (\mathcal{A}(t)|\tilde{T}|\mathcal{A}(t)e_\tau) \in \mathcal{M}_{(h+s)(t-1)\times(rt+2s(t-1)+1)}(\mathbb{Z})$. Nótese que e_τ sigue la definición dada en V–A para i–triangulaciones.

Lema V–B.1 ■ Con las notaciones anteriores, se tiene

$$||(\alpha - e_\tau, \lambda, 1)||_1 \leq (1 + 2 \max_j\{|a_j|\} + 4||\mathcal{A}||_1)^{(h+s)(d_i-1)},$$

con $d_i := \binom{r}{i+1}$.

Demostración. Usando los razonamientos anteriores, hemos llegado a que $(\alpha - e_\tau, \lambda, 1) \in \mathcal{H}(\mathcal{A}_\tau)$. Por (II–B.3)

$$||(\alpha - e_\tau, \lambda, 1)||_1 \leq (1 + ||\mathcal{A}_\tau||_1)^{(h+s)(t-1)}.$$

Como la matriz $\mathcal{A}_\tau$ tiene $(h+s)(t-1)$ filas, donde $\sharp\tau = t$, $\tau = \{F_1, \ldots, F_t\}$, $F_j \subset F$, y $\sharp F_j = i+1$, para cualquier j. Entonces $t = \sharp\tau \leq \binom{\sharp F}{i+1} \leq \binom{r}{i+1} = d_i$, y por lo tanto, $(h+s)(t-1) \leq (h+s)(d_i-1)$.

Veamos ahora que $||\mathcal{A}_\tau||_1 \leq 4||\mathcal{A}||_1 + 2\max\{|a_j|\}$.

$$\begin{array}{rcl} ||\mathcal{A}_\tau||_1 & \leq & ||\mathcal{A}(t)||_1 + ||\tilde{T}||_1 + ||\mathcal{A}(t)e_\tau||_1 \\ & = & 2||\mathcal{A}||_1 + 2\max\{|a_j|\} + ||\mathcal{A}(t)e_\tau||_1 \\ & \leq & 2||\mathcal{A}||_1 + 2\max\{|a_j|\} + 2||\mathcal{A}||_1 \\ & = & 4||\mathcal{A}||_1 + 2\max\{|a_j|\}. \end{array}$$

■

Aplicando este resultado a los grados de la resolución, obtenemos el siguiente teorema.

Teorema V–B.2 ■ Si $m \in S$ es un S–grado de una i–sicigia minimal de $k[S]$, entonces $m = \mathcal{A}x$ con $x \in \mathbb{N}^r$ tal que

$$||x||_1 \leq (1 + 2\max\{|a_j|\} + 4||\mathcal{A}||_1)^{(h+s)(d_i-1)} + (i+1)d_i - 1,$$

donde $d_i = \binom{r}{i+1}$.

Demostración. Con la notación del lema V–B.1 tenemos $m = \mathcal{A}\alpha^{(1)}$ con $\alpha = (\alpha^{(1)}, \dots, \alpha^{(t)})$ verificando el lema. Para la demostración es suficiente notar que

$$||\alpha^{(1)}||_1 \leq ||\alpha||_1 = ||\alpha - e_\tau + e_\tau||_1 \leq ||\alpha - e_\tau||_1 + ||e_\tau||_1 \leq ||(\alpha - e_\tau, \lambda, 1)||_1 - 1 + (i+1)t.$$

Ahora por V–B.1, $||\alpha^{(1)}||_1 \leq (1 + 2\,\text{máx}\{|a_j|\} + 4||\mathcal{A}||_{1,\infty})^{(h+s)(d_i-1)} + (i+1)d_i - 1$. ■

En el caso $i = 1$, puede conseguirse una sustancial mejora en la cota anterior. Dicha mejora proviene de que un F–hueco es un tipo especial de 1−triangulación.

En

$$\mathcal{M}_{(t-1)(h+s)\times((r-t+2)t+2s(t-1))}(\mathbb{Z}),$$

consideramos la matriz

$$\tilde{\mathcal{A}}_\sigma := \begin{pmatrix} \mathcal{A}_{F_1} & -\mathcal{A}_{F_2} & 0 & 0 & 0 & & 0 & 0 & T & 0 & 0 & & 0 \\ 0 & \mathcal{A}_{F_2} & -\mathcal{A}_{F_3} & 0 & 0 & \cdots & 0 & 0 & 0 & T & 0 & \cdots & 0 \\ 0 & 0 & \mathcal{A}_{F_3} & -\mathcal{A}_{F_4} & 0 & & 0 & 0 & 0 & 0 & T & & 0 \\ & & \ddots & \ddots & \ddots & & & & & \ddots & \ddots & & \\ 0 & 0 & 0 & 0 & 0 & & \mathcal{A}_{F_{t-1}} & -\mathcal{A}_{F_t} & 0 & 0 & 0 & & T \end{pmatrix}$$

Vamos a definir unos enteros positivos que dependen directa y exclusivamente del conjunto de generadores tomados en S : sea

$$D := max_{\eta \text{ polígono sobre } F, F\subset\Lambda}\{D_\eta\}$$

con

$$D_\eta := sup_i\{\sum_j |(\mathcal{A}_\eta \mid \mathcal{A}_\eta e_\eta)(i,j)|\} \in \mathbb{N}.$$

Obtenemos así el siguiente resultado que nos da una cota sobre la escritura de los S–grados de los sistemas minimales de generadores de las primeras sicigias de $k[S]$.

Teorema V–B.3 ■ Sea $m \in S$ un *grado* de un elemento minimal de un sistema homogéneo de generadores del primer módulo de sicigias de $k[S]$. Entonces $\exists \beta \in \mathbb{N}^r$ tal que $m = \mathcal{A}\beta$ y $||\beta||_1$ es a lo más

$$(1 + 2max_{i=1,\dots,s}\{|a_i|\} + D)^{(h+s)(r-1)} + 2r - 1.$$

En cualquier caso, este grado es simplemente exponencial en el número de variables.

Apliquemos estos resultados a acotar la regularidad de una variedad tórica.

V–C. REGULARIDAD DE UNA VARIEDAD TÓRICA PROYECTIVA

Vamos a suponer que I es un ideal homogéneo para la graduación natural. Esto es equivalente a que exista un vector $w \in \mathbb{Q}^h$ tal que $n_i \cdot w = 1$, $\forall i = 1, \ldots, r$ ([STU91, lema 4.14]). Geométricamente, I define una variedad proyectiva en $\mathbb{P}^{r-1}(k)$. Nótese que si $f \in I$ es S-homogéneo de grado $m \in S$, se tiene que $grado(f) = ||\alpha||_1$, para $\alpha \in \mathbb{N}^r$ con $\mathcal{A}\alpha = m$. En este caso el semigrupo S es libre de torsión.

Supongamos que $\{f_1, \ldots, f_b\}$ es un sistema minimal de generadores de I, con $S - grado(f_i) = p_i \in S$ y $grado(f_i) = ||\alpha_i||_1$, donde $p_i = \mathcal{A}\alpha_i$, $1 \leq i \leq b$. Si $g = (g_1, \ldots, g_b) \in N_1$ es una primera sicigia de S–grado $m \in S$, entonces $S - grado(g_i) = m - p_i$ y $grado(g_i) = ||\beta_i||_1$ donde $\mathcal{A}\beta_i = m - p_i$. Además, $m = \mathcal{A}(\alpha_i + \beta_i)$ y $grado(g) = ||\alpha_i + \beta_i||_1$.

En general, si $h = (h_1, \ldots, h_{b_i}) \in N_i$ es una i–sicigia de S–grado $m \in S$, se tiene que $grado(h) = ||\alpha||_1$, para $\alpha \in \mathbb{N}^r$ tal que $m = \mathcal{A}\alpha$.

Así obtenemos una cota para la regularidad de Castelnuovo-Mumford de I.

Teorema V–C.1 ■ Con las notaciones anteriores,

$$reg(I) \leq (1 + 4||\mathcal{A}||_1)^{h(d-1)} + (r + 1)(d - 1)$$

donde $d = \binom{r}{\lfloor r/2 \rfloor}$.

Demostración. La regularidad de I es $reg(I) = max_{1 \leq i \leq r}\{t_i - i\}$, donde t_i es el máximo grado de las i–sicigias de I (ver [BS87]).

Por el teorema V–B.2,

$$t_i \leq (1 + 4||\mathcal{A}||_1)^{h(d_i-1)} + (i + 1)d_i - 1,$$

con $d_i = \begin{pmatrix} r \\ i+1 \end{pmatrix}$. Es fácil ver que $d_i \leq d$, para cualquier i. Entonces

$$t_i - i \leq (1 + 4||\mathcal{A}||_1)^{h(d-1)} + (r+1)(d-1).$$

Ahora es suficiente considerar el máximo de estas diferencias. ■

Para concluir, veamos que no es necesario calcular la resolución minimal de I para dar de manera efectiva su regularidad.

Algoritmo V–C.2 ■ Cálculo de la Regularidad

Entrada: Un conjunto de generadores $\{n_1, \ldots, n_r\}$ de S (todos ellos en un hiperplano racional).

Salida: La regularidad del ideal I de S.

1. Para cualquier i, $1 \leq i \leq r$
   - Calcular C_i' (teorema V–A.8).
   - Chequear los elementos $m \in C_i'$ tales que $\tilde{H}_i(\Delta_m) \neq 0$ y obtener C_i.
   - Calcular $t_i = \{||\alpha||_1 \mid m = \mathcal{A}\alpha \in C_i\}$.
2. $reg(I) = \text{máx}\{t_i - i \mid i = 1, \ldots, r\}$.

CAPÍTULO VI

Ejemplos

En este capítulo vamos a desarrollar una serie de ejemplos para aclarar el funcionamiento de algunos algoritmos dados en la memoria. La gran mayoría de los ejemplos han sido construidos a partir del software implementado por nosotros mismos en MapleV3. Por ello, damos unas pequeñas notas de cómo realizar parte del cálculo mediante dicho software.

VI–A. IDEAL DE SEMIGRUPO

Como ejemplo ilustrativo de cálculo del ideal de un semigrupo con torsión, vamos a aplicar el algoritmo I–D.2 al siguiente semigrupo:

$$S =< (2,0,1,\bar{0}), (0,1,0,\bar{1}), (1,0,0,\bar{2}), (0,1,3,\bar{0}), (3,0,0,\bar{1}), (1,1,1,\bar{1}) >\subset \mathbb{Z}^3 \oplus \mathbb{Z}/3\mathbb{Z},$$

obteniendo un sistema de generadores minimal del ideal de S en $k[x_1,x_2,x_3,x_4,x_5,x_6]$.

Para ello construimos en primer lugar el semigrupo de $\mathbb{Z}^4$:

$$S' =< (2,0,1,0), (0,1,0,1), (1,0,0,2), (0,1,3,0), (3,0,0,1), (1,1,1,1), (0,0,0,3) > .$$

Sea C' un conjunto de generadores del retículo $\ker(S')$, es decir, el núcleo entero de la matriz

$$\begin{pmatrix} 2 & 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 3 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 & 1 & 3 \end{pmatrix}.$$

$$C' = \{(1, 1, 2, 0, -1, -1, -1), (0, 2, 0, 1, 1, -3, 0), (3, 1, -3, -1, -1, 0, 2)\}.$$

Un sistema de generadores del retículo $\ker(S)$, C, lo obtenemos proyectando C' sobre sus seis primeras coordenadas:

$$C = \{(1, 1, 2, 0, -1, -1), (0, 2, 0, 1, 1, -3), (3, 1, -3, -1, -1, 0)\}$$

Ahora tenemos que calcular el ideal de $\ker(S)$ para obtener el ideal de S. Este paso lo vamos a realizar usando el algoritmo I–C.12.

Partimos del sistema de generadores, C, del retículo $\ker(S)$. Un sistema de generadores ortogonal (ver I–C.10) de este retículo viene dado por las filas de la matriz

$$\begin{pmatrix} 1 & 1 & 2 & 0 & -1 & -1 \\ 2 & 4 & 4 & 1 & -1 & -5 \\ 11 & 17 & 13 & 3 & -5 & -20 \end{pmatrix}$$

Con la notación de I–C.12, tenemos que: $A = \{5, 6\}$ y

$$C_A = \{(1, 1, 2, 0, 1, 1), (2, 4, 4, 1, 1, 5), (11, 17, 13, 3, 5, 20)\}.$$

El sistema de generadores de J_{C_A} es

$$G_A = \left[x_1\, x_2\, x_3^{\,2}\, x_5\, x_6 - 1, x_1^{\,2}\, x_2^{\,4}\, x_3^{\,4}\, x_4\, x_5\, x_6^{\,5} - 1, x_1^{\,11}\, x_2^{\,17}\, x_3^{\,13}\, x_4^{\,3}\, x_5^{\,5}\, x_6^{\,20} - 1\right]$$

Tomamos $a = 5 \in A$ y consideramos la base de Gröbner reducida de J_{C_A} respecto del orden lexicográfico inducido por $x_5 > x_1 > x_2 > x_3 > x_4 > x_6$:

$$\left[x_5 - x_2^{\,2}\, x_4\, x_6^{\,3}, x_1 - x_4^{\,2}\, x_6^{\,5}\, x_3^{\,7}\, x_2^{\,3}, -1 + x_4^{\,3}\, x_6^{\,9}\, x_3^{\,9}\, x_2^{\,6}\right]$$

Por lo tanto, $G_{\{6\}}$ es el resultado de aplicar $T_{\{5\}}$ al conjunto anterior,

$$G_{\{6\}} = \left[-x_2^{\,2}\, x_4\, x_6^{\,3}\, x_5 + 1, x_1 - x_4^{\,2}\, x_6^{\,5}\, x_3^{\,7}\, x_2^{\,3}, -1 + x_4^{\,3}\, x_6^{\,9}\, x_3^{\,9}\, x_2^{\,6}\right]$$

y $A = A \setminus \{5\} = \{6\}$.

Una base de Gröbner de J_{C_A} respecto del orden lexicográfico inducido por $x_6 > x_1 > x_2 > x_3 > x_4 > x_5$ es:

$$\left[x_2^2\, x_4\, x_6^3\, x_5 - 1, -x_3^5 + x_6^2\, x_2^2\, x_5\, x_1^2, -x_1\, x_3^2 + x_6^2\, x_2\, x_4\, x_5^2, -x_5 + x_1\, x_2\, x_3^2\, x_6, x_1\, x_2\, x_6\, x_5^2 - x_3^7, -x_1^2 + x_6\, x_3^5\, x_4, x_6\, x_4\, x_5^3 - x_1^2\, x_3^4, -x_3^3\, x_4\, x_5 + x_1^3\, x_2, -x_5^3 + x_3^9\right]$$

Por lo tanto, el conjunto $G_{\emptyset}$ igual a

$$\left[-x_6^3 + x_2^2\, x_4\, x_5, -x_6^2\, x_3^5 + x_2^2\, x_5\, x_1^2, -x_1\, x_3^2\, x_6^2 + x_2\, x_4\, x_5^2, -x_6\, x_5 + x_1\, x_2\, x_3^2, -x_3^7\, x_6 + x_1\, x_2\, x_5^2, -x_1^2\, x_6 + x_3^5\, x_4, -x_1^2\, x_3^4\, x_6 + x_4\, x_5^3, -x_3^3\, x_4\, x_5 + x_1^3\, x_2, -x_5^3 + x_3^9\right],$$

es un sistema de generadores de $I_{\ker(S)}$. Tenemos así un sistema de generadores del ideal de S.

Nótese que S es Nakayama, ya que en el conjunto anterior no hay ningún binomio de S–grado cero (I–B.4). Así podemos considerar el siguiente sistema irreducible de generadores del ideal de S con la seguridad de que es minimal, i.e. de cardinal mínimo,

$$\left[-x_3^3\, x_4\, x_5 + x_1^3\, x_2, -x_6^2\, x_3^5 + x_2^2\, x_5\, x_1^2, x_1^2\, x_6 - x_3^5\, x_4, -x_6\, x_5 + x_1\, x_2\, x_3^2, -x_3^7\, x_6 + x_1\, x_2\, x_5^2, x_1\, x_3^2\, x_6^2 - x_2\, x_4\, x_5^2, -x_6^3 + x_2^2\, x_4\, x_5, -x_5^3 + x_3^9\right]$$

Si queremos realizar este cálculo usando el software desarrollado por nosotros, debemos realizar en MapleV3 los siguientes pasos:

```
>read totsemig:
>S:=[[2,0,1,0],[0,1,0,1],[1,0,0,2],[0,1,3,0],[3,0,0,1],[1,1,1,1],[3]]:
>totsemig(S);
```

Ideal de Semigrupo, $\left[-x_6^3 + x_2^2\, x_4\, x_5, -x_6^2\, x_3^5 + x_2^2\, x_5\, x_1^2, -x_1\, x_3^2\, x_6^2 + x_2\, x_4\, x_5^2, -x_6\, x_5 + x_1\, x_2\, x_3^2, -x_3^7\, x_6 + x_1\, x_2\, x_5^2, -x_1^2\, x_6 + x_3^5\, x_4, -x_1^2\, x_3^4\, x_6 + x_4\, x_5^3, -x_3^3\, x_4\, x_5 + x_1^3\, x_2, -x_5^3 + x_3^9\right]$

$$\textit{Base de Grobner del Ideal,}\Big[-x_3{}^3\,x_4\,x_5+x_1{}^3\,x_2, -x_6{}^2\,x_3{}^5+x_2{}^2\,x_5\,x_1{}^2, x_1{}^2\,x_6-x_3{}^5\,x_4,\\ -x_6\,x_5+x_1\,x_2\,x_3{}^2, -x_3{}^7\,x_6+x_1\,x_2\,x_5{}^2, x_1\,x_3{}^2\,x_6{}^2-x_2\,x_4\,x_5{}^2,\\ -x_2\,x_3{}^7\,x_4+x_1\,x_6{}^2\,x_5, x_1\,x_6{}^5-x_2{}^3\,x_4{}^2\,x_3{}^7, -x_6{}^3+x_2{}^2\,x_4\,x_5, -x_5{}^3+x_3{}^9\Big]$$

$$\Big[-x_3{}^3\,x_4\,x_5+x_1{}^3\,x_2, -x_6{}^2\,x_3{}^5+x_2{}^2\,x_5\,x_1{}^2, x_1{}^2\,x_6-x_3{}^5\,x_4, -x_6\,x_5+x_1\,x_2\,x_3{}^2,\\ -x_3{}^7\,x_6+x_1\,x_2\,x_5{}^2, x_1\,x_3{}^2\,x_6{}^2-x_2\,x_4\,x_5{}^2, -x_6{}^3+x_2{}^2\,x_4\,x_5, -x_5{}^3+x_3{}^9\Big]$$

La salida final es un sistema minimal de generadores del ideal de S en $k[x_1, x_2, x_3, x_4, x_5, x_6]$.

VI–B. SISTEMAS DIOFÁNTICOS

Veamos ejemplos de algunos algoritmos del capítulo II.

■ $\mathbb{N}$–solución Particular

El siguiente ejemplo nos ilustra el algoritmo II–D.5. Para ello consideremos el sistema diofántico no homogéneo en congruencias:

$$(Sist) \equiv \left\{\begin{array}{ccccccccl} 4x_1 & -x_2 & & +7x_4 & -2x_5 & +3x_6 & = & 3 & \\ x_1 & -2x_2 & & -x_4 & -x_5 & & = & 4 & \text{mód}\,5 \\ 4x_1 & -7x_2 & -3x_3 & & +x_5 & & = & -2 & \text{mód}\,2 \\ 5x_1 & & +2x_3 & +2x_4 & +x_5 & +x_6 & = & 2 & \text{mód}\,3 \end{array}\right.$$

Para calcular una $\mathbb{N}$–solución particular (caso de existir) del sistema $(Sist)$, construimos en primer lugar el semigrupo, $S \subset \mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, formado por las columnas el sistema:

$$< (4, \bar{1}, \bar{4}, \bar{5}), (-1, -\bar{2}, -\bar{7}, \bar{0}), (0, \bar{0}, -\bar{3}, \bar{2}), (7, -\bar{1}, \bar{0}, \bar{2}), (-2, \bar{1}, \bar{1}, \bar{1}), (3, \bar{0}, \bar{0}, \bar{1}), (3, \bar{4}, -\bar{2}, \bar{2}) >$$

El paso siguiente es computar el ideal de dicho semigrupo (usaremos I–D.2), obteniendo un conjunto, C, igual a:

$$\Big[x_1-x_6{}^4\,x_5{}^4, x_2-x_6\,x_7{}^6\,x_5{}^{11}, -x_5{}^{15}\,x_7{}^{10}+x_3, x_4-x_7{}^2\,x_5{}^4\,x_6{}^3, x_5{}^{18}\,x_7{}^{12}-1,\\ x_7{}^{14}\,x_5{}^6-x_6{}^{10}, -x_7{}^{15}+x_6{}^{15}\Big]$$

Como el semigrupo es no Nakayama, $x_7^{12}-1 \in C$, tenemos que calcular un base de Gröbner del ideal respecto de un orden donde x_7 es la variable con mayor peso. En este caso vamos a considerar en orden lexicográfico inducido por $x_7 > x_1 > x_2 > x_3 > x_4 > x_5 > x_6$:

$$\left[x_7 - x_5{}^6\, x_6{}^5, x_1 - x_6{}^4\, x_5{}^4, x_2 - x_6{}^{31}\, x_5{}^{47}, x_3 - x_6{}^{50}\, x_5{}^{75}, x_4 - x_5{}^{16}\, x_6{}^{13}, x_6{}^{60}\, x_5{}^{90} - 1\right]$$

Una $\mathbb{N}$–solución particular de sistema nos la da el binomio $x_7 - x_5^6 x_6^5$, i.e. [0, 0, 0, 0, 6, 5].

Si se quieren utilizar las rutinas implementadas por nosotros en MapleV3, debe tenerse en cuenta que en la implementación de este algoritmo se ha considerado no el semigrupo $< n_1, \ldots, n_r, b >$, sino el semigrupo $< b, n_1, \ldots, n_r >$. Por ello aparecen resultados distintos a los que hemos obtenido con anterioridad. En conclusión, deberíamos hacer lo siguiente:

```
>read solsyst:
>S:=[[3,4,-2,2],[4,1,4,5],[-1,-2,-7,0],[0,0,-3,2],
>[7,-1,0,2],[-2,-1,1,1],[3,0,0,1],[5,2,3],[1]]:
>solveN(S);
```

$$\mathit{Ideal\ de\ Semigrupo}, \left[- x_7{}^{10}\, x_6{}^{15}\, x_4 + 1, -x_6{}^6\, x_7{}^5 + x_1, -x_6{}^4\, x_7{}^4 + x_2, x_3 - x_7{}^{31}\, x_6{}^{47}, -x_6{}^{16}\, x_7{}^{13} + x_5, -1 + x_6{}^{90}\, x_7{}^{60}\right]$$

$$\mathit{NO\ NAKAYAMA}\ !!, -x_7{}^{10}\, x_6{}^{15}\, x_4 + 1$$

$$-x_6{}^6\, x_7{}^5 + x_1$$

En este caso, una $\mathbb{N}$–solución es: [0, 0, 0, 0, 6, 5].

■ $\mathbb{N}$–solución General

Veamos un ejemplo ilustrativo del algoritmo II–D.6. Para ello consideremos el siguiente sistema de ecuaciones diofánticas homogéneas en congruencias:

$$\left\{\begin{array}{lllll} -x_1 & & +3x_3 & -3x_4 & = 0 \\ -2x_1 & & -x_3 & & = 0 \quad \text{mód}\, 3 \\ & +2x_2 & +2x_3 & +x_4 & = 0 \quad \text{mód}\, 3 \end{array}\right.$$

Denotaremos por $\mathcal{G}$ al conjunto de $\mathbb{N}$–soluciones del sistema anterior, y por $\mathcal{G}(i, \alpha)$ al conjunto

$$\{x \in \mathcal{G} \subset \mathbb{N}^4 | x_i = \alpha\}.$$

Con esta idea definimos recurrentemente $\mathcal{G}(i_1, \alpha_1) \cdot \cdot \cdot (i_j, \alpha_j)$.

Por el lema II–B.5, para calcular un sistema minimal de generadores de nuestro sistema, es suficiente, dada una $\mathbb{N}$–solución particular, construir el conjunto

$$F = \{s\} \cup \bigcup_{i=1}^{r} \bigcup_{\alpha=0}^{s_i-1} \mathcal{HG}(i, \alpha),$$

y a partir de él tendríamos que $\mathcal{HG} = \mathcal{HF}$.

El primer paso es calcular una $\mathbb{N}$–solución particular, s, del sistema. Este paso lo realizamos mediante el algoritmo II–D.5 y obtenemos la upla $s = (0, 3, 0, 0)$.

Por lo tanto, tenemos que calcular el conjunto

$$\begin{aligned} F &= \{(0, 3, 0, 0)\} \cup \textstyle\bigcup_{i=1}^{4} \bigcup_{\alpha=0}^{s_i-1} \mathcal{HG}(i, \alpha) \\ &= \{(0, 3, 0, 0)\} \cup \mathcal{HG}(2, 0) \cup \mathcal{HG}(2, 1) \cup \mathcal{HG}(2, 2), \end{aligned}$$

usando el propio algoritmo II–D.6 recurrentemente para obtener los conjuntos $\mathcal{HG}(2, \alpha)$.

Calculemos $\mathcal{HG}(2, 0)$. Para ello tenemos que considerar el sistema inicial haciendo $x_2 = 0$,

$$\left\{ \begin{array}{lllll} -x_1 & +3x_3 & -3x_4 & = 0 & \\ -2x_1 & -x_3 & & = 0 & \text{mód}\,3 \\ & +2x_3 & +x_4 & = 0 & \text{mód}\,3 \end{array} \right.$$

De nuevo tenemos que calcular, a partir de una $\mathbb{N}$–solución particular s' del anterior sistema, un conjunto

$$F' = \{s'\} \cup \bigcup_{i=1}^{4} \bigcup_{\alpha=0}^{s'_i-1} \mathcal{HG}(2, 0)(i, \alpha).$$

Una tal s' es $(0,0,3,3)$, luego

$$\begin{aligned} F' &= \{s'\}\cup \textstyle\bigcup_{i=1}^{4}\bigcup_{\alpha=0}^{s'_i-1}\mathcal{HG}(2,0)(i,\alpha)\\ &= \{(0,0,3,3)\}\cup \mathcal{HG}(2,0)(3,0)\cup \mathcal{HG}(2,0)(3,1)\cup \mathcal{HG}(2,0)(3,2)\cup\\ &\quad \cup\mathcal{HG}(2,0)(4,0)\cup \mathcal{HG}(2,0)(4,1)\cup \mathcal{HG}(2,0)(4,2). \end{aligned}$$

$\mathcal{HG}(2,0)(3,0)$ es $\{0,0,0,0)\}$ ya que el sistema

$$\begin{cases} -x_1 \quad -3x_4 &= 0\\ -2x_1 &= 0 \quad \text{mód}\, 3\\ \qquad\quad +x_4 &= 0 \quad \text{mód}\, 3 \end{cases}$$

no posee más $\mathbb{N}$–solución que la trivial.

Análogamente, $\mathcal{HG}(2,0)(3,1)=\varnothing$, ya que el sistema

$$\begin{cases} -x_1 \quad -3x_4 &= -3\\ -2x_1 &= 1 \quad \text{mód}\, 3\\ \qquad\quad +x_4 &= -2 \quad \text{mód}\, 3 \end{cases}$$

no posee ninguna $\mathbb{N}$–solución particular. Mediante el mismo razonamiento tenemos que $\mathcal{HG}(2,0)(3,2)=\varnothing$.

En cambio, el conjunto $\mathcal{HG}(2,0)(4,0)$ es no vacío ya que el sistema asociado a él (homogéneo en este caso)

$$\begin{cases} -x_1 \quad 3x_3 &= 0\\ -2x_1 \quad -x_3 &= 0 \quad \text{mód}\, 3\\ \qquad\quad +2x_2 &= 0 \quad \text{mód}\, 3 \end{cases}$$

tiene, por ejemplo, como $\mathbb{N}$–solución particular $s''=(9,0,3,0)$. De nuevo tenemos que calcular $\mathcal{HG}(2,0)(4,0)$ mediante un conjunto auxiliar

$$F''=\{s''\}\cup\bigcup_{i=1}^{4}\bigcup_{\alpha=0}^{s''_i-1}\mathcal{HG}(2,0)(4,0)(i,\alpha).$$

Para el conjunto $\mathcal{HG}(2,0)(4,0)(1,0)$, tenemos que encontrar una $\mathbb{N}$–solución particular del sistema

$$\begin{cases} 3x_3 &= 0\\ -x_3 &= 0 \quad \text{mód}\, 3\\ +2x_3 &= 0 \quad \text{mód}\, 3 \end{cases}$$

Cuadro VI.1. $\mathcal{HG}(2,0)$

$\mathcal{HG}(2,0)$ $(0,0,3,3)$	$\mathcal{HG}(2,0)(3,0)=\{(0,0,0,0)\}$ $\mathcal{HG}(2,0)(3,1)=\varnothing$ $\mathcal{HG}(2,0)(3,2)=\varnothing$ $\mathcal{HG}(2,0)(4,0)=\{(9,0,3,0)\}$ $\mathcal{HG}(2,0)(4,1)=\varnothing$ $\mathcal{HG}(2,0)(4,2)=\varnothing$	$\mathcal{HG}(2,0)(4,0)(1,0)=\{0,0,0,0\}$ $\mathcal{HG}(2,0)(4,0)(1,1)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,2)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,3)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,4)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,5)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,6)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,7)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,8)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,0)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,1)=\varnothing$ $\mathcal{HG}(2,0)(4,0)(1,2)=\varnothing$

Al encontrarnos con un sistema de ecuaciones con una sola incógnita, es trivial ver si tiene o no alguna $\mathbb{N}$–solución. En este caso la única es la trivial $\mathcal{HG}(2,0)(4,0)(1,0)=\{0,0,0,0\}$.

Nótese que hemos ido, mediante nuestra recurrencia, reduciendo el número de incógnitas del sistema hasta llegar a uno de resolución inmediata (con una sola incógnita). Además, al llegar a una sola incógnita también es trivial el calcular el conjunto de las $\mathbb{N}$–soluciones minimales.

Continuando con este proceso para $\mathcal{HG}(2,0)$, y para el resto de los conjuntos, $\mathcal{HG}(2,1)$ y $\mathcal{HG}(2,2)$, obtenemos las tablas VI.1, VI.2 y VI.3.

Por lo tanto, tenemos que
$$\boxed{\begin{array}{rcc} \mathcal{HG}(2,0) & = & \{(0,0,3,3),(9,0,3,0)\} \\ \mathcal{HG}(2,1) & = & \{(6,1,3,1)\} \\ \mathcal{HG}(2,0) & = & \{(0,0,3,3),(9,0,0,3)\} \\ \mathcal{HG}(2,2) & = & \{(3,2,3,2)\} \end{array}}$$

El conjunto dado por las uniones de los anteriores y s es

$$F=\{(0,3,0,0),(9,0,3,0),(6,1,3,1),(0,0,3,3),(9,0,0,3),(3,2,3,2)\}.$$

Sus elementos minimales coinciden, en este caso, con el propio F, $\mathcal{H}F=$

Cuadro VI.2. $\mathcal{HG}(2,1)$

$\mathcal{HG}(2,1)$ (6, 1, 3, 1)	$\mathcal{HG}(2,1)(1,0) = \varnothing$
	$\mathcal{HG}(2,1)(1,1) = \varnothing$
	$\mathcal{HG}(2,1)(1,2) = \varnothing$
	$\mathcal{HG}(2,1)(1,3) = \varnothing$
	$\mathcal{HG}(2,1)(1,4) = \varnothing$
	$\mathcal{HG}(2,1)(1,5) = \varnothing$
	$\mathcal{HG}(2,1)(3,0) = \varnothing$
	$\mathcal{HG}(2,1)(3,1) = \varnothing$
	$\mathcal{HG}(2,1)(3,2) = \varnothing$
	$\mathcal{HG}(2,1)(4,0) = \varnothing$

Cuadro VI.3. $\mathcal{HG}(2,2)$

$\mathcal{HG}(2,2)$ (3, 2, 3, 2)	$\mathcal{HG}(2,2)(1,0) = \varnothing$
	$\mathcal{HG}(2,2)(1,1) = \varnothing$
	$\mathcal{HG}(2,2)(1,2) = \varnothing$
	$\mathcal{HG}(2,2)(3,0) = \varnothing$
	$\mathcal{HG}(2,2)(3,1) = \varnothing$
	$\mathcal{HG}(2,2)(3,2) = \varnothing$
	$\mathcal{HG}(2,2)(4,0) = \varnothing$
	$\mathcal{HG}(2,2)(4,1) = \varnothing$

F.

Por lo tanto deducimos que el conjunto minimal de generadores de las $\mathbb{N}$–soluciones (base de Hilbert) de nuestro sistema diofántico homogéneo de partida es

$$\mathcal{HG} = \mathcal{HF} = \{(0,3,0,0),(9,0,3,0),(6,1,3,1),(0,0,3,3),(9,0,0,3),(3,2,3,2)\}.$$

VI–C. RESOLUCIÓN LIBRE MINIMAL

Vamos a aplicar el algoritmo IV–A.8 al siguiente semigrupo

$$S =< (1,0,0),(0,1,0),(0,0,1),(4,2,-5),(3,-3,1) >\subset \mathbb{Z}^3.$$

Este semigrupo corresponde a una superficie proyectiva simplicial (ver [BCMP98a]). Denotaremos $\Lambda = \{1,2,3,4,5\}$.

El primer paso de nuestro algoritmo consiste en determinar el conjunto $\mathcal{F} = \{F \subset \mathcal{P}(\Lambda) |\ \sharp F \geq 3\}$. En nuestro caso, este conjunto es

$$\begin{array}{rcl}\mathcal{F} & = & \{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,5\},\{1,4,5\},\\ & & \{2,3,4\},\{2,3,5\},\{2,4,5\},\{3,4,5\},\{1,2,3,4\},\{1,2,3,5\},\\ & & \{1,2,4,5\},\{2,3,4,5\},\{1,3,4,5\},\{1,2,3,4,5\}\}\end{array}$$

En general estos conjuntos se pueden tomar considerando los conjuntos formados por las combinaciones sin repetición de elementos de Λ tomados en grupos de 3 en 3, 4 en 4, etc, hasta $\sharp\Lambda$.

Comencemos con el primero de los elementos de $\mathcal{F}$. Sea $F = \{1,2,3\} \in \mathcal{F}$, En este caso, sólo es posible un único polígono sobre F, $\sigma = (1\ 2\ 3)$, con $F_1 = \{1,2\}$, $F_2 = \{2,3\}$ y $F_3 = \{3,1\}$.

Fijado este polígono, el siguiente paso consiste en computar el conjunto de $\mathbb{N}$–soluciones, $\mathcal{HR}_{(1\ 2\ 3)}$, el cual es el conjunto de $\mathbb{N}$–soluciones minimales del sistema diofántico

$$\underbrace{\begin{pmatrix} \mathcal{A}_{F_1} & -\mathcal{A}_{F_2} & 0 \\ 0 & \mathcal{A}_{F_2} & -\mathcal{A}_{F_3} \end{pmatrix}}_{\mathcal{A}_{(1\ 2\ 3)}} \alpha = 0,$$

igual a

$$\begin{pmatrix} 1 & 0 & 4 & 3 & 0 & 0 & -4 & -3 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & -3 & -1 & 0 & -2 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & -5 & 1 & 0 & -1 & 5 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 3 & -1 & 0 & -4 & -3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & -3 & 0 & 0 & -2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & -4 & 1 & 0 & -1 & 5 & -1 \end{pmatrix} \alpha = 0,$$

tales que $\alpha \gg e_{(1\ 2\ 3)}$, con $e_{(1\ 2\ 3)} = [1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0]$ como se definió en el capítulo IV. Por la nota II–A.4, para obtener dicho conjunto, debemos computar las $\mathbb{N}$–soluciones minimales, $\mathcal{HR}_{\sigma e_\tau}$, de:

$$\underbrace{\begin{pmatrix} 1 & 0 & 4 & 3 & 0 & 0 & -4 & -3 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & -3 & -1 & 0 & -2 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & -5 & 1 & 0 & -1 & 5 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 3 & -1 & 0 & -4 & -3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & -3 & 0 & 0 & -2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & -4 & 1 & 0 & -1 & 5 & -1 \end{pmatrix}}_{\mathcal{A}_{(1\ 2\ 3)}} \alpha = \underbrace{\begin{pmatrix} -1 \\ 0 \\ 1 \\ 1 \\ -1 \\ 0 \end{pmatrix}}_{-\mathcal{A}_{(1\ 2\ 3)} e_{(1\ 2\ 3)}}$$

Este conjunto es

{[0, 5, 0, 2, 0, 5, 1, 1, 6, 1, 0, 0], [0, 7, 0, 2, 2, 5, 1, 1, 2, 6, 1, 0], [0, 17, 0, 4, 12, 5, 1, 3, 0, 18, 3, 0],
[0, 12, 0, 3, 7, 5, 1, 2, 1, 12, 2, 0], [0, 15, 1, 6, 10, 5, 2, 5, 22, 0, 0, 0], [0, 28, 2, 11, 5, 24, 6, 6, 41, 0, 0, 0],
[0, 41, 3, 16, 0, 43, 10, 7, 60, 0, 0, 0], [1, 28, 2, 11, 0, 30, 7, 5, 42, 0, 0, 0], [1, 15, 1, 6, 5, 11, 3, 4, 23, 0, 0, 0],
[2, 15, 1, 6, 0, 17, 4, 3, 24, 0, 0, 0], [3, 2, 0, 1, 0, 4, 1, 1, 6, 0, 0, 0], [3, 4, 0, 1, 2, 4, 1, 1, 2, 5, 1, 0],
[3, 14, 0, 3, 12, 4, 1, 3, 0, 17, 3, 0], [3, 9, 0, 2, 7, 4, 1, 2, 1, 11, 2, 0], [281, 0, 0, 0, 192, 0, 15, 74, 0, 203, 47, 31],
[15, 0, 0, 0, 10, 0, 1, 4, 4, 8, 2, 1], [12, 0, 0, 0, 7, 1, 1, 3, 1, 8, 2, 1], [47, 0, 0, 0, 30, 2, 3, 12, 0, 34, 8, 5],
[29, 0, 0, 0, 12, 8, 3, 6, 0, 21, 5, 3], [17, 0, 0, 0, 0, 12, 3, 2, 6, 8, 2, 1], [13, 0, 0, 0, 2, 7, 2, 2, 2, 8, 2, 1],
[16, 0, 0, 0, 5, 6, 2, 3, 5, 8, 2, 1], [148, 1, 0, 0, 102, 0, 8, 39, 0, 108, 25, 16], [15, 1, 0, 0, 11, 0, 1, 4, 11, 4, 1, 0],
[12, 1, 0, 0, 8, 1, 1, 3, 8, 4, 1, 0], [9, 1, 0, 0, 5, 2, 1, 2, 5, 4, 1, 0], [6, 1, 0, 0, 2, 3, 1, 1, 2, 4, 1, 0],
[22, 1, 0, 0, 12, 4, 2, 5, 0, 17, 4, 2], [10, 1, 0, 0, 0, 8, 2, 1, 6, 4, 1, 0], [15, 2, 0, 0, 12, 0, 1, 4, 0, 13, 3, 1],
[72, 35, 0, 0, 84, 0, 4, 19, 0, 89, 18, 0], [53, 25, 0, 0, 61, 0, 3, 14, 1, 64, 13, 0],
[34, 15, 0, 0, 38, 0, 2, 9, 2, 39, 8, 0], [15, 5, 0, 0, 15, 0, 1, 4, 3, 14, 3, 0], [15, 3, 0, 0, 13, 0, 1, 4, 7, 9, 2, 0],
[15, 2, 0, 1, 12, 0, 1, 5, 18, 0, 0, 0], [53, 30, 0, 1, 66, 0, 3, 15, 0, 70, 14, 0], [15, 20, 0, 3, 30, 0, 1, 7, 0, 32, 6, 0],
[34, 25, 0, 2, 48, 0, 2, 11, 0, 51, 10, 0], [34, 20, 0, 1, 43, 0, 2, 10, 1, 45, 9, 0], [15, 15, 0, 2, 25, 0, 1, 6, 1, 26, 5, 0],
[15, 10, 0, 1, 20, 0, 1, 5, 2, 20, 4, 0], [12, 5, 0, 0, 12, 1, 1, 3, 0, 14, 3, 0], [12, 3, 0, 0, 10, 1, 1, 3, 4, 9, 2, 0],
[12, 2, 0, 1, 9, 1, 1, 4, 15, 0, 0, 0], [9, 8, 0, 1, 12, 2, 1, 3, 0, 15, 3, 0], [9, 3, 0, 0, 7, 2, 1, 2, 1, 9, 2, 0],
[9, 2, 0, 1, 6, 2, 1, 3, 12, 0, 0, 0], [6, 11, 0, 2, 12, 3, 1, 3, 0, 16, 3, 0], [6, 2, 0, 1, 3, 3, 1, 2, 9, 0, 0, 0],
[6, 6, 0, 1, 7, 3, 1, 2, 1, 10, 2, 0]}

Ahora, aplicando una vez más el resultado II–A.4, debemos añadir $e_{(1\ 2\ 3)}$ a cada elemento del anterior conjunto para obtener $\mathcal{HR}_{(1\ 2\ 3)}$, y de ahí $\Sigma\mathcal{HR}_{(1\ 2\ 3)}$:

$$\begin{aligned}\Sigma R_{(1\ 2\ 3)} = < & [7,0,2],[7,2,2],[13,6,4],[10,4,3],[19,-2,7],[34,-4,13],[49,-6,19],\\ & [35,-4,13],[20,-2,7],[21,-2,7],[7,0,1],[7,2,1],[13,6,3],\\ & [10,4,2],[282,1,0],[16,1,0],[13,1,0],[48,1,0],[30,1,0],\\ & [18,1,0],[14,1,0],[17,1,0],[149,2,0],[16,2,0],[13,2,0],\\ & [10,2,0],[7,2,0],[23,2,0],[11,2,0],[16,3,0],[73,36,0],\\ & [54,26,0],[35,16,0],[16,6,0],[16,4,0],[19,0,1],[57,28,1],\\ & [25,12,3],[41,20,2],[38,18,1],[22,10,2],[19,8,1],[13,6,0],\\ & [13,4,0],[16,0,1],[13,6,1],[10,4,0],[13,0,1],[13,6,2],\\ & [10,0,1],[10,4,1] >\end{aligned}$$

Los elementos S–minimales de $\Sigma R_{(1\ 2\ 3)}$ son

$$C_{(1\ 2\ 3)} = \{[13,1,0],[7,2,0],[7,0,1]\}.$$

Este conjunto lo hemos obtenido restando dos a dos los elementos de $\Sigma\mathcal{HR}_{(1\ 2\ 3)}$ y comprobando si su diferencia está o no en S.

Repitiendo este proceso con todos los polígonos asociados a los elementos de $\mathcal{F}$, obtenemos los resultados de la tabla VI.4

Sea ahora

$$\begin{aligned}G &= \bigcup C_\sigma\\ &= \{[13,1,0],[7,2,0],[7,0,1],[12,1,4],[23,0,1],[7,2,1],\\ &\quad [22,1,1],[15,3,1],[25,2,2],[72,0,5],[38,10,0],\\ &\quad [30,6,10],[28,14,3]\}.\end{aligned}$$

El paso siguiente es computar el conjunto

$$C = \{m_\sigma \in G \mid \sigma\ F-\text{hueco de } \Delta_{m_\sigma}\}.$$

Para ello vamos a considerar los diferentes complejos simpliciales asociados a los elementos de G dados en la tabla VI.5. El cálculo de dichos

Cuadro VI.4. Lista de C_σ

$\sharp F = 3$	$C_{(1\ 2\ 3)} = \{[13,1,0],[7,2,0],[7,0,1]\}$ $C_{(1\ 2\ 4)} = \{[13,1,0],[7,2,0]\}$ $C_{(1\ 2\ 5)} = \{[13,1,0],[12,1,4]\}$ $C_{(1\ 3\ 4)} = \{[23,0,1]\}$ $C_{(1\ 3\ 5)} = \{[7,0,1]\}$ $C_{(1\ 4\ 5)} = \{[7,2,1]\}$ $C_{(2\ 3\ 4)} = \{[22,1,1]\}$ $C_{(2\ 3\ 5)} = \{[12,1,4]\}$ $C_{(2\ 4\ 5)} = \{[15,3,1]\}$ $C_{(3\ 4\ 5)} = \{[25,2,2]\}$
$\sharp F = 4$	$C_{(1\ 2\ 3\ 4)} = \varnothing$ $C_{(1\ 2\ 4\ 3)} = \{[72,0,5]\}$ $C_{(1\ 3\ 2\ 4)} = \varnothing$ $C_{(1\ 2\ 3\ 5)} = \varnothing$ $C_{(1\ 2\ 5\ 3)} = \{[38,10,0]\}$ $C_{(1\ 3\ 2\ 5)} = \varnothing$ $C_{(1\ 2\ 4\ 5)} = \varnothing$ $C_{(1\ 2\ 5\ 4)} = \{[30,6,10]\}$ $C_{(1\ 4\ 2\ 5)} = \varnothing$ $C_{(2\ 3\ 4\ 5)} = \varnothing$ $C_{(2\ 3\ 5\ 4)} = \varnothing$ $C_{(2\ 4\ 3\ 5)} = \varnothing$ $C_{(1\ 3\ 4\ 5)} = \{[28,14,3]\}$ $C_{(1\ 3\ 5\ 4)} = \varnothing$ $C_{(1\ 4\ 3\ 5)} = \varnothing$
$\sharp F = 5$	$C_{(1\ 2\ 3\ 4\ 5)} = \varnothing$ $C_{(1\ 2\ 3\ 5\ 4)} = \varnothing$ $C_{(1\ 2\ 4\ 3\ 5)} = \varnothing$ $C_{(1\ 2\ 4\ 5\ 3)} = \varnothing$ $C_{(1\ 2\ 5\ 3\ 4)} = \varnothing$ $C_{(1\ 2\ 5\ 4\ 3)} = \varnothing$ $C_{(1\ 3\ 2\ 4\ 5)} = \varnothing$ $C_{(1\ 3\ 2\ 5\ 4)} = \varnothing$ $C_{(1\ 3\ 4\ 2\ 5)} = \varnothing$ $C_{(1\ 3\ 5\ 2\ 4)} = \varnothing$ $C_{(1\ 4\ 2\ 3\ 5)} = \varnothing$ $C_{(1\ 4\ 3\ 2\ 5)} = \varnothing$

complejos lo hemos realizado a través de los resultados dados en el capítulo II. Por ejemplo, para calcular $\Delta_{[7,0,1]}$, consideramos el sistema diofántico

$$(7,0,1)=\alpha_1(1,0,0)+\alpha_2(0,1,0)+\alpha_3(0,0,1)+\alpha_4(4,2,-5)+\alpha_5(3,-3,1)$$

cuyos coeficientes son los generadores de S, y calculamos el conjunto minimal de las $\mathbb{N}$–soluciones:

$$\{[7,0,1,0,0],[0,1,5,1,1],[4,3,0,0,1]\}.$$

Los soportes de estas $\mathbb{N}$–soluciones minimales son las caras maximales de $\Delta_{[7,0,1]}$. De hecho, estas $\mathbb{N}$–soluciones son las únicas escrituras de $[7,0,1]$ en función de los generadores de S.

Los elementos que cuyos polígonos corresponden realmente con F–huecos de sus complejos son:

$$\mathrm{C}=\{[7,2,0],\ [7,0,1],\ [7,2,1]\}.$$

Este es precisamente el conjunto que se obtiene al aplicar el algoritmo IV–A.8.

Para calcular ahora el conjunto C_1, tenemos que ver cuales de los elementos de C tienen homologías no nulas. Por lo tanto tenemos que calcular las homologías asociadas a sus complejos simpliciales.

Realicemos este cálculo para, por ejemplo, $[7,0,1]$. Entonces tenemos que considerar las aplicaciones

$$\tilde{C}_2(\Delta_{[7,0,1]})\xrightarrow{\partial_2}\tilde{C}_1(\Delta_{[7,0,1]})\xrightarrow{\partial_1}\tilde{C}_0(\Delta_{[7,0,1]}),$$

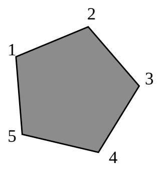
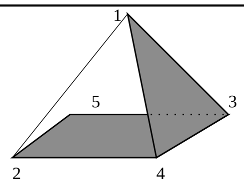
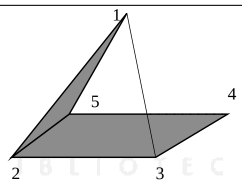
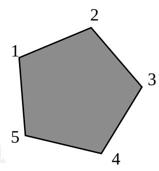
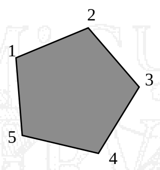
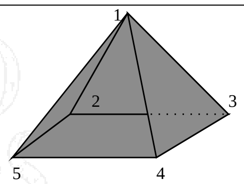
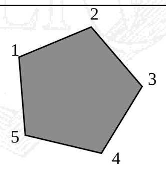
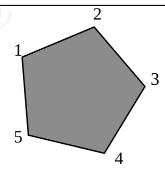
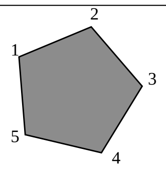
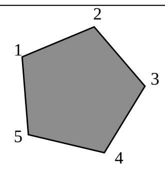
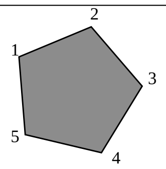
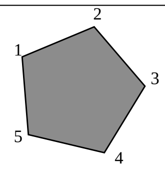
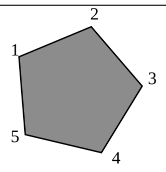
donde

$$\tilde{C}_2(\Delta_{[7,0,1]})=<\{1,5,2\},\{2,3,4\},\{2,3,5\},\{2,4,5\},\{3,4,5\}>,$$

$$\tilde{C}_1(\Delta_{[7,0,1]})=<\{1,2\},\{1,3\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}>\ \text{ y}$$

$$\tilde{C}_0(\Delta_{[7,0,1]})=<\{1\},\{2\},\{3\},\{4\},\{5\}>.$$

Cuadro VI.5. Lista de complejos

$\Delta_{[13,1,0]}$ $\longrightarrow$		$\Delta_{[7,2,0]}$ $\longrightarrow$	
$\Delta_{[7,0,1]}$ $\longrightarrow$		$\Delta_{[12,1,4]}$ $\longrightarrow$	
$\Delta_{[23,0,1]}$ $\longrightarrow$		$\Delta_{[7,2,1]}$ $\longrightarrow$	
$\Delta_{[22,1,1]}$ $\longrightarrow$		$\Delta_{[15,3,1]}$ $\longrightarrow$	
$\Delta_{[25,2,2]}$ $\longrightarrow$		$\Delta_{[72,0,15]}$ $\longrightarrow$	
$\Delta_{[38,10,0]}$ $\longrightarrow$		$\Delta_{[30,6,10]}$ $\longrightarrow$	
$\Delta_{[28,14,3]}$ $\longrightarrow$			

Sus matrices asociadas son

$$\partial_2 \equiv \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \text{ y}$$

$$\partial_1 \equiv \begin{pmatrix} -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Usando álgebra lineal, vemos que $d_1 = \{1,2\} + \{2,3\} - \{1,3\} \in \tilde{H}_1(\Delta_{[7,0,1]}) \setminus \{0\}$ y $\dim(\tilde{H}_1(\Delta_{[7,0,1]})) = 1$.

Análogamente $d_2 = \{1,2\} + \{2,4\} - \{1,4\} \in \tilde{H}_1(\Delta_{[7,2,0]}) \setminus \{0\}$ y $\dim(\tilde{H}_1(\Delta_{[7,2,0]})) = 1$, y $\tilde{H}_1(\Delta_{[7,2,1]}) = (0)$.

En este caso, ambos conjuntos, C y C_1, coinciden. Luego

$$C_1 = \{[7,2,0],\ [7,0,1]\}.$$

Una vez obtenido C_1, pasamos a computar un sistema minimal de generadores del primer módulo de sicigias, N_1, de $k[S]$ mediante el isomorfismo $\tilde{H}_1(\Delta_m) \cong V_1(m)$. Para ello usaremos la sección III–C de esta memoria.

Comenzamos calculando un conjunto minimal de generadores de N_0. Nosotros hemos usado para ello el software aparecido en [VT99] (algoritmo I–D.2) y hemos obtenido

$$N_1 = I = \left\langle (N_1^1 =) - x_2\, x_4\, x_5\, {x_3}^4 + {x_1}^7, (N_1^2 =) - {x_3}^5\, x_4 + {x_1}^4\, {x_2}^2, (N_1^3 =) x_3\, {x_1}^3 - {x_2}^3\, x_5 \right\rangle$$

Sigamos los pasos y las notaciones de III–C para $d_1 = \{1,2\} + \{2,3\} - \{1,3\}$, por lo tanto $\lambda_{\{1,2\}} = 1, \lambda_{\{2,3\}} = 1, \lambda_{\{1,3\}} = -1$.
Para cualquier F' con $\dim(F') = 1 - 1 = 0$ (i.e. puntos), consideramos $b_{F'} \in I_{m-n_{F'}}$ dado por

$$b_{F'} = \sum_{F \in \Delta_{[7,0,1]}} \lambda_F \epsilon_{F'F} \frac{X_F}{X_{F'}} M_F$$

donde M_F es un monomio de grado $m - n_F$ para cualquier $F \in \Delta_{[7,0,1]}$. Entonces tomamos $a_{F'} = (a^l_{F'}) \in (R^3)_{m-n_{F'}}$, con $b_{F'} = \sum_l a^l_{F'} N^l_1$.

- $F' = \{1\}$.

$$\begin{array}{rcl} b_{\{1\}} & = & \sum_{F\in\Delta_{[7,0,1]}} \lambda_F \epsilon_{F'F} \frac{X_F}{X_{F'}} M_F \\ & = & \lambda_{\{1,2\}} \epsilon_{\{1\}\{1,2\}} \frac{X_1X_2}{X_1} X_1^3X_2^2X_5 + \lambda_{\{1,3\}} \epsilon_{\{1\}\{1,3\}} \frac{X_1X_3}{X_1} X_1^6 \\ & = & X_1^3X_2^3X_5 - X_1^6X_3 \\ & \Rightarrow & a_{\{1\}} = (0,0,-X_1^3) \end{array}$$

- $F' = \{2\}$.

$$\begin{array}{rcl} b_{\{2\}} & = & \sum_{F\in\Delta_{[7,0,1]}} \lambda_F \epsilon_{F'F} \frac{X_F}{X_{F'}} M_F \\ & = & \lambda_{\{1,2\}} \epsilon_{\{2\}\{1,2\}} \frac{X_1X_2}{X_2} X_1^3X_2^2X_5 + \lambda_{\{2,3\}} \epsilon_{\{2\}\{2,3\}} \frac{X_2X_3}{X_2} X_3^4X_4X_5 \\ & = & -X_1^4X_2^2X_5 + X_3^5X_4X_5 \\ & \Rightarrow & a_{\{2\}} = (0,-X_5,0) \end{array}$$

- $F' = \{3\}$.

$$\begin{array}{rcl} b_{\{3\}} & = & \sum_{F\in\Delta_{[7,0,1]}} \lambda_F \epsilon_{F'F} \frac{X_F}{X_{F'}} M_F \\ & = & \lambda_{\{1,3\}} \epsilon_{\{3\}\{1,3\}} \frac{X_1X_3}{X_3} X_1^6 + \lambda_{\{2,3\}} \epsilon_{\{3\}\{2,3\}} \frac{X_2X_3}{X_3} X_3^4X_4X_5 \\ & = & X_1^7 - X_3^4X_2X_4X_5 \\ & \Rightarrow & a_{\{3\}} = (1,0,0) \end{array}$$

- $F' = \{4\}$.

$$b_{\{4\}} = 0 \Rightarrow a_{\{4\}} = 0.$$

- $F' = \{5\}$.

$$b_{\{5\}} = 0 \Rightarrow a_{\{5\}} = 0.$$

Entonces $N^1_1 = X_1a_{\{1\}} + X_2a_{\{2\}} + X_3a_{\{3\}} = (X_2^2, -X_1^3, -X_3^4X_4)$.

Realizando el mismo cálculo con d_2, obtenemos que un conjunto minimal de generadores de N_1 es

$$\{(X_3, -X_2X_5, -X_1^4), (X_2^2, -X_1^3, -X_3^4X_4)\}.$$

Vamos a ver que el segundo módulo de sicigias es nulo.

Si el módulo fuese no nulo, existirían $g_1, g_2 \in k[X_1, \ldots, X_5]$ tales que

$$g_1 \cdot (X_3, -X_2X_5, -X_1^4) + g_2 \cdot (X_2^2, -X_1^3, -X_3^4X_4) = 0.$$

En tal caso, el cociente $g1/g2$ tendría que valer simultáneamente

$$-X_2^2/X_3, \quad -X_1^3/X_2X_5 \ \text{ y } -X_3^4X_4/X_1^4,$$

lo cual es imposible. Por lo tanto $g_1 = g_2 = 0$, luego $N_2 = 0$, y $N_i = 0$ $\forall i \geq 2$.

La resolución queda como sigue:

$$0 \to k[X_1, X_2, X_3, X_4, X_5]^2 \to k[X_1, X_2, X_3, X_4, X_5]^3 \to k[X_1, X_2, X_3, X_4, X_5] \to K[S] \to 0$$

BIBLIOGRAFÍA

[BCMP98a] E. BRIALES, A. CAMPILLO, C. MARIJUÁN, and P. PISÓN. Combinatorics of syzygies for semigroup algebra. *Collect. Math.*, 49:239–256, 1998.

[BCMP98b] E. BRIALES, A. CAMPILLO, C. MARIJUÁN, and P. PISÓN. Minimal systems of generators for ideals of semigroups. *J. of Pure and Applied Algebra*, 127:7–30, 1998.

[BH97] W. BRUNS and J. HERZOG. Semigroup rings and simplicial complexes. *J. of Pure and Applied Algebra*, 122:185–208, 1997.

[BLSR99] A.M. BIGATTI, R. LA SCALA, and L. ROBBIANO. Computing toric ideals. *J. Symbolic Computation*, 27:351–365, 1999.

[BLVS+93] A. BJÖRNER, M. LAS VERGNAS, B. STURMFELS, N. WHITE, and G. ZIEGLER. *Oriented Matroids*, volume 46 of *Encyclopedia of Mathematics and its Applications.* Cambridge Press, 1993.

[BM93] D. BAYER and D. MUMFORD. What can be computed in algebraic geometry? *Simposia Mathematica*, XXXIV:1–48, 1993.

[BMPCVT99] E. BRIALES-MORALES, P. PISÓN-CASARES, and A. VIGNERON-TENORIO. The regularity of a toric variety. *Preprint de la Universidad de Sevilla*, 55, 1999.

[BS87] D. BAYER and M. STILLMAN. A criterion for detecting m–regularity. *Inventiones mathematicae*, 87:1–11, 1987.

[BS98] D. BAYER and B. STURMFELS. Cellular resolution of monomial modules. *Journal für die Reine und Angewandte Mathematik*, 502:123–140, 1998.

[BW93] T. BECKER and V. WEISPFENNING. *Gröebner Bases. A Computational Approach to Commutative Albegra*. Springer-Verlag, 1993.

[CD94] E. CONTEJEAN and H. DEVIE. An efficient incremental algorithm for solving systems of linear equations. *Information and Computation*, 113:143–172, 1994.

[CF89] M. CLAUSEN and A. FORTENBACHER. Efficient solution of linear diophantine equations. *J. Symbolic Computation*, 8:201–216, 1989.

[CG00] A. CAMPILLO and P. GIMÉNEZ. Syzygies of affine toric varieties. *Journal of Algebra*, 225(1):142–161, 2000.

[CM91] A. CAMPILLO and C. MARIJUÁN. Higher relations for a numerical semigroup. *Sém. Théor. Nombres Bordeaux*, 3:249–260, 1991.

[CoC] CoCoA. Sistema de cálculo simbólico. *http:://cocoa.dima.unige.it*.

[COH93] H. COHEN. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993.

[CP] A. CAMPILLO and P. PISÓN. Toric mathematics from semigroup viewpoint. *Lect. Notes in Pure and Applied Mathematics, SAGAV, por aparecer*.

[CT91] P. CONTI and C. TRAVERSO. Buchberger algorithm and integer programming. *Lecture Notes in Comput. Sci., Springer*, 539, 1991.

[DBU95] F. DI BIASE and R. URBANKE. An algorithm to calculate the kernel of certain polynomial ring homomorphisms. *Experimental Mathematics*, 4(3):227–234, 1995.

[DOM91] E. DOMENJOUD. Solving systems of linear diophantine equations: An algebraic approach. *Lecture Notes in Computen Science, Springer-Verlag*, 520:141–150, 1991.

[EIS95] D. EISENBUD. *Introduction to Commutative Algebra with a View Towards Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer, New York, 1995.

[ES96] D. EISENBUD and B. STURMFELS. Binomial ideal. *Duke Math. J.*, 84(1):1–45, 1996.

[GOR73] P. GORDAN. Ueber die auflösung linearer gleichungen mit reellen coefficienten. *Mathematische Annalen*, 6:23–28, 1873.

[HER70] J. HERZOG. Generators of relations of abelian semigroups and semigroups ring. *Manuscripta Math.*, 3:175–193, 1970.

[HIL90] D. HILBERT. Ueber die theorie der algebraischen formen. *Math. Ann.*, 36:473–534, 1890.

[HOC95] M. HOCHSTER. Cohen-macaulay rings, combinatorics, and simplicial complexes. *In BR. McDonald, R.A. Morris editors, Ring Theory II, LNPAM, Marcel-Dekker*, 26:171–223, 1995.

[HS] S. HOSTEN and J. SHAPIRO. Primary decomposition of lattice basis ideals. *J. Symbolic Computation, por aparecer.*

[HS95] S. HOSTEN and B. STURMFELS. Grin: An implementation of gröbner bases for integer programming. *In E. Balas and J. Clausen editors, Integer Programming and Combina-*

torial Optimization, LNCS 920, Springer-Verlag, 920:267–276, 1995.

[HUE78] G. HUET. An algorithm to generate the basis of solutions to homogeneous linear diophantine equations. *Inform. Process. Lett.*, 7(3), 1978.

[LAM87] J.L. LAMBERT. Une borne pour les gènèrateurs des solutions entières positives d'une èquation diophantienne linéaire. *C. R. Acad. Sci. Paris.*, 305:39–40, 1987.

[PCVT96] P. PISÓN CASARES and A. VIGNERON TENORIO. Ideales de semigrupos con torsión: Cálculos mediante maplev. *Actas del EACA'96, Sevilla (Spain)*, 1996.

[PCVT98] P. PISÓN-CASARES and A. VIGNERON-TENORIO. $\mathbb{N}$–solutions to linear systems over $\mathbb{Z}$. *Preprint of University of Sevilla*, 43, 1998.

[PCVTer] P. PISÓN-CASARES and A. VIGNERON-TENORIO. First syzygies of toric varieties and diophantine equations in congruence. *Communications in Algebra*, Por aparecer.

[POT91] L. POTTIER. Minimal solutions of linear diophantine systems: bounds and algorithms. *Proceedings of the Fourth International Conference on Rewriting Techniques and Applications, Italy*, pages 162–173, 1991.

[PS98] I. PEEVA and B. STURMFELS. Syzygies of codimension 2 lattice ideals. *Math. Z.*, 229:163–194, 1998.

[RGS98] J. ROSALES and P. GARCÍA-SÁNCHEZ. Presentaciones de monoides cancelativos. *Proceedings of EACA'98, Guadalajara (Spain)*, pages 130–141, 1998.

[ROS91] J.C. ROSALES. *Semigrupos numéricos.* PhD thesis, Universidad de Granada, 1991.

[ROS95] J.C. ROSALES. On finitely generated submonoids of $\mathbb{N}^k$. *Semigroup Forum*, 50:251–262, 1995.

[RUB96] J.C. ROSALES and J.M. URBANO-BLANCO. A deterministic algorithm to decide if a finitely presented abelian monoid is cancellative. *Communications in Algebra*, 24(13):4217–4224, 1996.

[SCH96] A. SCHRIJVER. *Theory of Linear and Integer Programming.* Wiley-Interscience, 1996.

[STA96] R. STANLEY. *Combinatorics and commutative algebra 2nd ed*, volume 41 of *Progress in Mathematics.* Boston Basel Berlin, Birkhäuser, 1996.

[STU91] B. STURMFELS. Gröbner bases of toric varieties. *Tôhoku Math. J.*, 43:249–261, 1991.

[STU95] B. STURMFELS. *Gröbner Basis and Convex Polytopes*, volume 8 of *University Lecture Series.* American Mathematical Society, Providence, RI, 1995.

[TOM97] A.P. TOMAS. *On Solving Linear Diophantine Constraints.* PhD thesis, Facultad de Ciencias, Universidad de Oporto, 1997.

[VAS98] W.V. VASCONCELOS. *Computational Methods in Commutative Algebra and Algebraic Geometry*, volume 2 of *Algorithms and Computations in Mathematics.* Springer, 1998.

[VT99] A. VIGNERON-TENORIO. Semigroup ideals and linear diophantine equations. *Linear Algebra and its Applications*, 295:133–144, 1999.

Índice alfabético

Resumen:

Dado un semigrupo abeliano, cancelativo, finitamente generado y con elemento neutro, S, y un cuerpo k, podemos considerar el álgebra S-graduada k[S]. El estudio de esta álgebra tiene un gran interés dentro de la Geometría Algebraica por su relación con la Geometría Tórica. En esta memoria nos centramos en el estudio de los módulos de sicigias de la resolución del álgebra asociada al semigrupo. Damos algoritmos basados en bases de Gröbner que nos permiten calcular sistemas irreducibles de generadores del ideal de un semigrupo con torsión. Además, damos un método efectivo, basado en el cálculo de N-soluciones de sistemas diofánticos en congruencias, para calcular los grados que aparecen en el primer módulo de sicigias de k[S], ampliando estos resultados a toda la resolución del álgebra k[S]. De estos métodos, deducimos cotas para los grados que aparecen en un sistema minimal de generadores el i-ésimo módulo de sicigias, en función solamente de los generadores del semigrupo. Explicitamos una cota para la regularidad de una variedad tórica, así como un algoritmo para hallar dicha regularidad.

Abstract

Given a finitely commutative cancelative semigroup with zero element, S, and a field k, we can consider the S-graduated algebra k[S]. The study of this algebra has a great interest inside the Algebraic Geometry because of its relation with the Toric Geometry. In this memory we study the modules of sizigies of the resolution of the algebra associated with the semigroup. We give algorithms based on Gröbner bases that allow us to compute irreducible systems of generators of the ideal of a semigroup with torsion. Besides, we give an effective method to compute the degrees that appear in the first module of sicigias of k[S] using diophantine equations in congruences, extending these results to the whole resolution of the algebra k[S]. Of these methods, we deduce bounds for the degrees of a minimal systems of generators of the i-sizigies by means of the semigroup generators. We give explicit bounds for the regularity of a toric variety, as well as an algorithm to find it.