UNIVERSIDAD DE SEVILLA
Departamento de Álgebra

Cálculo de invariantes combinatorios de semigrupos numéricos y aplicaciones

Guadalupe Márquez Campos

Tesis doctoral

Cálculo de invariantes combinatorios de semigrupos numéricos y aplicaciones

Memoria presentada por Guadalupe Márquez Campos para optar al grado de Doctora en Matemáticas por la Universidad de Sevilla

V^o B^o del Director:

Fdo. José María Tornero Sánchez
Profesor Titular de Universidad
Departamento de Álgebra
Universidad de Sevilla

Sevilla, enero de 2014

A mis padres, Benicio y Rufina

Agradecimientos

Quisiera en estas lineas, agradecer a todos aquellos a los que con su ayuda han colaborado, directa o indirectamente, en la realización de esta tesis. Igualmenmte quería dejar constancia de mi agradecimiento a todos los que me han apoyado y acompañado durantes estos años.

A mi director, José María Tornero. En primer lugar por aceptarme como alumna, sin conocerme y sin prejuzgarme. Por darme la libertad de elegir tema de tesis, asumiendo el riesgo de aventurarse en un nuevo tema de investigación, que nada o poco tenía que ver con lo que había hecho hasta ahora. Gracias por su implicación, a nivel académico y personal, gracias por su interés y por sus infinitas, infinitas correcciones. Por confiar en mí, aun cuando yo no lo hacía, por su paciencia (que conmigo ha sido mucha). Gracias por su apoyo, y por sus ánimos cuando era necesario, y por sus presiones cuando también las necesitaba.

Me siento afortunada como alumna, porque no podría haber tenido un director mejor. Y me siento afortunada como persona, por conocer y trabajar con alguien como él (*buena gente* como dirían en Cádiz).

Gracias a Jorge L. Ramirez Alfonsín, por haberme dado la oportunidad de trabajar y aprender junto a él, en Montpellier. Por abrirme las puertas de su casa, y por lo bien que cocina Sylvie. Gracias por tu inestimable ayuda matemática y por su gran amabilidad.

Quería mencionar también, a Pedro García Sánchez, de la universidad de Granada, por tenernos en cuenta, y acordarse de nosotros al organizar distintos seminarios o encuentros, por abrirnos las puertas del mundo de los semigrupos numéricos. A José Carlos Rosales, por su aportaciones y en general a toda la comunidad de semigrupos numéricos por acogernos como

lo han hecho.

Quiero agradecer así mismo al comité organizador de la *EACA First International School on Computer Algebra*, celebrado en Tenerife en 2011. Gracias a esta escuela descubrí los semigrupos numéricos y el número de Frobenius, el cual despertó hasta tal punto mi interés que decidí dedicarle mi tiempo y esfuerzo durante estos aos.

A mis compañeros de despacho. Alberto, Marta y Loles. Nos hemos reído, estresado y llorado juntos.

Alberto, nuestro "wiki–Alberto", gracias por tu inestimable ayuda con la burocracia, sin ti Marta y yo no hubiéramos sobrevivido, lo tenemos claro. Gracias por tu *correctud* siempre, has sido la guía que hacía falta, la voz de la cordura y la sensatez. Sin ti este despacho hubiera sido un despilfarro, todo el día con la luz y el aire encendidos.

Marta, nuestra "Marta Fogg", la más viajera, gracias por tus contactos para buscar aquí y allá, gracias a ti no me tuve que buscar ningún puente en Montpellier. Gracias por todos tus "Guadalupe, estás bien?", gracias por ser una compañera y por ser una amiga.

Loles, nuestra baloncestera más risueña. Gracias por esos buenos ratos y risas, y por esos intercambios de apuntes de Álgebra para los físicos.

Gracias a los tres por saber escuchar, por vuestras conversaciones, no siempre de matemáticas, gracias "apañeros", porque empezasteis siendo solo compañeros de despacho, y os habéis convertido en grandes amigos. A los que quiero, y espero seguir teniendo en mi vida, estemos donde estemos y acabemos donde acabemos.

A todos los becarios del Departamento de Álgebra, Laura, Marithania y Jeroen, y a Helena, que es la doctora becaria. Y a nuestro infiltrado, Jorge. Porque le han dado al departamento ese toque que le faltaba. Gracias por esa cerveza de vez en cuando. Gracias por esas conversaciones divertidas y a veces hasta didácticas durante las comidas en la sala de café / multiusos.

A la gente del Departamento de Álgebra. Especialmente a Lola, a Jesús y a todos los compañeros con los que he compartido asignatura. Gracias por esas risas a la hora del café, porque con gente así da gusto venir a trabajar.

A todos mis amigos. En especial a todos los petard@s, a Amanda, que aunque esté lejos fisicamente, siempre ha estado cerca. A Eli y Ali, que han andado junto a mí en este camino. Eli, porque sin ti a Ali y a mí se nos

pasarían todos los plazos. A Yoli, que aunque esté de un lado a otro siempre tiene un momento para nosotros, gracias por no quedarte corta dándome el tenedor apropiado para la ensaladilla. A Ángela, por seguir siendo mi amiga de toda la vida, a pesar de *tener que coger cita* para un café conmigo. A todos vosotros y a vuestros respectivos, por apoyarme en mis malos momentos personales, por animarme cuando lo necesitaba.

Quiero recordar también a todas las personas que he conocido a lo largo de esta andadura. A todos aquellos becarios con los que he coincidido en congresos y escuelas, algunos de ellos ya todos unos doctores. A Jorge Ortigas, con su peso ideal y su tesis terminada, por meterse conmigo sacándome una sonrisa, a Nacho y Eva, gente divertida, con los que siempre es un gusto coincidir en cualquier congreso. A Irene, Ana y otros muchos que son los que marcan la diferencia de volver con una sonrisa de un encuentro.

Y por último pero no menos importante, a mi familia. A mis hermanos, mis cuñad@s, mis sobrinos y a toda mi gran familia. Porque mi familia es grande no solo en número y amplitud.

A mis padres en especial, porque son los dos pilares fundamentales de mi vida, a ellos les debo todo. Por sentirse orgullosos a cada paso que doy. Por confiar en mí en cualquier aspecto de mi vida, gracias papá y mamá.

A Alfonso. Porque he encontrado la felicidad junto a ti, y eso se nota. Porque no podía tener nadie más comprensivo a mi lado. Por esa tranquilidad que me aportas, por tus consejos y por tu cariño.

A todos, GRACIAS.

Resumen de la tesis doctoral *"Cálculo de invariantes combinatorios de semigrupos numéricos y aplicaciones"*

Guadalupe Márquez Campos

Departamento de Álgebra, Universidad de Sevilla

Esta tesis trata básicamente, de utilizar la relación entre bases de Groebner y semigrupos numéricos para obtener diversos resultados. La memoria consta de tres capítulos y un apéndice con una pequeña sección final con conclusiones y algunos problemas abiertos de cara a futuros trabajos.

En el primer capítulo, se establece una biyección entre bases de Groebner y semigrupos numéricos. Utiliza a su vez, dicha relación para intentar relacionar una serie de invariantes de semigrupos numéricos que aparecen en la famosa Conjetura de Wilf. Se obtienen como resultado dos cotas para $n(S)$, el cardinal del conjunto de los elementos esporádicos que son los elementos del semigrupo más pequeños que el número de Frobenius. Dichas cotas son obtenidas utilizando dos procedimientos diferentes basados en las mismas técnicas. Las cotas resultantes quedan en función del número de Frobenius y de los generadores del semigrupo.

En el segundo capítulo, se da un algoritmo para hallar el conjunto de Apéry de un semigrupo numérico. Para ello utilizamos las bases de Groebner definiendo para ello un orden de eliminación *ad hoc*.

Por último en el tercer capítulo, nos centramos en un problema clásico, el conteo de puntos de coordenadas enteras en particular en un triángulo rectángulo de vértices racionales. Damos una fórmula cerrada para la obtención del número de dichos puntos, y una generalización a dimensiones superiores.

En el apéndice el lector puede encontrar resultados básicos y definiciones sobre las bases de Groebner, que serán utilizadas a lo largo de la memoria.

Índice general

Extended abstract

N.B.: Esta parte de la tesis está redactada en inglés de cara a cumplir con la normativa vigente de la Universidad de Sevilla relativa a la Mención Internacional en el Título de Doctor.

This thesis deals with numerical semigroups. A numerical semigroup is a very special kind of semigroup that can be thought of as a set

$$\langle a_1, ..., a_k \rangle = \{\lambda_1 a_1 + ... + \lambda_k a_k \mid \lambda_i \in \mathbb{Z}_{\geq 0}\}, \text{ with } \gcd(a_1, ..., a_k) = 1.$$

This object has been thoroughly studied in the last years, when a significant number of problems concerning the description of these semigroups and some of its more interesting invariants have been tackled.

This memoire consists of three chapters and an appendix, with a final small section for conclusions and open problems. We will review in some detail the results the reader can find in each part.

The appendix is devoted to the basic results and definitions concerning Groebner bases which are used in the text, sometimes without explicit mention. The reader who is familiar with this tool may as well skip this part, which is only included for the convenience of the readers who are not.

In the first chapter we introduce some of the basic definitions and invariants of a numerical semigroup S. For instance:

- The set of gaps ($G(S)$ in this thesis), its cardinal $g(S)$ and its maximum $f(S)$, the so–called Frobenius number.
- The embedding dimension $e(S)$ and the multiplicity $m(S)$

- The sporadic elements $N(S)$ (that is, the elements in S which are smaller than $f(S)$); and its cardinal $n(S)$.

The main section of this chapter is devoted to a characterization of integers in S (or in $G(S)$, which is equivalent) using Groebner basis. The main result goes as follows:

Theorem.– *Let $S = \langle a_1, ..., a_k \rangle \subset \mathbb{Z}_{\geq 0}$ be a numerical semigroup. Consider $I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, y_3 - x^{a_3}, ..., y_k - x^{a_k} \rangle \subset \mathbb{Q}[x, y_1, ..., y_k]$, let $\mathcal{B} = \{g_1, ..., g_r\}$ be the reduced Groebner basis of I with respect to an elimination ordering for x, and $N_{\mathcal{B}}$ the normal form with respect to $\mathcal{B}$. Write also:*

$$\begin{aligned} q_i &= exp(g_i) \\ K_{q_i} &= q_i + \mathbb{Z}_{\geq 0}^{k+1} \\ E(I) &= \bigcup_{i=1}^{r} K_{q_i} \end{aligned}$$

- *The mapping*

$$\begin{aligned} \mathcal{F} : G(S) &\longrightarrow \bigcap_i \overline{K}_{q_i} \setminus \{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1} \\ N &\longmapsto exp\left(N_{\mathcal{B}}\left(x^N\right)\right) \end{aligned}$$

  is bijective.

- *The mapping*

$$\begin{aligned} \mathcal{G} : S &\longrightarrow \left[\bigcap_i \overline{K_{q_i}}\right] \bigcap \{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1} \\ M &\longmapsto exp\left(N_{\mathcal{B}}\left(x^M\right)\right) \end{aligned}$$

  is bijective.

These bijections will be most used in the sequel as they provide an easy (not necessarily in complexity terms) and versatile characterization of elements in (or not in) S, as the choice of orderings is quite wide. A first direct application of this result is shown in the next sections, where the following results are proved.

Theorem.– *Let $S = \langle a_1, ..., a_k \rangle$ be a numerical semigroup. Then*

$$n(S) \leq \frac{1}{k! a_1 ... a_k} \prod_{j=1}^{k} \left(f(S) + \sum_{i \neq j} a_i \right).$$

Theorem.– *Let $S = \langle a_1, ..., a_k \rangle$ be a numerical semigroup. Then*

$$n(S) \leq \sum_{\lambda=0}^{a_2} \left(\left\lfloor a_1 \cdot \frac{a_2 - \lambda}{a_2} \right\rfloor + 1 \right)^{k-1} + f(S) - a_1 a_2.$$

The second chapter deals with the Apéry set of a semigroup S with respect to an element $a \in S$. This set can be defined as

$$Ap(S, a) = \{x \in S \mid x - a \notin S\}$$

and some of its highly interesting properties are displayed, mainly how it can be used to compute easily some invariants of S.

After that we show how to compute (and *see*) the Apéry set (for the generators of the semigroup) using the Groebner bases techniques introduced in the first chapter. The important result here is the following:

Theorem.– *Let $S = \langle a_1, ..., a_k \rangle$ be a numerical semigroup. Consider the polynomial ring $\mathbb{Q}[x, y_1, ..., y_k]$, and let us define an elimination ordering for x, written σ_j, as follows:*

1. *First, we take into account the exponent on x.*
2. *After that, we take a graded ordering in $\{y_1, ..., y_k\}$ leaving aside y_j, and determined by the generators $a_1, ..., a_n$, that is, we order by*

$$\sum_{i=1, i \neq j}^{i=k} \alpha_i a_i,$$

   where α_i is the exponent on y_i.
3. *Then we use the lex ordering for all variables y_i, where $i = 1, ..., k$ and $i \neq j$.*

4. Finally, we use the exponent on y_j.

Consider the ideal I defined by

$$I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, y_3 - x^{a_3}, ..., y_k - x^{a_k} \rangle \subset \mathbb{Q}[x, y_1, ..., y_k]$$

and its Groebner basis with respect to σ_j. Let us write N_j the normal form with respect to this basis.

We define the following set:

$$\Delta = \left\{ N \in \mathbb{Z}_{\geq 0} \mid exp\left(N_j\left(x^N\right)\right) \in \{x = y_j = 0\} \bigcap \overline{E(I)} \right\}.$$

Then one has $\Delta = Ap(S, a_j)$.

This set Δ might be useful in order to study a related concept: the set of pseudo–Frobenius elements ($PF(S)$) and the Gorenstein condition, which states under which circumstances we have

$$n(S) = \frac{1}{2}(f(S) + 1).$$

This connection is explored in the last part of the second chapter.

In the third chapter we have a closer look at the classical problem (closely related to chapter 1) of counting the number of integral points in a right triangle. This matter has been tackled from different angles but, as far as we know, not from the viewpoint of numerical semigroups. Specifically we prove the following result:

Theorem.– Let $a < b$ be coprime integers, $\gamma \in \mathbb{Z}$. Consider the following set:

$$T = \left\{ (y_1, y_2) \in \mathbb{Z}^2_{\geq 0} \mid ay_1 + by_2 \leq \gamma \right\}.$$

Then

$$\begin{aligned}
\sharp\, T &= (\sharp\, B_0 + \sharp\, B_1 + ... + \sharp\, B_{k-1}) + \sharp\, B_k \\
&= \left(\frac{a+b-ab+1}{2} + \gamma\right) + ... + \left(\frac{(a+b)-(1+2i)ab+1}{2} + \gamma\right) + \\
&\qquad +... + \sum_{i=0}^{\lfloor \frac{\gamma_k}{b} \rfloor} \left(\left\lfloor \frac{\gamma_k - ib}{a} \right\rfloor + 1\right) \\
&= \sum_{i=0}^{k-1} \left(\frac{(a+b)-(1+2i)ab+1}{2} + \gamma\right) + \sum_{i=0}^{\lfloor \frac{\gamma_k}{b} \rfloor} \left(\left\lfloor \frac{\gamma_k - ib}{a} \right\rfloor + 1\right) \\
&= -\frac{ab}{2}k^2 + \frac{a+b+1+2\gamma}{2}k + \sum_{i=0}^{\lfloor \frac{\gamma - kab}{b} \rfloor} \left(\left\lfloor \frac{\gamma - kab - ib}{a} \right\rfloor + 1\right)
\end{aligned}$$

where $k = \lfloor \gamma/(ab) \rfloor$.

This result can be generalized (and we do) to an arbitrary dimensional object (an n–tetrahedron), at the obvious cost of a much messier formula.

Interestingly enough, the proof gathers together both the Groebner bases techniques introduced in chapter 1 and some help from the Apéry set in order to compute the actual number of integral points.

CAPÍTULO 1

Semigrupos numéricos y bases de Groebner

1.1 Semigrupos. Invariantes.

Esta memoria trabaja, en su mayor parte, alrededor de la estructura de semigrupo, esto es, un par $(X, *)$ formado por un conjunto y una operación binaria interna asociativa y con elemento neutro. De todos los semigrupos, nos van a interesar particularmente los semigrupos denominados *semigrupos numéricos*. Las referencias para los conceptos básicos, que a menudo omitiremos son [24, 12].

Definición 1.1 *Un semigrupo numérico es un semigrupo $S \subset \mathbb{Z}_{\geq 0}$.*

Ejemplo 1.1 *El primer ejemplo natural de semigrupo numérico es el* semigrupo generado por $\{a_1, ..., a_k\} \subset \mathbb{Z}_{\geq 0}$*, que es el conjunto de combinaciones lineales de estos enteros con coeficientes enteros no negativos:*

$$\langle\, a_1, ..., a_k \,\rangle = \{\lambda_1 a_1 + ... + \lambda_k a_k \mid \lambda_i \in \mathbb{Z}_{\geq 0}\}\,.$$

A la postre, resulta que éste no es un ejemplo de semigrupo numérico, sino que todos los semigrupos numéricos interesantes se pueden expresar de esta forma.

Proposición 1.1 *Sean enteros no negativos* $0 \leq a_1 \leq ... \leq a_k$ *y supongamos* $\gcd(a_1, ..., a_k) = 1$. *Consideremos* $S = \langle a_1, ..., a_k \rangle$. *Entonces existe* $N \in \mathbb{Z}$ *tal que para todo entero* $x \geq N$, *se tiene que* $x \in S$.

Demostración: Escribamos, de la Identidad de Bezout,

$$m_1 a_1 + ... + m_k a_k = 1,$$

para ciertos $m_i \in \mathbb{Z}$ y sean

$$P = \sum_{m_i \geq 0} m_i a_i > 0, \quad Q = \sum_{m_j \leq 0} m_j a_j \leq 0.$$

Tomamos un entero $t \geq (a_1 - 1)(-Q)$ y lo escribimos como $t = -Q(a_1 - 1) + k$, para $k \geq 0$. Dividimos entonces k entre a_1 para obtener

$$k = qa_1 + r, \text{ con } 0 \leq r < a_1$$

y entonces

$$\begin{aligned} t &= -Q(a_1 - 1) + qa_1 + r \\ &= -Q(a_1 - 1) + qa_1 + rP - rQ \\ &= q \cdot a_1 + rP + (-Q)(a_1 - 1 - r) \end{aligned}$$

lo cual finaliza la demostración, porque $a_1, P, -Q \in S$ y todos están multiplicados por enteros no negativos. Así pues, $t \in S$. ■

En el caso de que tuviésemos $\gcd(a_1, ..., a_k) = d > 1$ la situación es análoga, salvo que hemos de trabajar en el anillo $\mathbb{Z}d$, en lugar de $\mathbb{Z}$. Por ello, en adelante, cuando hablemos de semigrupos numéricos asumiremos sin (demasiada) pérdida de generalidad que $\{a_1, ..., a_k\}$ generan $\mathbb{Z}$ como grupo aditivo.

Corolario 1.1 *Todo semigrupo numérico se puede escribir de la forma* $\langle a_1, ..., a_k \rangle$.

Demostración: Sea S un semigrupo numérico; si tomamos elementos $a_1, ..., a_k \in S$ tales que $\gcd(a_1, ..., a_k) = 1$ tenemos claramente $\langle a_1, ..., a_k \rangle \subset S$, por lo que existe $N \in \mathbb{Z}_{\geq 0}$ como en la proposición, determinado por $\langle a_1, ..., a_k \rangle$.

Se tiene entonces de manera inmediata que

$$\{a_1, ..., a_k\} \cup \{x \in S \mid x < N\}$$

es un conjunto de generadores de S. ■

Dado que el semigrupo $S = \langle a_1, ..., a_k \rangle$ no es sino el conjunto de enteros positivos que se puede escribir como combinación lineal con coeficientes no negativos de $\{a_1, ..., a_k\}$, en ocasiones llamaremos a los elementos del semigrupo enteros *representables*. Por esto mismo, los elementos de $\mathbb{Z} \setminus S$ se denominan a veces enteros *no representables*).

Definición 1.2 *Algunos invariantes asociados a un semigrupo numérico* $S = \langle a_1, ..., a_k \rangle$ *son:*

1. *El* conjunto de gaps*, que es el complementario (finito, como acabamos de ver) de* S *en* $\mathbb{Z}_{\geq 0}$*, notado* $G(S)$*.*
2. *El* género*, que es el cardinal de* $G(S)$*, notado* $g(S)$*.*
3. *El* número de Frobenius*, que es el máximo entero en* $G(S)$*, esto es, el mayor entero no representable, notado* $f(S)$*.*
4. *El* conductor*, que es* $f(S) + 1$*.*
5. *El* conjunto de elementos esporádicos*, que son los elementos de* S *menores que* $f(S)$*, esto es* $S \cap [0, f(S)]$*, notado* $N(S)$*.*
6. *El cardinal del conjunto de elementos esporádicos, que se notará* $n(S)$*.*
7. *La* multiplicidad*, que es el menor elemento no nulo de* S*, notado* $m(S)$*.*
8. *La* dimensión*, que es el cardinal de un conjunto minimal de generadores, notado* $e(S)$*.*

Observación 1.1 *El cálculo del número de Frobenius de un semigrupo (o equivalentemente, de su conductor) es un problema sumamente interesante en este contexto. El caso de dimensión* 2*,* $S = \langle a_1, a_2 \rangle$ *fue resuelto por Sylvester en 1884 [29], quien demostró que:*

$$f(S) = a_1 a_2 - a_1 - a_2, \quad g(S) = \frac{1}{2} f(S).$$

Este problema (también conocido como the money changing problem *o* the nugget problem*), no tiene una solución tan simple para el caso* $d(S) \geq 3$*. Hay fórmulas cerradas para algunos casos, pero Ramírez Alfonsín ya demostró [23] que el problema es, en general, NP–hard.*

1.2 Gaps y Bases de Groebner.

Observación 1.2 *La mayoría de los resultados importantes y las notaciones relativas a las bases de Groebner se pueden encontrar en el apéndice. En la referencia [1] se pueden encontrar varios de los resultados de esta sección, aunque incluimos las demostraciones para facilitar la tarea del lector.*

Sean b un número natural fijado, $\{a_1, a_2, a_3, ..., a_k\}$ un conjunto de enteros positivos primos entre sí, y $\{\sigma_1, \sigma_2, \sigma_3, ..., \sigma_k\}$ un conjunto de variables que tomarán valores enteros no negativos. Planteamos la ecuación:

$$\sigma_1 a_1 + \sigma_2 a_2 + \sigma_3 a_3 + ... + \sigma_k a_k = b.$$

Introduciendo una variable x podemos reescribir la ecuación anterior de la siguiente forma:

$$(x^{a_1})^{\sigma_1}(x^{a_2})^{\sigma_2}(x^{a_3})^{\sigma_3}...(x^{a_k})^{\sigma_k} = x^b.$$

Introducimos ahora una variable y_j, para cada $j = 1, ..., k$, tomando $x^{a_i} = y_i$. Tenemos entonces la siguiente ecuación polinómica:

$$y_1^{\sigma_1} y_2^{\sigma_2} y_3^{\sigma_3} ... y_k^{\sigma_k} = x^b$$

con $\sigma_1, \sigma_2, \sigma_3, ..., \sigma_k$ incógnitas.

Definimos ahora el siguiente ideal

$$I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, y_3 - x^{a_3}, ..., y_k - x^{a_k} \rangle \subset \mathbb{Q}[x, y_1, ..., y_k],$$

y sea $\mathcal{B} = \{g_1, g_2, g_3, ..., g_r\}$ una base de Groebner minimal de dicho ideal (no necesariamente reducida), tomando por ejemplo el orden lexicográfico $x > y_1 > y_2 > ... > y_k$.

Notemos como $q_i = exp(g_i)$ y al cuadrante positivo con origen q_i, como

$$K_{q_i} = q_i + \mathbb{Z}_{\geq 0}^{k+1} \subset \mathbb{Z}_{\geq 0}^{k+1}, \qquad E(I) = \bigcup i = 1^r K_{q_i}.$$

El objetivo inmediato es ver que existen correspondencias biyectivas y explícitas:

$$\begin{aligned} G(S) &\longleftrightarrow \left[\bigcap_i \overline{K}_{q_i}\right] \setminus \{x=0\} \subset \mathbb{Z}_{\geq 0}^{k+1} \\ S &\longleftrightarrow \left[\bigcap_i \overline{K}_{q_i}\right] \cap \{x=0\} \subset \mathbb{Z}_{\geq 0}^{k+1} \end{aligned}$$

Para demostrar esto necesitaremos la aplicación

$$\begin{aligned} \phi : \mathbb{Q}[y_1, y_2, ..., y_k] &\longrightarrow \mathbb{Q}[x] \\ y_j &\longmapsto x^{a_j} \end{aligned}$$

y su extensión

$$\begin{aligned} \widetilde{\phi} : \mathbb{Q}[x, y_1, y_2, ..., y_k] &\longrightarrow \mathbb{Q}[x] \\ y_j &\longmapsto x^{a_j} \\ x &\longmapsto x \end{aligned}$$

Lema 1.1 $\ker\left(\widetilde{\phi}\right) = I$.

Demostración: Es obvio que $I \subset \ker\left(\widetilde{\phi}\right)$. Consideremos un polinomio $f(x, y_1, ..., y_k) \in \ker\left(\widetilde{\phi}\right)$ y hagamos la división euclídea con respecto a $y_k, ..., y_1$ (en este orden) para lograr una expresión del tipo

$$f = q_k(x, y_1, ..., y_k)\,(y_k - x^{a_k}) + ... + q_1(x, y_1)\,(y_1 - x^{a_1}) + r(x)$$

donde $r(x)$ pertenece a $\ker\left(\widetilde{\phi}\right)$, y por tanto $r(x) = 0$. ■

Lema 1.2 *La base de Groebner es binomial, y por tanto $N_{\mathcal{B}}(x^N)$ siempre es un monomio.*

Demostración: La base de Groebner $\mathcal{B}$ es en efecto binomial, porque los polinomios que generan el ideal I, son todos binomios [10]. Ahora bien, si tenemos que reducir un monomio del tipo x^N, con N un entero positivo, entre $\mathcal{B}$ que está formada por binomios, siempre nos quedará como resultado un monomio. Veámoslo de forma general.

Supongamos que tenemos un binomio $M_2 - M_3$, siendo M_2 el monomio líder, tal que podamos dividir M_1 entre M_2. De esta forma el resto de la división sería:

$$M_1 - \frac{M_1}{M_2}(M_2 - M_3) = \frac{M_1}{M_2}M_3,$$

que es por tanto un monomio. ■

Lema 1.3 *Sea $I \subset k[x_1, ..., x_n]$ un ideal, y sea $\mathcal{B}$ una base de Groebner de I. Sean $g, f \in k[x_1, ..., x_n]$. Entonces*

$$f \equiv g \mod I \iff N_{\mathcal{B}}(f) = N_{\mathcal{B}}(g).$$

Demostración: La aplicación $f \longmapsto N_{\mathcal{B}}(f)$ es k–lineal (esto es un ejercicio sencillo). En consecuencia $f \equiv g \mod I$ si y sólo si $f - g = h \in I$, de donde

$$N_{\mathcal{B}}(f) - N_{\mathcal{B}}(g) = N_{\mathcal{B}}(f - g) = N_{\mathcal{B}}(h) = 0,$$

y se tiene el resultado. ■

Teorema 1.1 *Sea $I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, ..., y_k - x^{a_k} \rangle \subseteq \mathbb{Q}[x, y_1, ..., y_k]$ un ideal y sea $\mathcal{B}$ la base de Groebner reducida de I con respecto al orden de eliminación $x > y_1 > ... > y_k$.*

Entonces $f \in \mathbb{Q}[x]$ está en la imagen de ϕ si y sólo si existe $h \in \mathbb{Q}[y_1, ..., y_k]$ tal que $N_{\mathcal{B}}(f) = h$, en este caso,

$$f = \phi(h) = h\left(x^{a_1}, ..., x^{a_k}\right).$$

Demostración: Si existe g tal que $f = \phi(g)$, entonces $f = g\left(x^{a_1}, ..., x^{a_k}\right)$ y por tanto $f(x) - g(y_1, ..., y_k) \in \ker\left(\widetilde{\phi}\right) = I$. Tenemos que

$$N_{\mathcal{B}}(f) = N_{\mathcal{B}}(g) = h\left(x, y_1, ..., y_k\right).$$

Ahora bien, como $\mathcal{B}$ no depende de x, los polinomios de $\mathcal{B}$ que se usan para la división tienen sus términos líder en $\mathbb{Q}\left[y_1, ..., y_k\right]$. Pero al usar un orden de eliminación para x esto implica que esos polinomios de $\mathcal{B}$ deben estar forzosamente en $\mathbb{Q}\left[y_1, ..., y_k\right]$. Esto implica que $h \in \mathbb{Q}\left[y_1, ..., y_k\right]$.

Supongamos ahora que $N_{\mathcal{B}}(f) = h \in \mathbb{Q}\left[y_1, ..., y_k\right]$. Entonces $f - h \in I$, luego

$$f(x) - h\left(y_1, ..., y_k\right) = \sum_{i=1}^{k} g\left(x, y_1, ..., y_k\right)\left(y_i - x^{a_i}\right),$$

y haciendo $y_i = x^{a_i}$ tenemos que $f = \phi(h) = h\left(x^{a_1}, ..., x^{a_k}\right)$. ■

Lema 1.4 *Si x^N está en la imagen de ϕ, entonces es la imagen de un monomio $y_1^{\sigma_1}y_2^{\sigma_2}...y_k^{\sigma_k} \in \mathbb{Q}[y_1, y_2, ..., y_k]$.*

Demostración: Sean $I = \langle y_j - x^{a_j} \,|\, j = i, ..., k\rangle$, y $\mathcal{B}$ como antes. Entonces por el teorema anterior, tenemos que $x^N \in Im(\phi)$ si y sólo si $N_{\mathcal{B}}(x^N) = h$ con $h \in \mathbb{Q}[y_1, y_2, ..., y_m]$. En este caso tenemos que $x^N = \phi(h)$. Como vimos anteriormente, h es un monomio. ■

Observación 1.3 *A pesar de que hemos fijado el orden lexicográfico, es inmediato de la demostración que en realidad sólo estamos usando la propiedad de ser un orden de eliminación para la variable x. Esto nos permitirá, en el futuro, poder cambiar el orden a considerar para adecuarlo a nuestros objetivos concretos.*

Teorema 1.2 *Sea $S = \langle a_1, ..., a_k\rangle$, I y $\mathcal{B}$ como antes, y sea $N \in \mathbb{Z}_{\geq 0}$. Entonces*

$$N \in S \iff x^N \in Im(\phi).$$

Más aún:

- *Si $N \in S$, entonces $N_{\mathcal{B}}\left(x^N\right) = y_1^{\sigma_1}...y_k^{\sigma_k}$ y $N = \sigma_1 a_1 + ... + \sigma_k a_k$.*
- *Si $N \notin S$, entonces $N_{\mathcal{B}}\left(x^N\right) = x^{\sigma_0}y_1^{\sigma_1}...y_k^{\sigma_k}$, con $\sigma_0 \neq 0$ y $N = \sigma_0 + \sigma_1 a_1 + ... + \sigma_k a_k$.*

Demostración: Sea $N \in S$. Existen entonces $\sigma_1, ..., \sigma_k \in \mathbb{Z}_{\geq 0}$ verificando

$$N = \sigma_1 a_1 + ... + \sigma_k a_k,$$

y entonces

$$\begin{array}{rcccl} x^N & = & x^{a_1\sigma_1 + a_2\sigma_2 + ... + a_k\sigma_k} & = & (x^{a_1})^{\sigma_1}(x^{a_2})^{\sigma_2}...(x^{a_k})^{\sigma_k} \\ & = & \phi(y_1^{\sigma_1})...\phi(y_k^{\sigma_k}) & = & \phi(y_1^{\sigma_1}...y_k^{\sigma_k}), \end{array}$$

esto es, $x^N \in Im(\phi)$.

Por otra parte, si $x^N \in Im(\phi)$, sabemos por la proposición anterior que

$$x^N = \phi(h) = \phi\left(y_1^{\sigma_1}...y_k^{\sigma_k}\right) = \left(x_1^{a_1}\right)^{\sigma_1} ... \left(x_k^{a_k}\right)^{\sigma_k},$$

y $N = \sigma_1 a_1 + ... + \sigma_k a_k$. Ya sabemos que, en estas condiciones, $h = N_{\mathcal{B}}\left(x^N\right)$.

Supongamos entonces que $N \notin S$. Sabemos que también en este caso $N_{\mathcal{B}}\left(x^N\right)$ es un monomio, pongamos

$$N_{\mathcal{B}}\left(x^N\right) = x^{\sigma_0} y_1^{\sigma_1} ... y_k^{\sigma_k}.$$

Dado que $N \notin S$, $N_{\mathcal{B}}\left(x^N\right) \notin \mathbb{Q}[y_1, ..., y_k]$, luego $\sigma_0 \neq 0$. Como $N_{\mathcal{B}}(f) - f \in I$ para cualquier polinomio f,

$$\exists h_i \in \mathbb{Q}[x, y_1, ..., y_k] \mid x^N - x^{\sigma_0} y_1^{\sigma_1} ... y_k^{\sigma_k} = \Sigma_{i=1}^k h_i (y_i - x^{a_i}).$$

Hacemos entonces el cambio $y_i = x^{a_i}$ y

$$x^N - x^{\sigma_0} x^{a_1 \sigma_1} ... x^{a_k \sigma_k} = 0$$

de donde $N = \sigma_0 + \sigma_1 a_1 + ... + \sigma_k a_k$. ■

Ya podemos probar las biyecciones que explicitamos hace un momento.

Teorema 1.3 *Sea $S = \langle a_1, ..., a_k \rangle \subset \mathbb{Z}_{\geq 0}$ un semigrupo numérico. Consideremos $I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, y_3 - x^{a_3}, ..., y_k - x^{a_k} \rangle \subset \mathbb{Q}[x, y_1, ..., y_k]$ y sea $\mathcal{B} = \{g_1, ..., g_r\}$ la base de Groebner reducida de I con respecto a un orden de eliminación para la variable x, siendo $q_i = exp(g_i)$.*

- *La correspondencia*

$$\begin{array}{rcl} \mathcal{F} : G(S) & \longrightarrow & \bigcap\limits_i \overline{K}_{q_i} \setminus \{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1} \\ N & \longmapsto & exp\left(N_{\mathcal{B}}\left(x^N\right)\right) \end{array}$$

  es biyectiva.

- *La correspondencia*

$$\begin{array}{rcl} \mathcal{G} : S & \longrightarrow & \left[\bigcap\limits_i \overline{K_{q_i}}\right] \bigcap \{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1} \\ M & \longmapsto & exp\left(N_{\mathcal{B}}\left(x^M\right)\right) \end{array}$$

  es biyectiva.

Demostración: La mayoría del resultado ya está más o menos demostrado.

I. $\mathcal{F}$ es sobreyectiva.

Sea $(\sigma_0, \sigma_1, ..., \sigma_k) \in Im(\mathcal{F})$. Existe entonces $N \in G(S)$ tal que

$$exp\left(N_{\mathcal{B}}\left(x^N\right)\right) = (\sigma_0, \sigma_1, ..., \sigma_k).$$

Por tratarse de una forma normal, debe verificar

$$(\sigma_0, \sigma_1, ..., \sigma_k) \in \bigcap_i \overline{K_{q_i}},$$

y ya hemos visto que en ese caso $\sigma_0 \neq 0$.

Por otra parte, consideremos

$$(\sigma_0, \sigma_1, ..., \sigma_k) \in \left[\bigcap_i \overline{K_{q_i}}\right] \bigcap \{x = 0\} = \left[\overline{\bigcup_i K_{q_i}}\right] \bigcap \{x = 0\},$$

de donde $(\sigma_0, \sigma_1, ..., \sigma_k)$ no pertenece a ningún K_{q_i} y así se tiene que

$$x^{\sigma_0} x^{a_1\sigma_1} ... x^{a_k\sigma_k} = N_{\mathcal{B}}\left(x^{\sigma_0} x^{a_1\sigma_1} ... x^{a_k\sigma_k}\right).$$

Consideremos entonces $N = \sigma_0 + \sigma_1 a_1 + ... + \sigma_k a_k$. Se verifica que

$$\widetilde{\phi}\left(x^N\right) = \widetilde{\phi}\left(x^{\sigma_0} y_1^{\sigma_1} ... y_k^{\sigma_k}\right) \Longrightarrow x^N \equiv x^{\sigma_0} y_1^{\sigma_1} ... y_k^{\sigma_k} \quad \text{mód } I.$$

De un resultado anterior

$$N_{\mathcal{B}}\left(x^N\right) = N_{\mathcal{B}}\left(x^{\sigma_0} y_1^{\sigma_1} ... y_k^{\sigma_k}\right),$$

y el hecho de que N es un gap de S se sigue de la unicidad de la forma normal y de la caracterización de los elementos de S que vimos en el teorema anterior.

II. $\mathcal{G}$ es sobreyectiva.

La prueba sigue el esquema de la anterior, con las lógicas modificaciones. Tomamos primero $(\sigma_0, \sigma_1, ..., \sigma_k) \in Im(\mathcal{G})$. Entonces existe $N \in S$ con

$$exp\left(N_{\mathcal{B}}\left(x^N\right)\right) = (\sigma_0, \sigma_1, ..., \sigma_k).$$

Por ser una forma normal

$$(\sigma_0, \sigma_1, ..., \sigma_k) \in \bigcap_i \overline{K_{q_i}}$$

y tenemos que probar $\sigma_0 = 0$. Pero esto ya nos lo asegura el teorema anterior.

Veamos ahora

$$Im\,(\mathcal{G}) \supset \left(\bigcap_i \overline{K}_{q_i}\right) \bigcap \{x = 0\}, \;\; \forall i = 1, .., r.$$

Para ello, dado $(0, \sigma_1, ..., \sigma_k) \in \bigcap_i \overline{K}_{q_i}$, encontrarmos un cierto $M \in S$ con $exp\left(N_{\mathcal{B}}\left(x^M\right)\right) = (0, \sigma_1, ..., \sigma_k)$.

Tomemos $(0, \sigma_1, ..., \sigma_k) \in \bigcap \overline{K}_{q_i}$. Esto es, $(0, \sigma_1, ..., \sigma_k)$ no aparece en ningún K_{q_i}. Por tanto $y_1^{\sigma_1}...y_k^{\sigma_k} = N_{\mathcal{B}}\,(y_1^{\sigma_1}...y_k^{\sigma_k})$.

Definimos entonces $M = \sigma_1 a_1 + \sigma_2 a_2 + \sigma_3 a_3 + ... + \sigma_k a_k$ y a partir de $\widetilde{\phi}$ podemos comprobar que

$$\widetilde{\phi}\left(x^M\right) = \widetilde{\phi}\,(y_1^{\sigma_1}...y_k^{\sigma_k}) \Longrightarrow x^M \equiv y_1^{\sigma_1}...y_k^{\sigma_k} \mod I.$$

Esto implica que $N_{\mathcal{B}}\left(x^M\right) = N_{\mathcal{B}}\,(y_1^{\sigma_1}...y_k^{\sigma_k})$.

III. $\mathcal{F}$ y $\mathcal{G}$ son inyectivas.

Asumimos que tenemos dos enteros N_1, N_2 con

$$exp\left(N_{\mathcal{B}}\left(x^{N_1}\right)\right) = exp\left(N_{\mathcal{B}}\left(x^{N_2}\right)\right)$$

lo cual equivale a que $x^{N_1} \equiv x^{N_2} \mod I$. Entonces hay unos ciertos polinomios $h_1, ..., h_r$ tales que

$$x^{N_1} = x^{N_2} + \sum_{i=1}^{k} h_i(y_i - x^{a_i}),$$

y haciendo el cambio $y_i = x^{a_i}$ obtenemos $x^{N_1} = x^{N_2}$ y $N_1 = N_2$. ■

Ejemplo 1.2 *Veamos en primer lugar un ejemplo de los más simples, que son en este caso para un conjunto de dos generadores. Sean en este primer ejemplo, $a_1 = 5$ y $a_2 = 7$. En este caso, usando la fórmula de Sylvester, el número de Frobenius sería:*

$$f(5, 7) = 5 \cdot 7 - 5 - 7 = 23.$$

Y su conjunto de gaps:

$$G(S) = \{1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 11,\ 13,\ 16,\ 18,\ 23\}.$$

Tomemos ahora el ideal $I = \langle y_1 - x^5, y_2 - x^7 \rangle \subset \mathbb{Q}[x, y_1, y_2]$ *, y hallamos la base de Groebner de dicho ideal, usando un orden de eliminación en la variable* x*. En este caso hemos usado el orden habitual, el lexicográfico* $x > y_1 > y_2$ *. Con este orden escogido la base de Groebner resultante es la siguiente:*

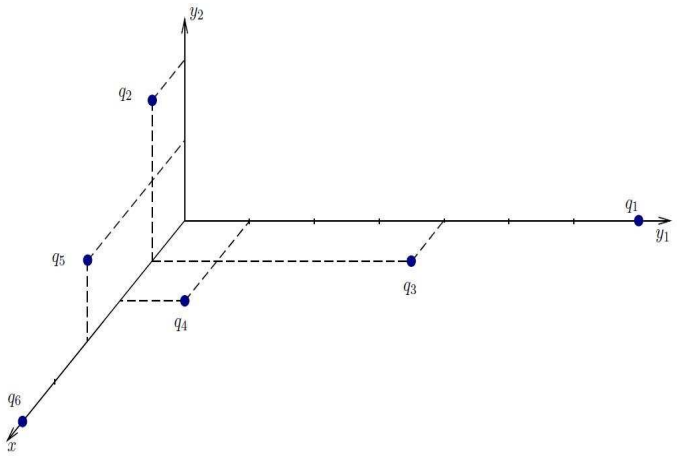
$$\mathcal{B} = \left\{-y_2^5 + y_1^7,\ -y_1^3 + y_2^2 x,\ -y_2^3 + y_1^4 x,\ y_1 x^2 - y_2,\ y_2 x^3 - y_1^2,\ -y_1 + x^5\right\}$$

Tras este cálculo el siguiente paso es representar la escalera de esta base, que estará formada por los cuadrantes positivos cuyos origenes serán los exponentes de los monomios líderes de cada elemento de la base, usando el orden correspondiente elegido. Notamos, como antes, $q_i = exp(g_i)$ *donde* g_i *es el elemnto* i*–ésimo de la base de Groebner.*

Tendríamos que representar los siguientes puntos en el sistema de referencia formado por las tres variables $\{x, y_1, y_2\}$*:*

$$\begin{array}{lllllllll} q_1 & = & (0,7,0), & q_2 & = & (1,0,2), & q_3 & = & (1,4,0), \\ q_4 & = & (2,1,0), & q_5 & = & (3,0,1), & q_6 & = & (5,0,0) \end{array}$$

Obteniendo la siguiente representación[1]*:*



[1]De ahora en adelante los q_i aparecerán representados como puntos azules.

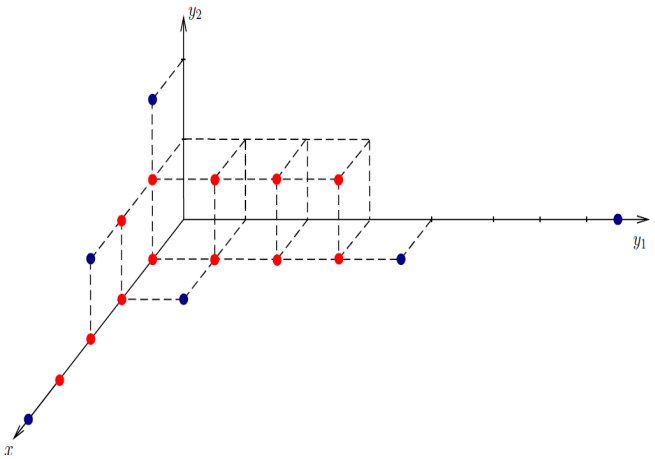
Veamos ahora que cada elemento de $G(S)$, se corresponde de manera unívoca con un punto de coordenadas enteras del conjunto

$$\left[\bigcap_i \overline{K}_{q_i}\right] \setminus \{x = 0\} \subset \mathbb{Z}^3_{\geq 0}.$$

Para ello calculamos la forma normal de los monomios x^{n_i} sindo n_i el elemento i–ésimo del conjunto $G(S)$, resultando lo siguiente:

$$\begin{array}{lllllllll}
N_{\mathcal{B}}(x^1) & = & x & N_{\mathcal{B}}(x^2) & = & x^2 & N_{\mathcal{B}}(x^3) & = & x^3 \\
N_{\mathcal{B}}(x^4) & = & x^4 & N_{\mathcal{B}}(x^6) & = & xy_1 & N_{\mathcal{B}}(x^8) & = & xy_2 \\
N_{\mathcal{B}}(x^9) & = & x^2y_2 & N_{\mathcal{B}}(x^{11}) & = & xy_1^2 & N_{\mathcal{B}}(x^{13}) & = & xy_1y_2 \\
N_{\mathcal{B}}(x^{16}) & = & xy_1^3 & N_{\mathcal{B}}(x^{18}) & = & xy_1^2y_2 & N_{\mathcal{B}}(x^{23}) & = & xy_1^3y_2
\end{array}$$

Una vez que tenemos las formas normales calculadas, obtenemos sus exponentes correspondientes y representamos dichos puntos en el sistema de referencia anterior[2]*:*



Observamos que los puntos anteriores coinciden exactamente con todos los puntos de coordenadas enteras que quedan fuera de la escalera de la base de Groebner, ilustrando así la biyección que hemos demostrado anteriormente.

[2]De ahora en adelante los puntos correspondientes a elementos de $G(S)$ aparecerán representados como puntos rojos.

Ejemplo 1.3 *Ahora vamos a ver un ejemplo con tres generadores. Sea* $S = \langle 7, 9, 11\rangle$. *El número de Frobenius de este semigrupo es:*

$$f(S) = 26,$$

y su conjunto de gaps:

$$G(S) = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,\ 10,\ 12,\ 13,\ 15,\ 17,\ 19,\ 24,\ 26\}.$$

Tomemos el ideal binomial

$$I = \langle y_1 - x^7, y_2 - x^9, y_3 - x^{11}\rangle \subset \mathbb{Q}[x, y_1, y_2, y_3]$$

y hallemos la base de Groebner $\mathcal{B}$ *de dicho ideal, usando un orden de eliminación en la variable* x. *En este caso volvemos a usar el orden lexicográfico* $x > y_1 > y_2 > y_3$. *Con este orden escogido la base de Groebner resultante es la siguiente:*

$$\begin{aligned}\mathcal{B} \;=\; & \{y_2^{11} - y_3^9, -y_2^2 + y_3y_1, y_2^9y_1 - y_3^8, y_2^7y_1^2 - y_3^7, y_2^5y_1^3 - y_3^6, y_2^3y_1^4 - y_3^5,\\ & y_1^5y_2 - y_3^4, -y_2y_3^3 + y_1^6, -y_2y_1^2 + y_3^2x, -y_1^3 + y_3y_2x, y_2^3x - y_1^4,\\ & y_2^2y_1^2x - y_3^3, -y_3^2 + y_1^3x, y_2x^2 - y_3, y_1x^2 - y_2, y_3x^3 - y_1^2, -y_1 + x^7\}\end{aligned}$$

Representemos ahora la escalera de esta base, que estará formada por los cuadrantes positivos cuyos orígenes serán los exponentes de los monomios líder de cada elemento de la base, con respecto al orden elegido. Notando al igual que en el ejemplo anterior $q_i = exp(lt(g_i))$ *donde* g_i *es el elemento* i*–ésimo de la base de Groebner, y al cuadrante positivo con origen* q_i, *como*

$$K_{q_i} = q_i + \mathbb{Z}_{\geq 0}^{k+1} \subset \mathbb{Z}_{\geq 0}^{k+1},$$

tendríamos el siguiente conjunto de exponentes líder

$$\begin{array}{lllllllll}
q_1 = (0,0,11,0), & q_2 = (0,1,0,1), & q_3 = (0,1,9,0),\\
q_4 = (0,2,7,0), & q_5 = (0,3,5,0), & q_6 = (0,4,3,0),\\
q_7 = (0,5,1,0), & q_8 = (0,6,0,0), & q_9 = (1,0,0,2),\\
q_{10} = (1,0,1,1), & q_{11} = (1,0,3,0), & q_{12} = (1,2,2,0),\\
q_{13} = (1,3,0,0), & q_{14} = (2,0,1,0), & q_{15} = (2,1,0,0),\\
q_{16} = (3,0,0,1), & q_{17} = (7,0,0,0) &
\end{array}$$

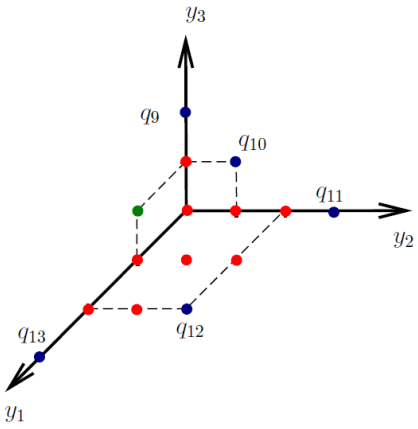
Veamos la biyección de la aplicación $\mathcal{F}$, para lo cual sólo consideraremos los puntos de $\overline{E(I)}$ que quedan fuera del hiperplano $x = 0$. Nos fijaremos separadamente en cada uno de los hiperplanos del tipo $x = \lambda$, con $\lambda \in \mathbb{Z}_{\geq 0}$, para poder representarlos gráficamente. Así, tendremos:

- $x = 1$. *En este hiperplano tenemos varios vértices q_i, concretamente*

$$q_9 = (0, 0, 2),\ q_{10} = (0, 1, 1),\ q_{11} = (0, 3, 0),$$

$$q_{12} = (2, 2, 0),\ q_{13} = (3, 0, 0)$$

Estos puntos delimitan los elementos de $\mathbb{Z}^4_{\geq 0} \setminus E(I)$, junto con el punto $(1, 1, 0, 1) \in K_{q_2}$, obteniendo[3]*:*



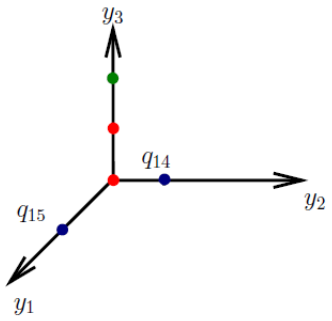
Como representación alternativa, usaremos en lo sucesivo tablas como la que presentamos a continuación. En la esquina superior izquierda aparecen los datos fijos de la tabla (en este caso x e y_3), mientras que en los ejes (cuadros amarillos) aparecen las variables. Los puntos del retículo determinan por tanto un punto de $\mathbb{Z}$, dado en este caso por $x + 7y_1 + 9y_2 + 11y_3$. Los cuadros azules representan puntos fuera de la escalera $E(I)$ y los números que aparecen en estos recuadros deben ser (por $\mathcal{F}$), elementos de $G(S)$.

[3]De ahora en adelante los puntos de $E(I)$ que no son vértices aparecerán representados por puntos verdes.

x	y3	y2					x	y3		
1	0	0	1	2	3		1	1	0	1
y1->	0	1	10	19	28			0	12	21
	1	8	17	26	35			1	19	28
	2	15	24	33	42			2	26	35
	3	22	31	40	49					

- *En el nivel $x = 2$ los siguientes puntos son los que delimitan los valores de y_1, y_2 e y_2:*

$$q_{14} = (0, 1, 0), \quad q_{15} = (1, 0, 0), \quad (0, 0, 2) \in K_{q_9}$$

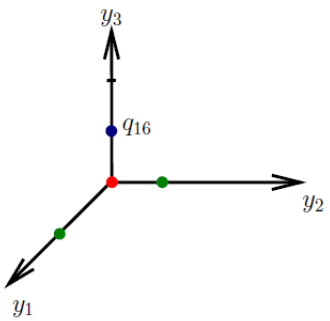


Al igual que antes, representamos los puntos de este hiperplano que se quedan fuera de la escalera en una tabla

x	y3	y2			x	y3		
2	0	0	1		2	1	0	1
y1->	0	2	11			0	13	22
	1	9	18			1	20	29
	2	16	25			2	27	36

- *Repetimos en el nivel $x = 3$, donde tenemos*

$$q_{16} = (0, 0, 1), \quad (1, 0, 0) \in K_{q_{15}}, \quad (0, 1, 0) \in K_{q_{14}}$$



x	y3	y2	
3	0	0	1
y1->	0	3	12
	1	10	19

- *Los puntos encerrados por la escalera en los hiperplanos* $x = 4$, $x = 5$, $x = 6$, *son únicamente el origen en cada uno de ellos, ya que las variables* y_i, *para* $i = 1, 2, 3$ *están acotadas en los niveles anteriores por* $y_i = 1$. *Por lo que tendriamos*

x	y3	y2	
4	0	0	1
y1->	0	4	13
	1	11	20

x	y3		
5	0	0	1
y1->	0	5	
	1	12	

x	y3		
6	0	0	1
y1->	0	6	
	1	13	

- *Por último, en el plano* $x = 7$ *tenemos que el origen es* $(7, 0, 0, 0) = q_{17}$, *por lo que hace de* techo *de la variable* x.

Si calculamos entonces la forma normal de los monomios x^{n_i}, *siendo* n_i *el gap* i*–ésimo del conjunto* $G(S)$, *obtenemos lo siguiente:*

$$\begin{array}{lllllllll} N_{\mathcal{B}}(x^1) & = & x & N_{\mathcal{B}}(x^2) & = & x^2 & N_{\mathcal{B}}(x^3) & = & x^3 \\ N_{\mathcal{B}}(x^4) & = & x^4 & N_{\mathcal{B}}(x^5) & = & x^5 & N_{\mathcal{B}}(x^6) & = & x^6 \\ N_{\mathcal{B}}(x^8) & = & xy_1 & N_{\mathcal{B}}(x^{10}) & = & xy_2 & N_{\mathcal{B}}(x^{12}) & = & xy_3 \\ N_{\mathcal{B}}(x^{13}) & = & x^2y_3 & N_G(x^{15}) & = & xy_1^2 & N_{\mathcal{B}}(x^{17}) & = & xy_1y_2 \\ N_{\mathcal{B}}(x^{19}) & = & xy_2^2 & N_{\mathcal{B}}(x^{24}) & = & xy_1^2y_2 & N_{\mathcal{B}}(x^{26}) & = & xy_1y_2^2 \end{array}$$

Observación 1.4 *Tenemos una forma de representar todo entero* $N \geq 0$ *con respecto a* S, *dada por los resultados anteriores*

$$exp\left(N_{\mathcal{B}}(x^N)\right) = (\sigma_0, ..., \sigma_k) \implies N = \sigma_0 + \sum_{i=1}^{k} a_i\sigma_i.$$

Esta representación es única si fijamos la condición

$$(\sigma_0, ..., \sigma_k) \in \bigcap_i \overline{K}_{q_i},$$

y determina rápidamente si $N \in S$ o no, simplemente comprobando si σ_0 es nulo o no.

Sea entonces $N \in S$. Una función muy interesante inducida por S (en realidad por el conjunto $\{a_1, ..., a_k\}$, para ser precisos) es la llamada función denumerante, definida como sigue

$$\begin{array}{rcl} d : S & \longrightarrow & \mathbb{Z} \\ N & \longmapsto & d(N) = \sharp \left\{ (y_1, ..., y_k) \in \mathbb{Z}_{\geq 0}^k \;\middle|\; N = \sum_{i=1}^{k} y_i a_i \right\} \end{array}$$

Esto es, $d(N)$ no es más que el número de representaciones diferentes de N como combinación lineal entera no negativa de $\{a_1, ..., a_k\}$.

Por otro lado, si tomamos $N \in S$, aparte de la representación que acabamos de mencionar, podemos muy bien tener muchas otras, sólo que todas deben estar en algún K_{q_i}. Por si acaso alguien se lo pregunta, no hay relación directa entre $d(N)$ y

$$\sharp \left\{ q_i \mid x^N \in K_{q_i} \right\},$$

como se puede demostrar con un ejemplo sencillo.

Consideremos $S = \langle 5, 7 \rangle$. Se tiene que $f(S) = 23$, y tenemos que de un mismo número, como es por ejemplo el 100, tenemos tantas representaciones como soluciones enteras para y_1 y y_2 de la siguiente ecuación:

$$y_1 = 7n + 6, \quad y_2 = -5n + 10, \quad n \in \mathbb{Z}.$$

O, siguiendo en el mismo conjunto, del número entero 327, tenemos tantas representaciones como soluciones enteras no negativas de la ecuación siguiente:

$$y_1 = 7n + 1, \quad y_2 = 46 - 5n, \quad n \in \mathbb{Z},$$

como por ejemplo;

$$327 = 5 + 7 \cdot 46 = 5 \cdot 8 + 7 \cdot 41 = 5 \cdot 15 + 7 \cdot 36 = 5 \cdot 22 + 7 \cdot 31,$$

Y como se puede comprobar fácilmente, todos estos puntos están en un mismo K_{q_i}.

1.3 Una aplicación *"á la Wilf"*.

Una de las conjeturas más famosas en semigrupos numéricos se la debemos a Wilf [32] quien estableció una relación muy sencilla entre tres invariantes.

Conjetura de Wilf.– Sea S un semigrupo numérico. Se tiene que

$$c(S) \leq e(S)n(S).$$

Dicho de otro modo, la conjetura de Wilf nos dice que los elementos esporádicos tienen que representar, como poco, la $e(S)$–ésima parte de los enteros menores que $f(S)$ (que es tanto como decir $c(S)$).

La conjetura se ha demostrado para familias de casos particulares (ver, por ejemplo, [15, 28]). También ha sido comprobada para todos los semigrupos de género menor que 50 por M. Bras–Amorós [5].

Lo que sigue es nuestro intento por usar las herramientas desarrolladas en la sección anterior al problema de relacionar $n(S)$ y $c(S)$, que obtuvo resultados distintos de los esperados.

Notación.– Dados números racionales positivos $\alpha_1, ..., \alpha_n$, definimos

$$\begin{aligned} P(\alpha_1, ..., \alpha_n) &= \left\{ (x_1, ..., x_n) \in \mathbb{Z}^n_{>0} \mid \frac{x_1}{\alpha_1} + ... + \frac{x_n}{\alpha_n} \leq 1 \right\}. \\ Q(\alpha_1, ..., \alpha_n) &= \left\{ (x_1, ..., x_n) \in \mathbb{Z}^n_{\geq 0} \mid \frac{x_1}{\alpha_1} + ... + \frac{x_n}{\alpha_n} \leq 1 \right\}. \end{aligned}$$

y

$$\begin{aligned} p(\alpha_1, ..., \alpha_n) &= \sharp\left(P(\alpha_1, ..., \alpha_n)\right) \\ q(\alpha_1, ..., \alpha_n) &= \sharp\left(Q(\alpha_1, ..., \alpha_n)\right) \end{aligned}$$

Esto es, $q(\alpha_1, ..., \alpha_n)$ determina el número de puntos enteros en el tetraedro limitado por los hiperplanos coordenados y el hiperplano

$$\frac{x_1}{\alpha_1} + ... + \frac{x_n}{\alpha_n} = 1,$$

mientras que $p(\alpha_1, ..., \alpha_n)$ calcula lo mismo, pero descartando los puntos sobre las caras coordenadas.

La relación entre ambas cantidades viene dada por este resultado:

Lema 1.5 *En las condiciones anteriores, si*

$$\alpha = \frac{1}{\alpha_1} + ... + \frac{1}{\alpha_n},$$

entonces

$$q(\alpha_1, ..., \alpha_n) = p(\alpha_1(1+\alpha), ..., \alpha_n(1+\alpha)).$$

Demostración: Consideremos la siguiente aplicación

$$\begin{array}{rcl} \Phi : Q(\alpha_1, ..., \alpha_n) & \longrightarrow & P(\alpha_1(1+\alpha), ..., \alpha_n(1+\alpha)) \\ (x_1, ..., x_n) & \longmapsto & (x_1 + 1, ..., x_n + 1) \end{array}$$

Notemos que está bien definida, ya que

$$\sum_{i=1}^{n} \frac{x_i + 1}{\alpha_i(1+\alpha)} = \frac{1}{1+\alpha} \left(\sum_{i=1}^{n} \frac{x_i}{\alpha_i} + \sum_{i=1}^{n} \frac{1}{\alpha_i} \right) \leq 1,$$

por lo que $Im(\Phi) \subset P(\alpha_1(1+\alpha), ..., \alpha_n(1+\alpha))$.

Φ es claramente inyectiva, pero también es sobre dado que

$$\sum_{i=1}^{n} \frac{x_i}{\alpha_i(1+\alpha)} \leq 1 \iff \sum_{i=1}^{n} \frac{x_i}{\alpha_i} \leq 1 + \alpha \iff \sum_{i=1}^{n} \frac{x_i - 1}{\alpha_i} \leq 1.$$

■

La búsqueda de una acotación fina y lo más simple posible de $Q(\alpha_1, ..., \alpha_n)$ y $P(\alpha_1, ..., \alpha_n)$ ha conducido a diversos resultados [17, 18, 19, 31, 33, 34, 35], que finalmente se vieron recogidos y resumidos en la denominada Conjetura GLY (por sus autores, Granville–Lin–Yau).

Conjetura GLY.– Supongamos que $n \geq 3$ y que tenemos números reales positivos $\alpha_1 \geq ... \geq \alpha_n \geq 1$. Entonces:

- (Estimación débil) Se tiene que

$$n! \cdot p(\alpha_1, ..., \alpha_n) \leq (\alpha_1 - 1)...(\alpha_n - 1),$$

con igualdad si y solo si $\alpha_n = 1$.

- (Estimación fuerte) Dado n, existe una constante $C(n)$ tal que, para $\alpha_n \geq C(n)$ se tiene que

$$n! \cdot p(\alpha_1, ..., \alpha_n) \leq A_n^n + (-1)\frac{S_1^{n-1}}{n} A_{n-1}^n + \sum_{l=2}^{n-1} (-1)^l \frac{S_l^{n-1}}{\left(\begin{array}{c} n-1 \\ l-1 \end{array} \right)} A_{n-l}^{n-1},$$

  donde los S_l^{n-1} son los números de Stirling y los A_i^l polinomios en $\alpha_1, ..., \alpha_l$ de grado i.

La conjetura fue probada, en su versión débil por Yau y Zhang [36]. En el mismo artículo se anuncia que la versión fuerte ha sido comprobada computacionalmente para $n \leq 10$. De hecho la conjetura puede ser comprobada computacionalmente para un n concreto, pero no parece que se vaya a mejorar espectacularmente esta situación ya que, según los autores, el caso $n = 10$ ya llevó varias semanas.

En nuestro ámbito de aplicación, consideramos un semigrupo numérico $S = \langle a_1, ..., a_k \rangle$ y, como hicimos en la sección anterior, consideramos el ideal

$$I = \langle y_i - x^{a_i} \mid i = 1, ..., k \rangle \subset \mathbb{Q}\left[x, y_1, ..., y_k\right].$$

Fijamos un orden de eliminación para x cualquiera y hallamos la base de Groebner $\mathcal{B}$ de I para este orden. Entonces, si notamos $E(I)$ a la escalera definida por $\mathcal{B}$, sabemos que

$$\begin{array}{rcl} S & \stackrel{1:1}{\longleftrightarrow} & \left[\mathbb{Z}_{\geq 0}^{k+1} \setminus E(I)\right] \cap \{x = 0\} \\ N = \sum \sigma_i a_i & \longleftrightarrow & (0, \sigma_1, ..., \sigma_k) \end{array}$$

Notemos entonces que

$$\begin{array}{rcl} n(S) & = & \sharp\{a \in S \mid a \leq f(S)\} \\ & = & \sharp\left\{(0, y_1, ..., y_k) \in \mathbb{Z}_{\geq 0}^{k+1} \setminus E(I) \mid \sum y_i a_i \leq f(S)\right\}, \end{array}$$

lo cual prueba que $n(S)$ es menor o igual que el número de puntos enteros del tetraedro definido por los hiperplanos coordenados y el hiperplano

$$\frac{y_1}{f(S)/a_1} + ... + \frac{y_k}{f(S)/a_k} \leq 1.$$

Esto es,

$$n(S) \leq q\left(\frac{f(S)}{a_1}, ..., \frac{f(S)}{a_k}\right),$$

y por el lema anterior y la estimación débil de la Conjetura GLY,

$$\begin{aligned} n(S) &\leq p\left(\frac{f(S)}{a_1}\left(1+\sum\frac{a_i}{f(S)}\right), ..., \frac{f(S)}{a_k}\left(1+\sum\frac{a_i}{f(S)}\right)\right) \\ &= p\left(\frac{f(S)+\sum a_i}{a_1}, ..., \frac{f(S)+\sum a_i}{a_k}\right) \\ &\leq \frac{1}{k!}\prod_{j=1}^{k}\left(\frac{f(S)+\sum a_i}{a_j}-1\right) \\ &= \frac{1}{k!a_1...a_k}\prod_{j=1}^{k}\left(f(S)+\sum_{i\neq j}a_i\right) \end{aligned}$$

De esta forma hemos demostrado el siguiente resultado:

Proposición 1.2 *Dado un semigrupo numérico $S = \langle a_1, ..., a_k\rangle$, se tiene*

$$n(S) \leq \frac{1}{k!a_1...a_k}\prod_{j=1}^{k}\left(f(S)+\sum_{i\neq j}a_i\right)$$

Corolario 1.2 *Dado un semigrupo numérico $S = \langle a_1, ..., a_k\rangle$, se tiene*

$$n(S) \leq \frac{(2f(S))^k}{k!a_1...a_k}.$$

En efecto, hemos probado un resultado en cierto sentido contrario al propuesto por Wilf, pues éste nos daba un mínimo para $n(S)$ y nosotros hemos probado una cota superior para éste en función de:

- k, que es una cota superior de la dimensión (aunque podemos suponer de partida que es efectivamente $e(S)$).
- $f(S)$.
- Los generadores de S.

Observación 1.5 *Como curiosidad, notemos que si hacemos $k = 2$, en la proposición obtenemos*

$$n(S) \leq \frac{1}{2a_1a_2}\left(a_1a_2 - a_1\right)\left(a_1a_2 - a_2\right) = \frac{(a_1-1)(a_2-1)}{2} = n(S),$$

por la fórmula de Sylvester. Así pues, en el caso $n = 2$ (donde curiosamente no podemos aplicar el razonamiento anterior, pues la Conjetura GLY es válida para $n \geq 3$), nuestra acotación es, de hecho, una igualdad.

Dimensión	Generadores	$f(S)$	$n(S)$	Cota	Cota/$n(S)$
3	$\{5, 6, 11\}$	19	8	19	$\simeq$ 2,375
3	$\{5, 6, 19\}$	14	5	10	$\simeq$ 2,000
3	$\{5, 7, 16\}$	18	8	14	$\simeq$ 1,750
3	$\{5, 7, 23\}$	18	7	13	$\simeq$ 1,857
3	$\{6, 9, 20\}$	43	21	44	$\simeq$ 2,095
3	$\{7, 9, 38\}$	40	18	28	$\simeq$ 1,555
3	$\{7, 9, 40\}$	38	16	26	$\simeq$ 1,625
3	$\{7, 9, 47\}$	40	17	28	$\simeq$ 1,647
3	$\{7, 48, 50\}$	143	62	94	$\simeq$ 1,516
3	$\{8, 9, 47\}$	46	20	31	$\simeq$ 1,550
3	$\{8, 9, 55\}$	47	20	32	$\simeq$ 1,600
3	$\{9, 10, 53\}$	61	28	42	$\simeq$ 1,500

Dimensión	Generadores	$f(S)$	$n(S)$	Cota	Cota/$n(S)$
4	$\{7, 11, 34, 37\}$	38	14	50	$\simeq$ 3,571
4	$\{7, 11, 23, 24\}$	27	8	31	$\simeq$ 3,875
4	$\{7, 11, 23, 17\}$	31	11	38	$\simeq$ 3,454
4	$\{11, 25, 37, 56\}$	101	40	110	$\simeq$ 2,750
4	$\{11, 25, 37, 115\}$	104	42	120	$\simeq$ 2,857
4	$\{11, 25, 37, 104\}$	101	40	111	$\simeq$ 2,775
4	$\{9, 13, 19, 21\}$	33	10	35	$\simeq$ 3,500
4	$\{9, 10, 21, 35\}$	43	18	59	$\simeq$ 3,277
4	$\{8, 11, 13, 15\}$	25	8	31	$\simeq$ 3,875
4	$\{13, 15, 31, 63\}$	81	34	94	$\simeq$ 2,764
4	$\{13, 16, 33, 56\}$	86	34	98	$\simeq$ 2,882
4	$\{13, 15, 31, 63\}$	81	34	94	$\simeq$ 2,764

Dimensión	Generadores	$f(S)$	$n(S)$	Cota	Cota/$n(S)$
5	$\{7, 11, 31, 34, 37\}$	30	9	86	$\simeq$ 9,555
5	$\{7, 15, 18, 26, 34\}$	38	17	112	$\simeq$ 6,588
5	$\{9, 10, 21, 35, 43\}$	34	11	99	$\simeq$ 9,000
5	$\{10, 19, 31, 37, 54\}$	65	25	154	$\simeq$ 6,160
5	$\{8, 11, 13, 15, 20\}$	25	11	72	$\simeq$ 6,545
5	$\{8, 11, 13, 15, 25\}$	20	6	53	$\simeq$ 8,833
6	$\{10, 19, 31, 37, 54, 65\}$	63	24	366	$\simeq$ 15,250
6	$\{10, 19, 31, 37, 54, 63\}$	65	26	382	$\simeq$ 14,692

Observación 1.6 *En estas tablas se pueden encontrar algunos ejemplos de semigrupos numéricos, con información relevante acerca del resultado anterior.*

Como es obvio, la cota se vuelve menos precisa conforme crece la dimensión del semigrupo. Un número significativo de ejemplos podrían resultar de ayuda a la hora de establecer una conjetura que mejore este resultado.

Trataremos ahora una nueva estrategia, basada en las mismas técnicas, pero utilizando la versatilidad de las bases de Groebner a nuestra disposición. Consideremos en esta ocasión el orden de eliminación para la variable x dado por

$$x > y_k > ... > y_2 > y_1.$$

Fijamos $\alpha \in \mathbb{Z}_{\geq 0}$ y consideramos

$$n(S, \alpha) = \sharp \{x \in S \mid x \leq \alpha\}.$$

En particular, $n(S, f(S)) = n(S)$. Tenemos entonces, exactamente igual que antes,

$$n(S, \alpha) = \sharp \left\{ Y = (y_1, ..., y_k) \in \mathbb{Z}_{\geq 0}^k \;\middle|\; y_i \geq 0,\ \sum a_i y_i \leq \alpha,\ Y \notin \left[\bigcup_i K_{q_i} \right] \right\}$$

Para ahorrar notación notaremos, sin especificar la biyección $\mathcal{G}$, por $N(S, \alpha)$ al conjunto anterior, cuyo cardinal se notará $n(S, \alpha)$. Tengamos en cuenta que

$$Y = (y_1, ..., y_k) \in N(S, \alpha) \implies 0 \leq y_1 \leq \frac{\alpha}{a_1}$$

Caso (1): $\alpha \geq a_1 a_2$. Resolveremos primero este caso, que es algo más complejo, desde el punto de vista de nuestra estrategia. Vamos a acotar el conjunto $N(S,\alpha)$ en dos etapas:

- Primero construiremos un prisma truncado C con base en un $(k-1)$–hipercubo, el cual contendrá a todos los puntos de $N(S,\alpha)$ que verifiquen $0 \leq y_1 \leq f(S,\alpha)/a_1 - a_2$.
- Una vez hecho esto, construiremos una pirámide D que contendrá el resto de los puntos enteros de $N(S,\alpha)$, y calcularemos sin demasiada dificultad el número de puntos enteros dentro de esta pirámide.

Comencemos por construir C. Notemos para empezar que los binomios $y_i^{a_1} - y_1^{a_i} \in I$, para todo $i = 2, ..., k$. Dado que sus exponentes son, precisamente,

$$(0, ..., 0, \overset{(i)}{a_1}, 0, ..., 0) \in \mathbb{Z}^k_{\geq 0},$$

tenemos que

$$(0, ..., 0, \overset{(i)}{a_1}, 0, ..., 0) \in \left[\bigcup_i K_{q_i}\right] \subset \mathbb{Z}^k_{\geq 0}.$$

y por consiguiente

$$\begin{aligned} N(S,\alpha) &= \left\{(y_1, ..., y_k) \in \mathbb{Z}^k_{\geq 0} \;\middle|\; y_i \geq 0,\ \sum a_i y_i \leq \alpha,\ Y \notin \left[\bigcup_i K_{q_i}\right]\right\} \\ &\subset \left\{(y_1, ..., y_k) \in \mathbb{Z}^k_{\geq 0} \mid 0 \leq y_i < a_1,\ \text{for } i = 2, ..., k\right\} = C_0, \end{aligned}$$

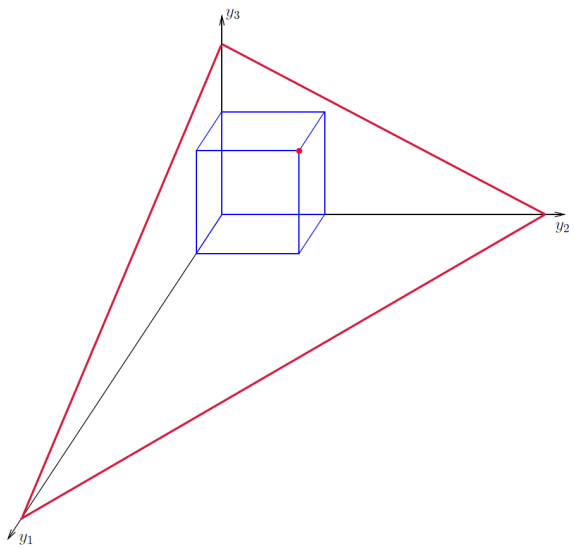
el cual es claramente un prisma con base en un $(k-1)$–hipercubo.

Esta cota por sí sola podría extenderse para adapatarse a todo $N(S)$, pero trataremos de ser algo más finos. Primero, calcularemos el punto en el cual C_0 *toca la pared* definida por

$$a_1 y_1 + ... + a_k y_k = \alpha.$$

Si hacemos $y_2 = ... = y_k = a_1$, es claro que la frontera entera de C_0 y el hiperplano se intersectan en el punto

$$R_0 = \left(\frac{\alpha}{a_1} - \sum_{i=2}^{k} a_i, a_1, ..., a_1\right).$$



Si hacemos $y_2 = ... = y_k = a_1$, es claro que la frontera entera de C_0 y el hiperplano se intersectan en el punto

$$R_0 = \left(\frac{\alpha}{a_1} - \sum_{i=2}^{k} a_i, a_1, ..., a_1 \right).$$

Para construir una pirámide con la que sea sencillo trabajar, vamos a considerar un subconjunto mayor de C_0 antes de truncarlo, de forma que en la práctica nos vamos a salir de $N(S)$. Concretamente, nos extenderemos hasta el punto

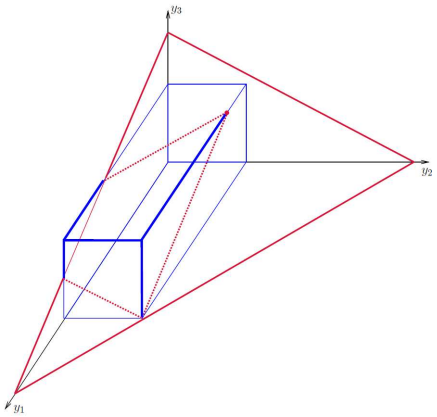
$$R_1 = \left(\frac{\alpha}{a_1} - a_2, a_1, ..., a_1 \right).$$

Así que, hasta ahora, lo que tenemos es que

$$N(S) \bigcap \left\{ y_1 \leq \frac{\alpha}{a_1} - a_2 \right\}$$

está contenido en el prisma truncado definido por

$$C = \left\{ (y_1, ..., y_k) \in \mathbb{Z}^k_{\geq 0} \mid y_1 \leq \frac{\alpha}{a_1} - a_2,\ y_i < a_1 \text{ for } i = 2, ..., k \right\}$$



Construyamos entonces la pirámide D, la cual tendrá como base un $(k-1)$–convexo sobre el hiperplano

$$y_1 = \frac{\alpha}{a_1} - a_2,$$

y su vértice en

$$V = \left(\frac{\alpha}{a_1}, 0, ..., 0\right).$$

La descripción precisa es

$$D = \left\{ V + \lambda_1 \left(-a_2, 0, ..., 0\right) + \sum_{i=2}^{k} \lambda_1 \lambda_i \left(0, ..., 0, \overset{(i)}{a_1}, 0, ..., 0\right) \;\middle|\; 0 \leq \lambda_i \leq 1,\ i = 1, ..., k \right\}.$$

Lema 1.6 *En las condiciones anteriores, se tiene que*

$$N(S, \alpha) \bigcap \left\{ y_1 \geq \frac{\alpha}{a_1} - a_2 \right\} \subset D.$$

Demostración: Tomamos un punto $Y = (y_1, ..., y_k) \in N(S)$, de forma que

$$\frac{\alpha}{a_1} - a_2 \leq y_1 \leq \frac{\alpha}{a_1},$$

y escribamos

$$y_1 = \frac{\alpha}{a_1} - \lambda_1 a_2 \implies \lambda_1 = \frac{\alpha/a_1 - y_1}{a_2},$$

lo cual claramente implica que $0 \leq \lambda_1 \leq 1$. Obviamente, tenemos que definir

$$\lambda_i = \frac{y_i}{\lambda_1 a_1}, \text{ for } i = 2, ..., k;$$

para poder escribir P como hemos hecho en la definición de D.

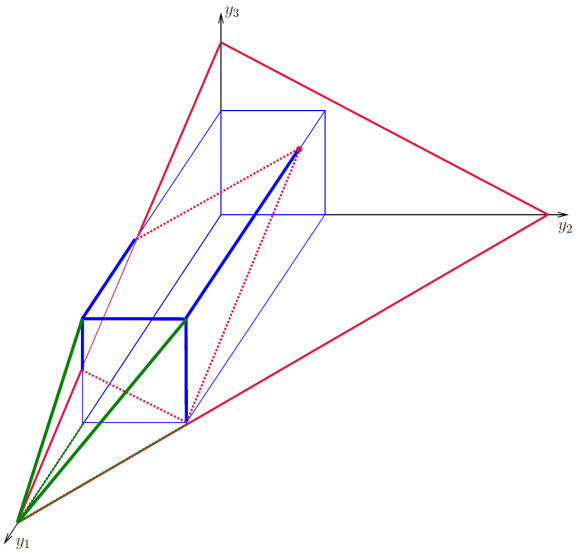
Es inmediato ver que $\lambda_i \geq 0$. Por otro lado tenemos que, como P está en $N(S, \alpha)$,

$$\alpha \geq a_1 y_1 + ... + a_k y_k = \alpha - \lambda_1 a_1 a_2 + \sum_{i=2}^{k} a_i y_i$$

y por tanto, para $i = 2, ..., k$;

$$a_i y_i \leq a_2 y_2 + ... + a_k y_k \leq \lambda_1 a_1 a_2 \leq \lambda_1 a_1 a_i,$$

lo cual implica que $y_i \leq \lambda_1 a_1$ y a su vez que $\lambda_i \leq 1$, para $i = 2, ..., k$. ■



Por tanto hemos demostrado:

Proposición 1.3 *En las condiciones anteriores,* $N(S, \alpha) \subset C \cup D$.

Corolario 1.3 *Con las definiciones anteriores,* $n(S, \alpha) \leq \sharp \left(C \cup D \cap \mathbb{Z}^k_{\geq 0} \right)$.

El número de puntos enteros de C es sencillo de calcular:

$$\sharp\left(C \cap \mathbb{Z}^k_{\geq 0}\right) = a_1^{k-1}\left(\left\lfloor \frac{\alpha}{a_1} - a_2 \right\rfloor + 1\right)$$

Si a_1 no es divisor de α, podemos expresar lo anterior de forma alternativa como:

$$\sharp\left(C \cap \mathbb{Z}^k_{\geq 0}\right) = a_1^{k-1}\left(\left\lceil \frac{\alpha}{a_1} \right\rceil - a_2\right).$$

Para encontrar el número de puntos enteros en D, fijamos nuestra atención en un nivel y_1–constante de la pirámide. Esto es, fijemos λ_1 tal que verifique

$$\frac{\alpha}{a_1} - \lambda_1 a_2 \in \mathbb{Z},$$

y entonces el conjunto

$$D \bigcap \left\{ y_1 = \frac{\alpha}{a_1} - \lambda_1 a_2 \right\} \bigcap \mathbb{Z}^k_{\geq 0}$$

es, una vez más, un $(k-1)$–hipercubo determinado por los vértices

$$\lambda_1(0, ..., 0, \overset{(i)}{a_1}, 0, ..., 0) \text{ para } i = 2, ..., k;$$

y por lo tanto tiene exactamente $(\lfloor \lambda_1 a_1 \rfloor + 1)^{k-1}$ puntos enteros.

Por tanto, lo que resta es describir de una forma lo más precisa posible el conjunto de los λ_1 que verifiquen

$$\frac{\alpha}{a_1} - \lambda_1 a_2 \in \mathbb{Z}.$$

Debe haber un $\lambda \in \mathbb{Z}$ de tal forma que

$$\frac{\alpha}{a_1} - \lambda_1 a_2 = \left\lfloor \frac{\alpha}{a_1} \right\rfloor - \lambda,$$

y este λ debe verificar $0 \leq \lambda \leq a_2 - 1$, para que se cumpla que

$$\alpha/a_1 - a_2 \leq y_1 \leq \alpha/a_1.$$

Como se tiene que

$$\lambda_1 = \frac{\lambda + \alpha/a_1 - \lfloor \alpha/a_1 \rfloor}{a_2} = \frac{\lambda + \{\alpha/a_1\}}{a_2},$$

es inmediato que el número de puntos en el nivel de la pirámide determinado por λ es

$$\sharp\left(D\bigcap\left\{y_1=\left\lfloor\frac{\alpha}{a_1}\right\rfloor-\lambda\right\}\bigcap\mathbb{Z}^k_{\geq 0}\right)=\left(\left\lfloor a_1\cdot\frac{\lambda+\{\alpha/a_1\}}{a_2}\right\rfloor+1\right)^{k-1}$$

y

$$\sharp\left(D\bigcap\mathbb{Z}^k_{\geq 0}\right)=\sum_{\lambda=0}^{a_2-1}\left(\left\lfloor a_1\cdot\frac{\lambda+\{\alpha/a_1\}}{a_2}\right\rfloor+1\right)^{k-1}$$

Teorema 1.4 *Sea $S=\langle a_1,...,a_k\rangle$ un semigrupo numérico, $\alpha\geq a_1a_2$ un entero. Entonces*

$$n(S,\alpha)\leq a_1^{k-1}\left(\left\lceil\frac{\alpha}{a_1}\right\rceil-a_2\right)+\sum_{\lambda=0}^{a_2-1}\left(\left\lfloor a_1\cdot\frac{\lambda+\{\alpha/a_1\}}{a_2}\right\rfloor+1\right)^{k-1}.$$

Corolario 1.4 *Sea $S=\langle a_1,...,a_k\rangle$ un semigrupo numérico. Entonces*

$$n(S,\alpha)\leq a_1^{k-1}\left\lfloor\frac{\alpha}{a_1}\right\rfloor$$

Demostración: Para verlo de forma directa, extiéndase el prisma C hasta $y_1=f(S)/a_1$. Indirectamente, dado que $0\leq\lambda\leq a_2-1$ tenemos

$$\frac{\lambda+\{\alpha/a_1\}}{a_2}<1$$

y en consecuencia

$$\left\lfloor a_1\cdot\frac{\lambda+\{\alpha/a_1\}}{a_2}\right\rfloor+1\leq a_1$$

de donde

$$\sharp\left(D\bigcap\mathbb{Z}^k_{\geq 0}\right)\leq\sum_{\lambda=0}^{a_2-1}a^{k-1}$$

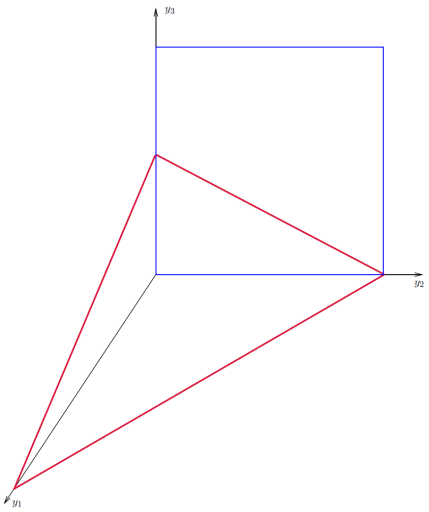
lo cual, para finalizar, nos lleva a que

$$n(S,\alpha)\leq a_1^{k-1}\left(\left\lceil\frac{\alpha}{a_1}\right\rceil-a_2\right)+(a_2-1)a_1^{k-1}=a_1^{k-1}\left\lfloor\frac{\alpha}{a_1}\right\rfloor,$$

como habíamos mencionado antes. ■

Caso (2): $\alpha \leq a_1 a_2$. Resolveremos ahora este caso. Geométricamente se corresponde con la situación en la cual, al construir el prisma, el $(k-1)$–hipercubo que nos sirve como base ya se sale de $N(S,\alpha)$. Podemos seguir construyendo, sin embargo, la pirámide D, aunque no podemos ser demasiado optimistas en esperar un resultado ajustado.

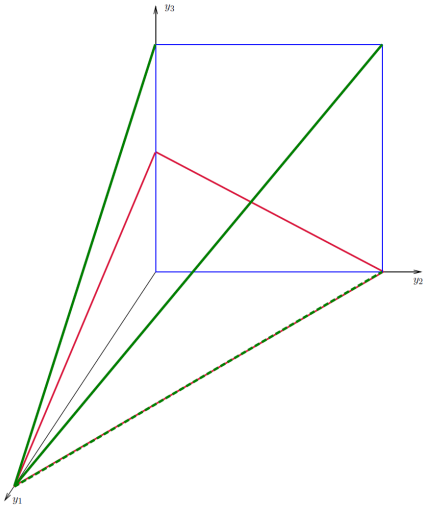
En este caso, es claro que podemos considerar que el $(k-1)$–hipercubo en el plano $y_1 = 0$ forma una cuadrado de longitud α/a_2.



Sin entrar a repetir todos los detalles simétricos con el caso anterior, mencionemos que la pirámide viene ahora dada por

$$V = \left(\frac{\alpha}{a_1}, 0, ..., 0\right),$$

$$D = \left\{ V + \lambda_1 \left(-\frac{\alpha}{a_1}, 0, ..., 0\right) + \sum_{i=2}^{k} \lambda_1 \lambda_i (0, ..., 0, \overset{(i)}{\frac{\alpha}{a_2}}, 0, ..., 0) \;\middle|\; 0 \leq \lambda_i \leq 1,\ i = 1, ..., k \right\}.$$



En este caso, simplemente consideramos un cierto $\lambda \in \mathbb{Z}$ tal que

$$0 \leq \lambda \leq \left\lfloor \frac{\alpha}{a_1} \right\rfloor,$$

el cual determina como antes un nivel y_1–constante que es de nuevo un $(k-1)$–hipercubo, en este caso definido por los puntos

$$\left(\lambda, ..., 0, \overset{(i)}{\frac{\alpha - \lambda a_1}{a_2}}, 0, ..., 0 \right), \text{ for } i = 2, ..., n.$$

El resultado equivalente al anterior se deduce sumando la cantidad de puntos enteros que aporta cada nivel y_1–constante.

Teorema 1.5 *Sea $S = \langle a_1, ..., a_k \rangle$ un semigrupo numérico, $0 \leq \alpha \leq a_1 a_2$ un entero. Entonces*

$$n(S, \alpha) \leq \sum_{\lambda=0}^{\lfloor \alpha/a_1 \rfloor} \left(\left\lfloor \frac{\alpha - \lambda a_1}{a_2} \right\rfloor + 1 \right)^{k-1}.$$

Corolario 1.5 *En las condiciones anteriores*

$$n(S) \leq \sum_{\lambda=0}^{a_2} \left(\left\lfloor a_1 \cdot \frac{a_2 - \lambda}{a_2} \right\rfloor + 1 \right)^{k-1} + f(S) - a_1 a_2.$$

Demostración: Dado que $a_1a_2 \geq f(S)$, podemos tomar $\alpha = a_1a_2$ y tenemos que

$$n(S, a_1a_2) = a_1a_2 - f(S) + n(S).$$

■

CAPÍTULO 2

Un algoritmo para el cálculo del conjunto de Apéry

2.1 El conjunto de Apéry.

El conjunto de Apéry (los conjuntos, para ser precisos) es una herramienta de enorme utilidad a la hora de estudiar los semigrupos numéricos. La idea que dio lugar a dicho conjunto, surgió por vez primera de la mano de Roger Apéry [2], matemático francés de origen griego que desarrolló gran parte de su carrera en la universidad de Caen.

Roger Apéry es recordado hoy principalmente, no por sus aportaciones en el campo de semigrupos numéricos, sino por el trabajo desarrollado en Teoría de Números, en particular su famoso *Teorema de Apéry* [30], donde demuestra que la función zeta de Riemann $\zeta(3)$ es irracional. Dicho valor se conoce como constante de Apéry. La cual nada tiene que ver con los semigrupos numéricos ni con el conjunto que trataremos en este capítulo.

Respecto a lo que nos atañe, en relación a semigrupos numéricos, la idea que utilizó por primera vez Apéry, y que dio lugar al conjunto que lleva su nombre, parte de que dos generadores minimales de un semigrupo numérico no pueden ser congruentes módulo la multiplicidad, y en particular lo mismo ocurre con respecto a cualquier elemento no nulo del semigrupo. Basándonos

en esta idea, podemos definir el conjunto de Apéry.

Definición 2.1 *Sea S un semigrupo numérico y consideremos un elemento de éste, $s \in S$. Definimos el conjunto de Apéry asociado al elemento s, y notaremos como $Ap(S, s)$ al siguiente conjunto*

$$\{0, w_0, ..., w_{s-1}\}$$

donde w_i es el menor elemento en S congruente con i módulo s.

Si s es la multiplicidad de S, a este conjunto se le suele llamar base estándar de S.

Lema 2.1 *Se tiene, en las condiciones anteriores, que*

$$Ap(S, s) = \{x \in S \mid x - s \notin S\}$$

Demostración: Si tomamos un elemento $w_i \in Ap(S, s)$, éste es el menor elemento de S que es congruente con i módulo s. Entonces es obvio que el elemento $w_i - s$ también es congruente con i modulo s, y por minimalidad este elemento no pertenecerá a S. La otra inclusión es análoga. ■

Ejemplo 2.1 *Veamos en primer lugar un ejemplo sencillo, de un semigrupo de dos generadores. Sea $S = \langle 4, 7\rangle$. Su conjunto de Apéry asociado al primer generador, sería;*

$$Ap(S, 4) = \{0, 7, 14, 21\}$$

Ejemplo 2.2 *Tomemos ahora un semigrupo numérico con más elementos. Sea $S = \langle 7, 9, 11, 15\rangle$. Algunos de los conjuntos de Apéry asociados a sus generadores son:*

$$Ap(S, 7) = \{0,\ 9,\ 11,\ 15,\ 20,\ 24,\ 26\}$$

$$Ap(S, 15) = \{0,\ 7,\ 9,\ 11,\ 14,\ 16,\ 18,\ 20,\ 21,\ 23,\ 25,\ 27,\ 28,\ 32,\ 34\}$$

En particular, para los semigrupos numéricos con dos generadores, los conjuntos de Apéry asociados a los generadores están totalmente identificados.

Lema 2.2 *Sea S el semigrupo generado por a_1 y a_2, ambos enteros. Entonces:*

$$Ap(S, a_i) = \{0,\ a_j,\ 2a_j, ...,\ (a_i - 1)a_j\}$$

Demostración: Sea $S = \langle a_1, a_2 \rangle$, sabemos que el conjunto de Apéry es el siguiente:

$$Ap(S, a_i) = \{w_0, ..., w_{a_i - 1}\}$$

para $i = 1, 2$ donde w_j es el menor elemento de S congruente con j módulo a_i.

Demostremos el resultado para $a_i = a_1$, ya que ambas pruebas son simétricas. Tomemos un elemento w_i cualquiera del conjunto $Ap(S, a_1)$ y veamos qué forma tiene.

Como w_i está en S existirá algún $(\alpha, \beta) \in \mathbb{Z}^2_{\geq 0}$ tal que

$$w_i = \alpha a_1 + \beta a_2.$$

Usando esta misma expresión se sigue que

$$w_i - a_1 = \alpha a_1 + \beta a_2 - a_1 = (\alpha - 1)a_1 + \beta a_2.$$

Pero sin embargo $w_i - a_1$ no está en el semigrupo por la propia definición de los elementos del conjunto de Apéry $Ap(S, a_1)$. Por lo tanto para que la expresión anterior no nos de una representación válida del número $w_i - a_1 \in G(S)$, $\alpha - 1$ tendría que ser un entero no positivo, en cuyo caso el único valor válido para α sería $\alpha = 0$.

Así, todos los elementos del conjunto de Apéry $Ap(S, a_1)$ son de la forma $w_i = \beta a_2$ con $\beta \in \mathbb{Z}_{\geq 0}$. Es más, podemos asegurar que

$$\beta \in \{1,\ 2, ...,\ a_1 - 1\}.$$

Veamos por qué. El mayor elemento del conjunto de Apéry $Ap(S, a_1)$ puede de ser, a lo más $F(S) + a_1$. En un semigrupo con dos generadores, por la fórmula de Sylvester [29], $F(S) = (a_1 - 1)(a_2 - 1)$. De modo que cualquier elemento $w_i \in Ap(S, a_1)$ debe verificar

$$w_i \leq (a_1 a_2 - a_1 - a_2) + a_1 = a_1 a_2 - a_2,$$

como queríamos probar. ■

Definición 2.2 *Definimos el orden parcial $\leq_S$ en un semigrupo numérico S, de la siguiente forma:*

$$x \leq_S y \iff y - x \in S.$$

Definición 2.3 *Sea S un semigrupo numérico. Decimos que un elemento $x \in \mathbb{Z}$ es un pseudo–número de Frobenius de S si:*

- $x \notin S$.
- $x + s \in S$ *para todo* $s \in S \setminus \{0\}$.

El conjunto de pseudo–números de Frobenius lo denotaremos como $PF(S)$ y a su cardinal que llamamos tipo de S, lo denotaremos como $t(S)$.

Observación.– Está claro que $f(S) \in PF(S)$ siempre. Los casos en los que $PF(S)$ es un conjunto unitario forman una familia de semigrupos muy estudiada y de especial relevancia.

Definición 2.4 *Un semigrupo numérico se dice que es simétrico cuando $t(S) = 1$, es decir el único elemento del conjunto $PF(S)$ es el número de Frobenius.*

Los semigrupos simétricos han sido estudiados con mucho detalle. Nosotros volveremos sobre ellos en la última sección de este capítulo.

La siguiente proposición explora algunas de las propiedades básicas del conjunto de Apéry, $Ap(S, s)$.

Proposición 2.1 *Sea S un semigrupo numérico $s \in S$. Se tiene:*

1. *Todo entero n se puede expresar de forma única como $n = ks + w_i$, para algún $k \in \mathbb{Z}$ y algún $w_i \in Ap(S, s)$. Además, $n \in S$ si y sólo si $k \geq 0$.*
2. *$w_i + w_j = w_{(i+j)} + ks$ para algún $k \geq 0$ y $w_i, w_j \in Ap(S, s)$.*
3. *Si $s_1, s_2 \in S$ y $s_1 + s_2 \in Ap(S, s)$, entonces $s_1, s_2 \in Ap(S, s)$.*
4. *$w_i - w_j = w_{(i-j)} + ks$ para algún $k \leq 0$ y $w_i, w_j \in Ap(S, s)$.*
5. *$f(S) = \text{máx}\big\{Ap(S, s) - s\big\}$.*

Demostración:

1. Sea n un entero cualquiera y sea $i \in \{0, 1, ..., s-1\}$ tal que n es congruente con i módulo s. Existe por tanto por cada i un único $w_i \in Ap(S, s)$ congruente también con i módulo s, siendo el menor elemento de S cumpliendo dicha propiedad. Por ser ambos números congruentes con i módulo s existe un entero k tal que podemos escribir $n = w_i + ks$.

   Si $k < 0$, en este caso w_i sería mayor que n, por lo que por la propia definición de w_i que es el menor elemento de S congruente con i, n no pertenecería al semigrupo. Si por el contrario $k \geq 0$ entonces n está en el semigrupo por construcción, ya que w_i y ks están en el semigrupo.

   Esta propiedad nos da una forma de saber si un elemento está en el semigrupo de forma que, si s pertenece a S, buscamos $w_i \in Ap(S, n)$ tal que $s \equiv w_i \mod n$ y entonces $s \in S$ si y sólo si $w_i \leq s$.

2. Nótese que
$$w_i + w_j \equiv i + j \mod m$$
   y $w_i + w_j \in S$ entonces S es cerrado para la suma. A partir de aquí, usando la primera propiedad, se obtiene lo que buscábamos demostrar.

3. Para demostrar esta propiedad usaremos la reducción al absurdo. Sean $s, s_1, s_2 \in S$ y supongamos que ni s_1 ni s_2 están en $Ap(S, s)$. Por la primera propiedad de esta proposición sabemos que
$$s_1 = k_1 s + w_i \text{ y que } s_2 = k_2 s + w_j$$
   con $k_1, k_2 \geq 0$ ya que ambos están en S. Por lo que usando esta expresión de s_1 y de s_2, tenemos que
$$s_1 + s_2 = k_1 s + w_i + k_2 s + w_j = w_{(i+j)} + (k_1 + k_2)s + ks,$$
   con $k \geq 0$.

   Teniendo de esta forma que
$$s_1 + s_2 = w_{(i+j)} + (k_1 + k_2 + k)s, \text{ con } k_1 + k_2 + k \geq 0,$$
   por lo que $s_1 + s_2 \notin Ap(S, s)$, contradiciendo una de las hipótesis de las que partíamos.

4. Para demostrar esta propiedad, consideremos $w_{(i-j)} + w_j$. Usando la segunda propiedad tenemos

$$w_{(i-j)} + w_j = w_{(i-j+j)} + k's = w_i + k's,$$

con $k' \geq 0$, para algún $s \in S$. Despejando tenemos que

$$w_i - w_j = w_{(i-j)} - k's,$$

llamando $k = k'$ tenemos que

$$w_i - w_j = w_{(i-j)} + ks \text{ con } k \leq 0,$$

como queríamos demostrar.

5. Esto es inmediato, ya que obviamente por definición el número de Frobenius es el mayor del conjunto de los gaps, y por tanto el mismo nos dará el máximo del conjunto de Apéry.

■

Generalizando lo anterior, podemos demostrar el siguiente resultado.

Proposición 2.2 *Un entero $g \in \mathbb{Z}$ es un pseudo–número de Frobenius de S si y sólo si para cualquier $n \in S$, se tiene que $g + n$ es maximal en $Ap(S, n)$ con respecto a $\leq_S$.*

Así

$$t(S) = \sharp \left(\bigcup_{n \in S} \left\{ \max_{\leq_S}(Ap(S, n)) \right\} \right).$$

Demostración: Vamos a demostrar en primer lugar que si $g \in PF(S)$, entonces $g + n$ es maximal en el conjunto $Ap(S, n)$ para cualquier $n \in S$. Si g es un pseudo–número de Frobenius, entonces por definición sabemos que $x \notin S$ y $x + s \in S$ para todo s de S.

Fijemos entonces $n \in S$. En particular $g + n \in S$ y por construcción $g + n \in Ap(S, n)$. Veamos ahora que este elemento $g + n$ es además maximal en el conjunto $Ap(S, n)$ con respecto al orden $\leq_S$.

Supongamos que existe un elemento $w \in Ap(S, n)$ tal que $g + n \leq_S w$, entonces

$$w - (g + n) = w - g - n \in S,$$

por lo que existirá un elemento $s \in S$, tal que podemos escribir

$$w - g - n = s,$$

de donde $w - n = g + s$. Pero como $w \in Ap(S, n)$, sabemos que $w - n \notin S$, por tanto $g + s \notin S$. Por lo que la única forma de que se cumpla sería que $s = 0$, y por tanto $w = g + n$.

Veamos ahora la implicación recíproca. Supongamos que $g+n$ es maximal en el conjunto $Ap(S, n)$ con respecto al orden $\leq_S$, y probemos que $g \in PF(S)$. Sabemos que al ser $g + n$ un elemento de $Ap(S, n)$,

$$g + n \in S, \qquad (g + n) - n = g \notin S.$$

Supongamos en estas condiciones, que g no es un pseudo–número de Frobenius. Entonces existe un $s \in S$ con $s \neq 0$ tal que $g + s \notin S$.

Por otro lado, sabemos que $g + n$ es maximal en $Ap(S, n)$ con respecto al orden $\leq_S$. Por lo que para todo elemento w en $Ap(S, n)$ se tiene que $g + n - w \in S$.

Como hemos supuesto que $g+s \notin S$ para algún $s \in S$ con $s \neq 0$, entonces $g + n + s \in Ap(S, n)$ (ya que $g + n + s \in S$).

Pero $g + n + s \geq_S g + s$ porque

$$g + n + s - (g + s) = n \in S$$

lo que contradice la maximalidad de $g + n$ con respecto al orden $\leq_S$ en el conjunto $Ap(S, n)$. ■

El conjunto de Apéry determina completamente numerosos invariantes del semigrupo, como es el número de Frobenius, el género o el tipo.

Proposición (Fórmula de Selmer).– Sea S un semigrupo numérico, $a \in S$. Entonces

$$g(S) = \frac{1}{a} \sum_{w \in Ap(S,a)} w + \frac{a-1}{2}.$$

Demostración: Sea el conjunto de gaps del semigrupo S:

$$G(S) = \{g_1, ..., g_k\}.$$

Definimos, dado $a \in S$, el conjunto siguiente:

$$G_a(S) = \{g_1 + a, ..., g_k + a\}$$

De este conjunto se podría construir el conjunto de Apéry del elemento a, ya que

$$Ap(S,a) = G_a(S) \cap S.$$

Sea $g_{j_1} + a \in G_a(S)$ un elemento del conjunto anterior. Pueden ocurrir dos cosas:

1. $g_{j_1} + a \in S$, con lo que existiría un $w_i \in Ap(S,a)$ tal que $g_{j_1} + a = w_i$. Y obviamente
$$g_{j_1} \equiv w_i \equiv i \mod a.$$

2. $g_{j_1} + a \notin S$, con lo que existirá un $g_{j_2} \in G(S)$ tal que $g_{j_1} + a = g_{j_2}$. Además existirá $w_i \in Ap(S,a)$ tal que
$$g_{j_2} = g_{j_1} + a \equiv w_i \equiv i \mod a.$$
Dentro de este caso, a su vez, puede darse dos casos: que $g_{j_2} + a \in S$, que al igual que en el primer caso, significaría que $g_{j_2} + a = w_i$, que $g_{j_2} + a \notin S$, y podríamos volver a razonar como en el segundo caso.

De esta forma, y razonando de manera recurrente, podemos llegar a que para cada $w_i \in Ap(S,a)$, existen $g_{j_1} \leq ... \leq g_{j_{p_i}}$ tales que:

$$g_{j_1} \equiv g_{j_2} \equiv ... \equiv g_{j_{p_i}} \equiv w_i \equiv i \mod a,$$

para cierto $p_i \in \mathbb{Z}$ y además:

$$w_i = g_{j_{p_i}} + a = (g_{j_{p_i-1}} + a) + a = ... = g_{j_1} + p_i a.$$

Con lo que si queremos contar el número de gaps, tenemos que calcular el p_i para cada w_i elemento de $Ap(S,a)$,, ya que para todo $g_j \in G(S)$ existe un único $i \in \{0, ..., a-1\}$ tal que

$$g_j + a \equiv i \mod a,$$

con lo que sabemos que

$$n(S) = \sum_{i=0}^{a-1} p_i.$$

En realidad lo que estamos haciendo no es sino distribuir los elementos de $G(S)$ en función de su congruencia módulo a. Notemos, en este sentido,

que bien podría suceder que $p_i = 0$. Así mismo debemos tener siempre que $g_{j_1} < a$ puesto que de otro modo, $g_{j_1} \mod a$ estaría en S y eso implicaría directamente que $g_{j_1} \in S$.

Escribimos entonces

$$w_i = g_{j_1} + ap_i \implies \left\lfloor \frac{w_i}{a} \right\rfloor = p_i + \left\lfloor \frac{g_{j_1}}{a} \right\rfloor = p_i.$$

Así pues,

$$n(S) = \sum_{i=0}^{a-1} p_i = \sum_{i=0}^{a-1} \left\lfloor \frac{w_i}{a} \right\rfloor.$$

Como

$$w_i = a \left\lfloor \frac{w_i}{a} \right\rfloor + i,$$

entonces tenemos que

$$\left\lfloor \frac{w_i}{a} \right\rfloor = \frac{w_i - i}{a},$$

y así

$$\begin{aligned} n(S) = \sum_{i=0}^{a-1} \frac{w_i - i}{a} &= \frac{1}{a} \sum_{i=0}^{a-1} w_i - \frac{1}{a} \sum_{i=0}^{a-1} i \\ &= \frac{1}{a} \sum_{i=0}^{a-1} w_i - \frac{1}{a} \frac{(a-1)a}{2} = \frac{1}{a} \sum_{i=0}^{a-1} w_i + \frac{a-1}{2}, \end{aligned}$$

como queríamos probar. ∎

2.2 Un algoritmo para el cálculo del conjunto de Apéry

El conjunto de Apéry ha sido estudiado profusamente en la bibliografía relativa a semigrupos numéricos. Algunos ejemplos son [7, 8, 25, 20, 27]. En esta sección nos vamos a ocupar de su cálculo explícito, un asunto no tan tratado.

Teniendo determinado $G(S)$, la obtención del conjunto de Apéry se convierte en algo sencillo. Lo interesante, es justamente lo contrario; hallar el conjunto de Apéry para obtener información de un semigrupo numérico, del que a priori no tengamos suficiente información como para conocer $G(S)$.

En este capítulo vamos a dar un método para obtener el conjunto de Apéry de un semigrupo numérico a partir de sus generadores haciendo uso de las bases de Groebner.

Definición 2.5 *Sean $A = \{a_1, a_2, a_3, ..., a_k\}$ un conjunto de enteros positivos primos entre sí, de forma que $a_1 < a_2 < ... < a_k$, $S = \langle a_1, ..., a_k \rangle$, y consideramos el ideal binomial asociado al semigrupo S:*

$$I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, y_3 - x^{a_3}, ..., y_k - x^{a_k} \rangle \subset \mathbb{Q}[x, y_1, ..., y_k].$$

Sobre el anillo de polinomios $\mathbb{Q}[x, y_1, ..., y_k]$, definimos un orden de eliminación sobre la primera variable x como se describe a continuación y al cual notaremos por σ_j.

1. *En primer lugar ordenamos según el exponente de la primera variable, x.*
2. *En caso de igualdad en el criterio anterior, ordenamos según el orden graduado ponderando con los valores de los generadores, en las variables $y_1, ..., y_k$ exceptuando la variable y_j, es decir según*

$$\sum_{i=1, i \neq j}^{i=k} \alpha_i a_i,$$

   siendo α_i el exponente de la variable y_i.
3. *El siguiente orden a usar es el lexicográfico en las todas las variables y_i, para $i = 1, ..., k$ con $i \neq j$.*
4. *Como último criterio ordenamos según el valor del exponente de la variable y_j.*

La matriz asociada al orden[1] *σ_j sería:*

$$\begin{pmatrix} & & & & \overbrace{\quad} & & \\ & & & & ^{(j+1)} & & \\ 1 & 0 & 0 & ... & 0 & ... & 0 \\ 0 & a_1 & a_2 & ... & 0 & ... & a_k \\ 0 & 1 & 0 & ... & 0 & ... & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & ... & 0 & ... & 1 \\ 0 & 0 & 0 & ... & 1 & ... & 0 \end{pmatrix}$$

[1] Ver apéndice.

Observación.– Notaremos como $\mathcal{B}_j$ a la base de Groebner del ideal I, tomando el orden de eliminación σ_j, que hemos definido con anterioridad. Escribiremos $N_j(f)$ para notar la forma normal de f con respecto a la base de Groebner $\mathcal{B}_j$.

Teorema 2.1 *Sea $S = \langle a_1, ..., a_k \rangle$ un semigrupo numérico. Usando la notación anterior, consideremos el ideal I definido como antes, y su respectiva base de Groebner con el orden σ_j.*

Definimos el siguiente conjunto:

$$\Delta = \left\{ N \in \mathbb{Z}_{\geq 0} \mid exp\left(N_j\left(x^N\right)\right) \in \{x = y_j = 0\} \bigcap \overline{E(I)} \right\}$$

En las condiciones anteriores, se cumple que $\Delta = Ap(S, a_j)$.

Demostración: Probaremos esta igualdad usando la doble inclusión.

- $Ap(S, a_j) \subseteq \Delta$.

  Sea $n \in Ap(S, a_j)$. Por tanto $n \in S$ y $n > a_j$. Como n está en el semigrupo, entonces existen $x_1, ..., x_k \in \mathbb{Z}_{\geq 0}$ tales que

  $$n = \sum_{i=1}^{k} a_i x_i$$

  y además por estar en el conjunto de Apéry sabemos que $n - a_j \notin S$.

  Queremos probar entonces que

  $$exp\left(N_j\left(x^n\right)\right) \in \{x = 0\} \cap \{y_j = 0\}.$$

  Pero no es necesario probar que la forma normal está en $\{x = 0\}$ ya que al ser n un número representable su forma normal esta en dicho hiperplano. Por lo cual tenemos que probar que

  $$exp\left(N_j\left(x^n\right)\right) \in \{y_j = 0\}.$$

  Sea entonces $exp\left(N_j\left(x^n\right)\right) = (\gamma_1, \gamma_2, ..., \gamma_k)$.

  De la expresión anterior tenemos

  $$\begin{aligned} n - a_j &= a_1\gamma_1 + ... + a_j\gamma_j + ... + a_k\gamma_k - a_j \\ &= a_1\gamma_1 + ... + a_j(\gamma_j - 1)... + a_k\gamma_k. \end{aligned}$$

Pero como n está en $Ap(S, a_j)$, sabemos que $n - a_j \in G(S)$, por lo que la expresión anterior no puede ser una representación. Dado que $\gamma_i \in \mathbb{Z}_{\geq 0}$ para todo $i = 1, ..., k$; entonces $(\gamma_j - 1) \notin \mathbb{Z}_{\geq 0}$, o de lo contrario la expresión sería una representación.

Así pues, ha de ser $\gamma_j = 0$, que era lo que queríamos demostrar.

- Veamos ahora que $\Delta \subseteq Ap(S, a_j)$.

  Sea $n \in \Delta$. Entonces, por definición del conjunto Δ sabemos que $n \in S$ con $exp\left(N_j\left(x^n\right)\right) \in \{y_j = 0\} \cap \{x = 0\}$. Por lo que existen

  $$\gamma_1, ..., \gamma_{j-1}, \gamma_{j+1}, ..., \gamma_k \in \mathbb{Z}_{\geq 0},$$

  tales que

  $$N_j\left(x^n\right) = y_1^{\gamma_1} ... y_{j-1}^{\gamma_{j-1}} \cdot y_{j+1}^{\gamma_{j+1}} ... y_k^{\gamma_k}.$$

  Hay que probar que $n \in Ap(S, a_j)$. Para ello procedemos por reducción al absurdo y suponemos que $n \notin Ap(S, a_j)$. Por tanto tendríamos que, o bien $n \notin S$ (lo cual no puede ser porque $n \in \Delta$) o bien $n > a_j$ y además $n - a_j \in S$.

  Por tanto existirán $\alpha_1, ..., \alpha_k \in \mathbb{Z}_{\geq 0}$ tales que

  $$n - a_j = \sum_{i=1}^{k} a_i \alpha_i$$

  y despejando n de la expresión anterior:

  $$n = \sum_{i=1, i \neq j}^{k} a_i \alpha_i + a_j(\alpha_j + 1)$$

  Esto nos da otra representación para n, caracterizada por la n–upla $(\alpha_1, ..., (\alpha_j + 1), ..., \alpha_k) \in \mathbb{Z}_{\geq 0}^n$.

  Teniendo entonces la siguiente igualdad:

  $$a_1\gamma_1 + ... + a_{j-1}\gamma_{j-1} + a_{j+1}\gamma_{j+1} + ... + a_k\gamma_k =$$

  $$= a_1\alpha_1 + ... + a_j(\alpha_j + 1) + ... + a_k\alpha_k$$

De aquí deducimos que

$$\sum_{i=1,i\neq j}^{k} a_i(\alpha_i - \gamma_i) + a_j(\alpha_j + 1) = 0. \qquad (*)$$

Por otro lado, tenemos dos representaciones para n:

-) La que nos da su forma normal:

$$(\gamma_1, ..., \overbrace{0}^{(j)}, ..., \gamma_k)$$

-) La que nos da la representación de $n - a_j$:

$$(\alpha_1, ..., (\alpha_j + 1), ..., \alpha_k)$$

Por definición de forma normal, tenemos que

$$\begin{aligned} N_j(x^n) &= N_j\left(y_1^{\alpha_1} \cdot ... \cdot y_j^{\alpha_j+1} \cdot ... \cdot y_k^{\alpha_k}\right) \\ &= y_1^{\gamma_1} \cdot ... \cdot y_{j-1}^{\alpha_{j-1}} \cdot y_{j+1}^{\alpha_{j+1}} \cdot ... \cdot y_k^{\gamma_k} \end{aligned}$$

Usando el orden σ_j, sabemos que

$$(0, \gamma_1, ..., \overbrace{0}^{(j)}, ..., \gamma_k) <_{\sigma_j} (0, \alpha_1, \alpha_2, ..., \alpha_k)$$

Esto quiere decir que

$$\sum_{i=1,i\neq j}^{k} \gamma_i a_i \leq \sum_{i=1,i\neq j}^{k} \alpha_i a_i \implies \sum_{i=1,i\neq j}^{k} a_i(\alpha_i - \gamma_i) \geq 0.$$

Pero esto nos da una contradicción ya que en la expresión $(*)$ la primera parte de la suma es positiva y obviamente $a_j(\alpha_j+1)$ es también positivo. Por lo que la igualdad a cero solo podría darse en el caso de que ambos sumandos fueran nulos. Para ello a_j tendría que ser nulo, por lo que llegaríamos a una contradicción.

■

Observación 2.1 *A raíz de la proposición 2.2., este mismo procedimiento nos permite calcular el conjunto $PF(S)$.*

Para ello tomamos cualquier generador de $S = \langle a_1, ..., a_k \rangle$, hallamos $Ap(S, a_i)$ usando el algoritmo anterior y establecemos el orden parcial $\leq_S$. Restando a_i a los elementos maximales de $Ap(S, a_i)$ para $\leq_S$ obtendremos $PF(S)$.

Ejemplo 2.3 *Veamos un ejemplo con tres generadores de este resultado. Sea el semigrupo numérico $S = \langle 3, 7, 11 \rangle$. Definimos el ideal binomial asociado a dicho semigrupo.*

$$I = \left\langle y_1 - x^3, y_2 - x^7, y_3 - x^{11} \right\rangle \subset \mathbb{Q}[x, y_1, y_2, y_3],$$

y hallamos su base de Groebner con el orden σ_3, definido anteriormente obteniendo:

$$\begin{aligned} \mathcal{B}_3 \;=\; \{ & x^3 - y_1,\ x^2y_2 - y_1^3,\ xy_1y_2 - y_3,\ xy_1^2 - y_2,\ xy_3 - y_1^4, \\ & y_1^5y_2 - y_3^2,\ y_1^6 - y_2y_3,\ y_2^2 - y_1y_3 \}. \end{aligned}$$

El conjunto de Apéry asociado al tercer generador es:

$$Ap(S, 11) = \{0,\ 3,\ 6,\ 7,\ 9,\ 10,\ 12,\ 13,\ 15,\ 16,\ 19\}.$$

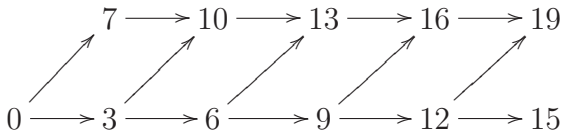
Hallamos el conjunto Δ y comprobaremos que ambos coinciden. Para ello representemos en el plano $\{x = 0\} \cap \{y_3 = 0\}$ los elementos del semigrupo y sombreamos en azul los enteros cuya representación coinciden con sus forma normal, que compondrán el conjunto Δ. En esta representación el conjunto de Apéry asociado al tercer generador son los elementos que aparecen en rojo.

x	y3	y1						
0	0	0	1	2	3	4	5	6
y2->	0	0	3	6	9	12	15	18
	1	7	10	13	16	19	22	25
	2	14	17	20	23	26	29	32
	3	21	24	27	30	33	36	39

Obteniendo

$$\Delta = \{0,\ 3,\ 6,\ 7,\ 9,\ 10,\ 12,\ 13,\ 15,\ 16,\ 19\}.$$

Si queremos calcular el conjunto $PF(S)$ podemos hacerlo como indicamos antes. El orden $\leq_S$ induce el siguiente diagrama en $Ap(S, 11)$ (una flecha de x a y indica $x \leq_S y$):



Por tanto los elementos maximales son $\{15,\ 19\}$ *y* $PF(S) = \{4,\ 8\}$.

Ejemplo 2.4 *Veamos otro ejemplo con tres generadores pero con otro orden. Sea* $S = \langle 9, 10, 31\rangle$ *y su correspondiente conjunto de Apéry asociado al segundo elemento:*

$$Ap(S, 10) = \{0,\ 9,\ 18,\ 27,\ 31,\ 36,\ 45,\ 54,\ 62,\ 63\}.$$

Tomamos el ideal

$$I = \left\langle y_1 - x^9, y_2 - x^{10}, y_3 - x^{31}\right\rangle \subset \mathbb{Q}[x, y_1, y_2, y_3],$$

y su base de Groebner respecto del orden σ_2

$$\begin{aligned}\mathcal{B}_2 \ = \ \{&x^9 - y_1,\ x^8y_2 - y_1^2,\ x^7y_2^2 - y_1^3,\ x^5y_3 - y_1^4,\ x^4y_2y_3 - y_1^5,\\ &x^3y_2^2y_3 - y_1^6,\ xy_2^2y_3^2 - y_1^7y_2^2,\ xy_2y_3^2 - y_1^7y_2,\ xy_3^2 - y_1^7,\\ &xy_1 - y_2,\ xy_2^8 - y_2^5y_3,\ xy_2^3 - y_3,\ y_2^5y_3^3 - y_1^7y_2^8,\ y_3^3 - y_1^7y_2^3,\\ &y_1^8y_2^8 - y_2^9y_3^2,\ y_1^8y_2^4 - y_2^5y_3^2,\ y_1^8y_2 - y_2^2y_3^2,\ y_1^8 - y_2y_3^2,\ y_1y_3 - y_2^4\}.\end{aligned}$$

Localicemos ahora los elementos de S *cuyas formas normales están en el plano* $\{x = 0\} \cap \{y_2 = 0\}$, *que son los elementos del conjunto* Δ. *Y los sombreamos en azul como en el ejemplo anterior. Y veremos que coinciden con todos los elementos del* $Ap(S, 10)$, *que son los elementos que aparecen en rojo.*

x	y2	y1								
0	0	0	1	2	3	4	5	6	7	8
y3->	0	0	9	18	27	36	45	54	63	72
	1	31	40	49	58	67	76	85	94	103
	2	62	71	80	89	98	107	116	125	134
	3	93	102	111	120	129	138	147	156	165
	4	124	133	142	151	160	169	178	187	196

Ejemplo 2.5 *Consideremos un ejemplo con cuatro generadores, para lo cual tomemos el semigrupo numérico generado por la cuaterna* $\{7,\ 9,\ 11,\ 15\}$.

Definimos el ideal correspondiente

$$I = \langle y_1 - x^7, y_2 - x^9, y_3 - x^{11}, y_4 - x^{15} \rangle \subset \mathbb{Q}[x, y_1, y_2, y_3, y_4],$$

y hallamos su base de Groebner asociada al orden σ_1*:*

$$\begin{aligned}\mathcal{B}_1 \;=\; \{&x^7 - y_1,\ x^3y_3 - y_1^2,\ x^2y_2 - y_3,\ x^2y_1 - y_2,\ xy_2y_3 - y_1^3,\ y_1^2y_4^2 - y_1^5y_2,\\ &xy_4 - y_1y_2,\ xy_1^3 - y_1y_4,\ xy_1^2 - y_4,\ y_1y_2y_3y_4 - y_1^6,\ y_2y_3y_4 - y_1^5,\\ &xy_1y_4 - y_1^2y_2,\ y_1y_4^2 - y_1^4y_2,\ y_4^2 - y_1^3y_2,\ y_3^2 - y_1y_4,\ y_2^2 - y_1y_3\}\end{aligned}$$

Representemos ahora el conjunto Δ*. Para ello tenemos que representar las formas normales en* $\{x = 0\} \bigcap \{y_1 = 0\}$*. Vamos a representar una tabla por cada hiperplano* $y_4 = k$ *con* k *entero hasta donde nos haga falta.*

x	y1	y4	y3			
0	0	0	0	1	2	3
	y2->	0	0	11	22	33
		1	9	20	31	42
		2	18	29	40	51
		3	27	38	49	60

x	y1	y4	y3			
0	0	1	0	1	2	3
	y2->	0	15	26	37	48
		1	24	35	46	57
		2	33	44	55	66
		3	42	53	64	75

Como podemos comprobar los números sombreados en azul son los elementos del conjunto Δ*:*

$$\Delta = \{0,\ 9,\ 11,\ 15,\ 20,\ 24,\ 26\}$$

que se corresponden con el conjunto

$$Ap(S, 7) = \{0,\ 9,\ 11,\ 15,\ 20,\ 24,\ 26\}.$$

2.3 La condición de Gorenstein.

En [21] Nijenhuis y Wilf partieron del caso $n = 2$ donde, gracias al trabajo de Sylvester, sabemos que

$$n(S) = \frac{1}{2}c(S)$$

y se preguntaron en qué condiciones podemos asegurar que se tiene esta igualdad. En concreto, demostraron el siguiente resultado (probado independientemente por Kunz en [16]).

Teorema 2.2 *Sea $S = \langle a_1, ..., a_k \rangle$ un semigrupo numérico. Consideremos el conjunto*

$$T(S) = \{m \in Ap(S, a_k) \mid m + a_i \notin Ap(S, a_k),\ \forall i = 1, ..., k\}.$$

Entonces se tiene que

$$n(S) = \frac{1}{2}c(S) \iff \sharp T(S) = 1.$$

Esta condición ($\sharp T(S) = 1$) se denomina (en [21]) *condición de Gorenstein*. Dada la relación directa con el conjunto de Apéry, pensamos que sería interesante ver si esta condición se puede visualizar en nuestro algoritmo de cálculo.

El conjunto $T(S)$ está íntimamente relacionado con $PF(S)$, mediante el siguiente resultado (también de [21]).

Proposición 2.3 *En las condiciones anteriores se tiene que*

$$PF(S) = \{m - a_k \mid m \in T(S)\}.$$

Demostración: Un número m está en $T(S)$ si verifica todas las condiciones siguientes:

$$\begin{cases} m \in S & \text{y} \quad m - a_k \in G(S) \\ m + a_1 \in G(S) & \text{o} \quad m + a_1 - a_k \in S \\ \quad \vdots & \qquad \vdots \\ m + a_k \in G(S) & \text{o} \quad m + a_k - a_k \in S \end{cases}$$

Claramente la primera condición de la primera línea excluye que se den las primeras condiciones de las demás, de forma que ha de ser:

$$T(S) = \{m \in S \mid m - a_k \in G(S),\ m - a_k + a_i \in S\}.$$

Evidentemente un entero $m - a_k$ que no esté en S pero que entre en S al sumarle cualquier generador ha de ser necesariamente un pseudo–número de Frobenius, y viceversa. ■

Corolario 2.1 *En las condiciones anteriores:*

- $\sharp\, T(S) = t(S)$.
- *Un semigrupo verifica la condición de Gorenstein si y sólo si es simétrico.*
- $T(S) = \max_{\leq_S} Ap(S, a_k)$.

Demostración: Únicamente la tercera afirmación no es inmediata de la proposición. Pero si nos fijamos en el enunciado de la proposición 2.2. para el caso $n = a_k$, el resultado es directo. ■

Vamos a intentar dar una interpretación de esta propiedad (da lo mismo que la llamemos condición de Gorenstein que semigrupo simétrico) en los términos relacionados a las bases de Groebner que hemos usado con anterioridad.

Para ello intentaremos construir el conjunto $T(S)$, dado que la condición de Gorenstein equivale a $\sharp T(S) = 1$. Comenzamos buscando los elementos de $Ap(S, a_k)$ y trataremos de ordenarlos por $\leq_S$. Para ello, ya sabemos que basta con fijar el orden monomial $\leq_k$, su base de Groebner $\mathcal{B}_k$ y quedarnos en los elementos que aparecen en el conjunto que hemos denominado Δ.

Supongamos que tenemos un $N \in \Delta$. Eso quiere decir que

$$exp\left(N_k\left(x^N\right)\right) = (0, \gamma_1, ..., \gamma_{k-1}, 0); \qquad N = \sum_{i=0}^{k-1} \gamma_i a_i.$$

Imaginemos que se tiene, para algún $i = 1, ..., k-1$, que

$$(0, \gamma_1, ..., \gamma_i + 1, ..., \gamma_{k-1}, 0) \in \overline{E(I)} \cap \{\ x = y_k = 0\ \}.$$

Esto es equivalente a decir que $N + a_i \in \Delta$. Dicho de otra forma, si podemos movernos una unidad dentro de $\overline{E(I)} \cap \{\ x = y_k = 0\ \}$ (el conjunto sombreado de azul en los ejemplos) sin abandonar este conjunto, es porque partimos de un elemento de Δ que *no* es maximal para $\leq_S$.

Definición 2.6 *En las condiciones anteriores, sea $N \in \Delta$, y pongamos*

$$exp\left(N_k\left(x^N\right)\right) = (0, \gamma_1, ..., \gamma_{k-1}, 0).$$

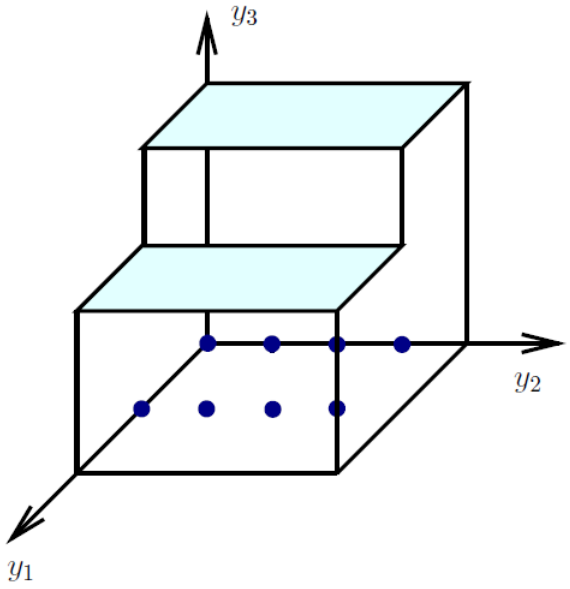
Diremos que N es un elemento extremo de Δ si para todo $i = 1, ..., k$ se tiene que

$$(0, \gamma_1, ..., \gamma_i + 1, ..., \gamma_{k-1}, 0) \notin \overline{E(I)} \cap \{\ x = y_k = 0\ \}.$$

Observación 2.2 *De lo anterior podemos deducir inmediatamente que todos los elementos de $T(S)$ han de ser necesariamente elementos extremos de Δ.*

En los diversos cálculos concretos que hemos realizado hasta el momento, el conjunto $T(S)$ ha coincidido con el conjunto de elementos extremos de Δ. Es por ello que terminamos este capítulo formulando las siguientes conjeturas.

Conjetura (Caracterización de la condición de Gorenstein, versión débil). En las condiciones anteriores, se verifica la condición de Gorenstein si y sólo si el conjunto de elementos extremos de Δ es unitario. Equivalentemente, $\overline{E(I)} \cap \{x = y_k = 0\}$ es un $(k-1)$–ortoedro en $\mathbb{Z}^{n-1}_{\geq 0}$.



Conjetura (Caracterización de la condición de Gorenstein, versión fuerte). En las condiciones anteriores, el conjunto de elementos extremos de Δ coincide con el conjunto $T(S)$.

CAPÍTULO 3

El número de puntos enteros en un triángulo rectángulo

3.1 El problema clásico.

El cálculo (o la estimación) del números de puntos con coordenadas enteras del interior o interior y frontera de un polígono es un problema clásico en el que se cruzan la combinatoria y la teoría de números.

Uno de los primeros resultados sobresalientes en este ámbito es el Teorema de Pick [22]. Este sorprendente resultado relaciona el área de un polígono simple con el números de puntos con coordenadas enteras en su interior y en su frontera, siempre y cuando sus vértices sean coordenadas enteras.

Teorema 3.1 *Sea P un polígono simple, es decir sin agujeros, tal que sus vértices tienen todos coordenadas enteras. Entonces:*

$$A = I + \frac{B}{2} - 1$$

donde A es el área de P, I es el número de puntos enteros interiores de P, y B el número de puntos enteros en el borde de P.

Cabe mencionar como curiosidad, que existe una generalización del Teorema de Pick para polígonos con agujeros en el interior. En esta versión

para hallar el área del polígono con agujeros, simplemente hay que sumar el número de agujeros a la fórmula obtenida en el teorema clásico.

El Teorema de Pick no es válido si el polígono no tiene vértices enteros y, desafortunadamente, este resultado no se generaliza a $\mathbb{R}^3$ ó dimensiones superiores. Hecho que demostró J. Reeve utilizando el tetraedro que lleva su nombre como contraejemplo [26].

Existen diversas demostraciones del Teorema de Pick, que han ido apareciendo en los más de cien años de edad que tiene el resultado. Por ejemplo, una que utiliza la fórmula de Euler para poliedros y grafos simples. Aunque la mayoría de las demostraciones, incluida la original, reducen el problema al de un triángulo rectángulo con vértices enteros.

En esta línea, el problema de contar puntos enteros dentro de un triángulo rectángulo ha aparecido de forma recurrente en la literatura. Por ejemplo, Hardy y Littlewood, entre otros, intentaron ampliar el enfoque del problema, dando estimaciones [13] para el número de puntos enteros de un triángulo rectángulo limitado por los semiejes positivos y una recta de pendiente irracional.

Buscando resultados en la línea del Teorema de Pick que generalicen a dimensiones superiores, nos encontramos con que Eugéne Ehrhart probó en 1960 [11] que la cantidad de puntos enteros encerrados por el dilatado de un politopo P, esto es,

$$tP = \{(tx_1, ..., tx_n) \mid (x_1, ..., x_n) \in P\},$$

con $t \in \mathbb{N}$, cuando P posee vértices enteros, es un polinomio en la variable t de grado n, la dimensión de P. En concreto, el coeficiente de mayor grado es el volumen del politopo y el de menor grado su característica de Euler. Este polinomio es el que se conoce como polinomio de Ehrhart de P:

$$i(P, t) = e_n(P)t^n + e_{n-1}(P)t^{n-1} + ... + e_0$$

En el caso de que el politopo convexo sea racional (es decir con los vértices puntos de coordenadas racionales), existe una generalización, el denominado Quasi–Polinomio de Ehrhart. En esta línea Matthias Beck y Sinai Robins dan en [4] una fórmula estable para calcular el número de puntos enteros encerrados por un politopo convexo racional P, y de sus correspondientes dilatados tP, con $t \in \mathbb{Z}$. Para ello calculan los coeficientes del Quasi–Polinomio de Ehrhart con una construcción que se reduce al cálculo de puntos enteros

encerrados por un triángulo rectángulo de vértices racionales. En este cálculo se utilizan las sumas de Dedekind–Fourier.

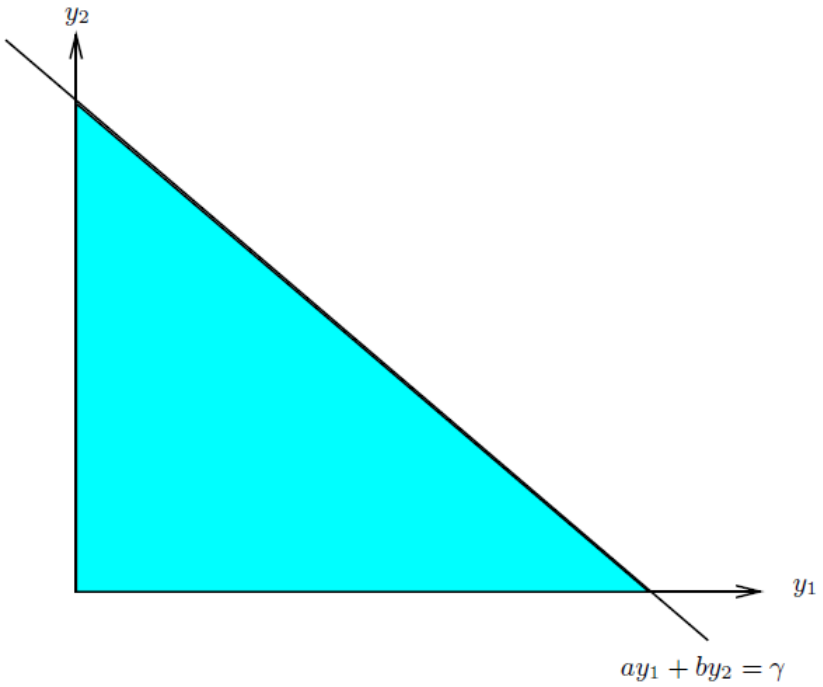
3.2 El problema visto desde los semigrupos numéricos.

Observación 3.1 *Por nuestra parte, en este trabajo nos centramos en un problema que, como hemos visto, posee una gran tradición: el cálculo del número de puntos enteros encerrados en un triángulo rectángulo de vértices racionales limitado por los semiejes positivos. La principal diferencia de nuestro tratamiento es que resolveremos este problema utilizando técnicas de semigrupos numéricos.*

Consideramos un triángulo definido por los semiejes positivos en dimensión 2 y por una recta de ecuación

$$ay_1 + by_2 = \gamma, \quad a, b, \gamma \in \mathbb{Z} \text{ y } gcd(a, b) = 1,$$

donde por convenio fijaremos $a < b$, sin pérdida de generalidad.



Definimos el siguiente conjunto:

$$T = \left\{(y_1, y_2) \in \mathbb{Z}^2_{\geq 0} \mid ay_1 + by_2 \leq \gamma\right\}$$

Definimos el subgrupo numérico asociado a nuestro triángulo como el semigrupo $S = \langle a,\ b\rangle$. S tendrá, por tanto, como número de Frobenius $f(S) = ab - (a + b)$.

Como hemos hecho anteriormente, definimos el ideal binomial asociado a S:

$$I = \langle y_1 - x^a, y_2 - x^b\rangle \subset k[x, y_1, y_2]$$

y hallamos su base de Groebner $\mathcal{G} = \{g_1, ..., g_r\}$ respecto al orden lexicográfico.

Notemos como

$$q_i = exp(lt(g_i)),$$

siendo como siempre $lt(f)$ el monomio líder respecto al orden anteriormente elegido del polinomio f y al cuadrante positivo con origen q_i, como

$$K_{q_i} = q_i + \mathbb{Z}^3_{\geq 0} \subset \mathbb{Z}^3_{\geq 0}.$$

Y definimos la escalera asociada a la base de Groebner $\mathcal{G}$,

$$E(I) = \left\{(x, y_1, y_2) \in \bigcup_i K_{q_i}\right\} \subset \mathbb{Z}^3_{\geq 0}.$$

Nos fijaremos (en la línea de los resultados del capítulo 1) en la escalera restringida al plano $\{x = 0\}$:

$$E_0 = \left\{(y_1, y_2) \mid (0, y_1, y_2) \in \bigcup_i K_{q_i} \subset \mathbb{Z}^3_{\geq 0}\right\}.$$

Observación 3.2 *Sea $g = y_1^b - y_2^a$. En las condiciones anteriores podemos suponer, sin pérdida de generalidad, que $g \in G$. Si no estuviese, podemos añadirlo, y para justificarlo bastaría con probar que $g = y_1^b - y_2^a$ está en el ideal.*

Pero esto es trivial, ya que por el Lema 1.1, sabemos que $I = \ker\left(\widetilde{\phi}\right)$, y obviamente $g = y_1^b - y_2^a \in \ker\left(\widetilde{\phi}\right)$ ya que

$$\widetilde{\phi}(y_1^b - y_2^a) = x^{ab} - x^{ba} = 0.$$

Teorema 3.2 *En las condiciones anteriores, y con la notación previamente usada, E_0 sólo tiene un cuadrante con vértice en el eje y_1. En concreto*

$$E_0 = \{(y_1, y_2) \mid y_1 \geq b\} \subset \mathbb{Z}^2_{\geq 0}.$$

Demostración: Veamos que la interesección de E con el plano $\{x = 0\}$ consiste en sólo un cuadrante K_q con $q = (b, 0)$. Para ello vamos a demostrar que no existe ningún elemento g_i de la base de Groebner de forma que

$$g_i = y_1^{\alpha_1} y_2^{\alpha_2} - y_1^{\beta_1} y_2^{\beta_2} \text{ con } \alpha_1 < b,\ \beta_1 < \alpha_1.$$

Recordemos que la base de Groebner está formada por binomios, como vimos en el primer capítulo. Razonemos por reducción al absurdo y supongamos que existe dicho g_i.

Por tanto por los resultados de Buchberger (ver apéndice) sabemos que la sizigia de todo par de elementos de la base de Groebner tiene que ser cero. Y conocemos por la observación anterior un elemento de la base, $g = y_1^b - y_2^a \in G$. Por tanto ha de ser $S(g, g_i) = 0$.

Calculemos esta sizigia:

$$S(g, g_i) = \frac{\operatorname{lcm}\left(y_1^{\alpha_1} y_2^{\alpha_2}, y_1^b\right)}{y_1^{\alpha_1} y_2^{\alpha_2}}(y_1^{\alpha_1} y_2^{\alpha_2} - y_1^{\beta_1} y_2^{\beta_2}) - \frac{\operatorname{lcm}\left(y_1^{\alpha_1} y_2^{\alpha_2}, y_1^b\right)}{y_1^b}(y_1^b - y_2^a).$$

Teniendo en cuenta que $\alpha_1 < b$ entonces

$$\operatorname{lcm}\left(y_1^{\alpha_1} y_2^{\alpha_2}, y_1^b\right) = y_1^b y_2^{\alpha_2},$$

y por tanto

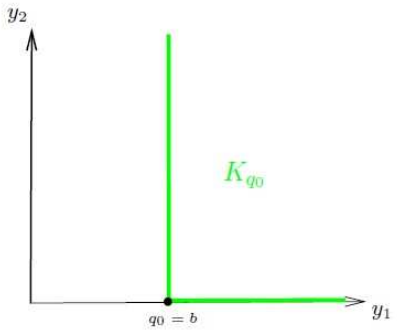
$$\begin{aligned} S(g, g_i) &= y_1^{b-\alpha_1}(y_1^{\alpha_1} y_2^{\alpha_2} - y_1^{\beta_1} y_2^{\beta_2}) - y_2^{\alpha_2}(y_1^b - y_2^a) \\ &= y_2^{a+\alpha_2} - y_1^{b-\alpha_1+\beta_1} y_2^{\beta_2} \end{aligned}$$

Por lo que si imponemos que esta sizigia sea cero, tendríamos lo siguiente:

$$S(g, g_i) = 0 \iff b - \alpha_1 + \beta_1 = 0 \text{ y } a + \alpha_2 = \beta_2$$

Si despejamos β_1 de la expresión anterior tendríamos que $\beta_1 = \alpha_1 - b$, pero por hipótesis $\alpha_1 < b$ por lo que β_1 sería un numero negativo, llegando a un absurdo que demuestra el resultado. ∎

Si representamos por tanto E_0, tendremos

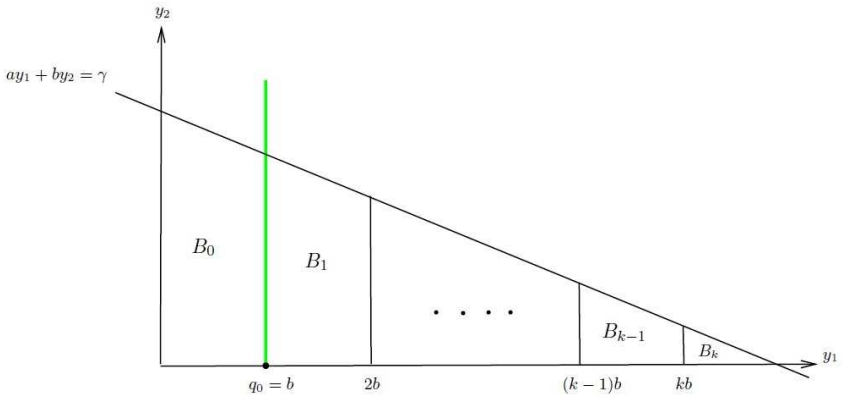


En este plano, podemos dibujar nuestro triángulo T de nuevo, junto al cuadrante $K_{(b,0)}$ que aparece en el dibujo.

Dividimos entonces T en polígonos cuyas bases tienen todas longitud b. Y definimos los siguientes conjuntos,

$$\begin{aligned}
B_0 &= \left\{(y_1,y_2) \in \overline{K_{(b,0)}} \text{ tales que } ay_1+by_2 \le \gamma\right\}\\
B_1 &= \left\{(y_1,y_2) \in K_{(b,0)} \text{ tales que } ay_1+by_2 \le \gamma,\ \ b \le y_1 < 2b\right\}\\
&\vdots \qquad \vdots\\
B_i &= \left\{(y_1,y_2) \in K_{(b,0)} \text{ tales que } ay_1+by_2 \le \gamma,\ \ ib \le y_1 < (i+1)b\right\}\\
&\vdots \qquad \vdots\\
B_k &= \left\{(y_1,y_2) \in K_{(b,0)} \text{ tales que } ay_1+by_2 \le \gamma,\ \ kb \le y_1\right\}
\end{aligned}$$

siendo $k = \lfloor \gamma/(ab) \rfloor$. Los conjuntos $\{B_i\}$ definen obviamente una partición de los puntos enteros de T.



Nuestro objetivo es contar los puntos enteros de T, por tanto lo que queremos hallar es:

$$\sharp\, T = \sharp\, B_0 + \sharp\, B_1 + ... + \sharp\, B_{k-1} + \sharp\, B_k.$$

- Empezamos por contar los puntos enteros en B_0. La biyección $\mathcal{G}$ del Teorema 1.3. nos dice que

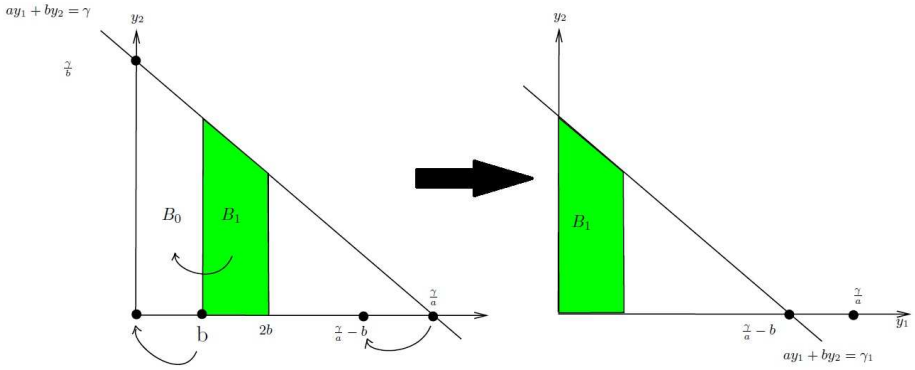
$$S \overset{1:1}{\longleftrightarrow} \overline{K_{(b,0)}},$$

y por tanto el cardinal de B_0 se reduce a::

$$\begin{aligned} \sharp\, B_0 &= \sharp\, (S \cap [0,\gamma]) \\ &= \sharp\, (S \cap [0, f(S)]) + (\gamma - f(S)) \\ &= \frac{ab-(a+b)+1}{2} + (\gamma - (ab-(a+b))) \\ &= \frac{a+b-ab+1}{2} + \gamma, \end{aligned}$$

dado que sabemos que $n(S) = f(S)/2$, en el caso de semigrupos de dimensión 2.

- Para calcular la cantidad de puntos del conjunto B_1, hacemos una traslación del polígono, de tal forma que trasladamos $q_0 = b$ al origen de coordenadas. De igual forma la recta $ay_1 + by_2 = \gamma$ la trasladamos b unidades a la izquierda, como se muestra en el dibujo;



Abusando de notación, redefinimos B_1 como sigue:

$$B_1 = \left\{(y_1, y_2) \in \overline{K_{(b,0)}} \text{ tales que } ay_1 + by_2 \leq \gamma_1\right\}$$

donde $\gamma_1 = \gamma - ab$ (lógicamente esto tiene sentido en el caso $\gamma > ab$). De esta forma, utilizando el razonamiento del apartado anterior, tenemos

$$\begin{aligned} \sharp\, B_1 &= \sharp\, (S \cap [0, \gamma_1]) \\ &= \sharp\, (S \cap [0, \gamma - ab]) \\ &= \frac{ab - (a+b) + 1}{2} + (\gamma - ab - (ab - (a+b) + 1)) \\ &= \frac{a + b - 3ab + 1}{2} + \gamma, \end{aligned}$$

procediendo de manera similar al caso B_0.

- Procedemos de forma recurrente para calcular los puntos enteros de los conjuntos B_i con $i = 1, ...k-1$, donde $k = \lfloor \gamma/(ab) \rfloor$. Reescribiendo $\gamma_i = \gamma - iab$, siempre que $\gamma > iab$ tendremos que:

$$\begin{aligned} \sharp\, B_i &= \sharp\, (S \cap [0, \gamma_i]) \\ &= \sharp\, (S \cap [0, \gamma - iab]) \\ &= \frac{ab - (a+b) + 1}{2} + \gamma - iab - (ab - (a+b)) \\ &= \frac{(a+b) - (1+2i)ab + 1}{2} + \gamma \end{aligned}$$

- Por último nos queda calcular los puntos enteros del conjunto B_k. Hacemos igualmente una traslación al origen, de forma que el número de puntos enteros de B_k coincide con el número de puntos enteros del conjunto siguiente (que también denominamos B_k):

$$B_k = \left\{ (y_1, y_2) \in \overline{K_{(b,0)}} \text{ tales que } ay_1 + by_2 \leq \gamma_k \right\}$$

En este caso, nos encontramos que $\gamma_k < ab-(a+b)$, por definición de k. Por tanto debemos proceder de forma diferente a los casos anteriores.

Sabemos que $\gamma_k = \gamma - kab$, es decir, $\gamma_k = \gamma \mod ab$, y

$$\sharp\, B_k = \sharp\, (S \cap [0, \gamma_k]) = \sharp\, (S \cap [0, \gamma - kab])\,.$$

Por lo que ahora tratamos de contar los elementos del semigrupo menores que $\gamma - kab < f(S)$. Utilizamos para ello el conjunto de Apéry,

que para el caso de dos generadores está perfectamente controlado como demostramos en el capítulo anterior.

En concreto sabemos que:

$$Ap(S,a) = \{0, b, 2b, ..., (a-1)b\}$$

y por tanto

$$\{w \in Ap(S,a) \mid w \leq \gamma_k\} = \left\{ib \mid i = 0, 1, ..., \left\lfloor \frac{\gamma_k}{b} \right\rfloor\right\}$$

Si tomamos entonces $i \in \{0, ..., \lfloor \gamma_k/b \rfloor\}$, tenemos que

$$ib + ja \leq \gamma_k \iff j \leq \left\lfloor \frac{\gamma_k - ib}{a} \right\rfloor,$$

y por tanto

$$\begin{aligned} S \cap [0, \gamma_k] &= \{ib + ja \leq \gamma_k \mid i, j \in \mathbb{Z}_{\geq 0}\} \\ &= \left\{ib + ja \;\middle|\; i \in \left\{0, ..., \left\lfloor \frac{\gamma_k}{b} \right\rfloor\right\},\ j \leq \left\lfloor \frac{\gamma_k - ib}{a} \right\rfloor\right\} \\ &= \sum_{i=0}^{\lfloor \frac{\gamma_k}{b} \rfloor} \left(\left\lfloor \frac{\gamma_k - ib}{a} \right\rfloor + 1 \right) \end{aligned}$$

Sumando los elementos de cada conjunto obtenemos finalmente los enteros del triángulo T.

Teorema 3.3 *En las condiciones anteriores, se tiene que*

$$\begin{aligned} \sharp\, T &= \left(\frac{a+b-ab+1}{2} + \gamma \right) + ... + \left(\frac{(a+b)-(1+2i)ab+1}{2} + \gamma \right) + \\ &\qquad +... + \sum_{i=0}^{\lfloor \frac{\gamma_k}{b} \rfloor} \left(\left\lfloor \frac{\gamma_k - ib}{a} \right\rfloor + 1 \right) \\ &= \sum_{i=0}^{k-1} \left(\frac{(a+b)-(1+2i)ab+1}{2} + \gamma \right) + \sum_{i=0}^{\lfloor \frac{\gamma_k}{b} \rfloor} \left(\left\lfloor \frac{\gamma_k - ib}{a} \right\rfloor + 1 \right) \\ &= -\frac{ab}{2}k^2 + \frac{a+b+1+2\gamma}{2}k + \sum_{i=0}^{\lfloor \frac{\gamma - kab}{b} \rfloor} \left(\left\lfloor \frac{\gamma - kab - ib}{a} \right\rfloor + 1 \right) \end{aligned}$$

donde $k = \lfloor \gamma/(ab) \rfloor$.

Ejemplo 3.1 *Empecemos por un ejemplo simple, tomamos para ello un triángulo rectángulo sin demasiados puntos de coordenadas enteras en su interior. Sea triángulo formado por los semiejes positivos y la recta* $3x + 7y = 46$.

Según la fórmula los puntos enteros encerrados por este triángulo serían:

$$\sharp\, T = -\frac{3\cdot 7}{2}k^2 + \frac{3+7+1+2\cdot 46}{2}\cdot k + \sum_{i=0}^{\left\lfloor \frac{46-k3\cdot 7}{7}\right\rfloor}\left(\left\lfloor \frac{46-k3\cdot 7-i7}{3}\right\rfloor + 1\right)$$

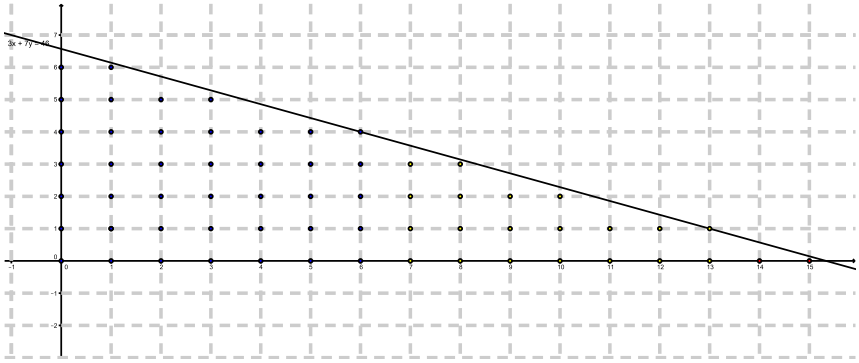
donde $k = \left\lfloor \frac{46}{3\cdot 7}\right\rfloor = 2$.

Sustituyendo k *en la fórmula anterior y realizando los cálculos pertinentes tenemos*

$$\sharp\, T = -\frac{3\cdot 7}{2}2^2 + \frac{3+7+1+2\cdot 46}{2}\cdot 2 + \sum_{i=0}^{\left\lfloor \frac{46-2\cdot 3\cdot 7}{7}\right\rfloor}\left(\left\lfloor \frac{46-2\cdot 3\cdot 7-i7}{3}\right\rfloor + 1\right) =$$

$$= -42 + 103 + 2 = 61 + 2 = 63$$

Veamos ahora el recuento.



En el dibujo hemos dividido por colores los diferentes conjuntos B_j*, correspondientes al proceso seguido para obtener la fórmula. Si contamos los puntos que aparecen en azul, obtenemos* 41*, que son los puntos encerrados por el conjunto* B_0*, de acuerdo con la fórmula:*

$$\sharp\, B_0 = \frac{a+b-ab+1}{2} + \gamma = \frac{3+7-3\cdot 7+1}{2} + 46 = 41.$$

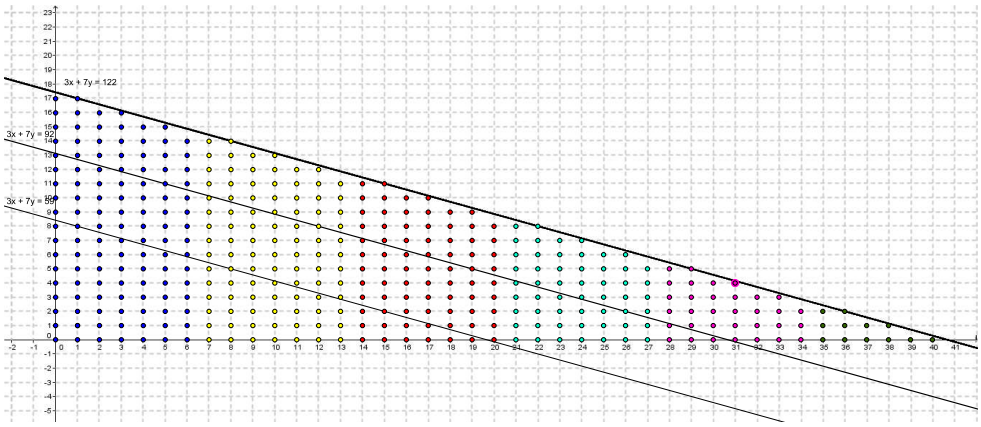
Los puntos amarillos corresponden al conjunto B_1:

$$\sharp\, B_1 = \frac{a+b-3ab+1}{2} + \gamma = \frac{3+7-3\cdot 3\cdot 7+1}{2} + 46 = 20.$$

Y por último el conjunto B_2 son los puntos rojos:

$$\sharp\, B_2 = \sum_{i=0}^{\left\lfloor \frac{\gamma_k}{b} \right\rfloor} \left(\left\lfloor \frac{\gamma_k - ib}{a} \right\rfloor + 1 \right) = \left\lfloor \frac{46-42}{3} \right\rfloor + 1 = 2.$$

Ejemplo 3.2 *Veamos ahora varios ejemplos con los mismos coeficientes que el anterior pero variando el termino independiente, γ.*

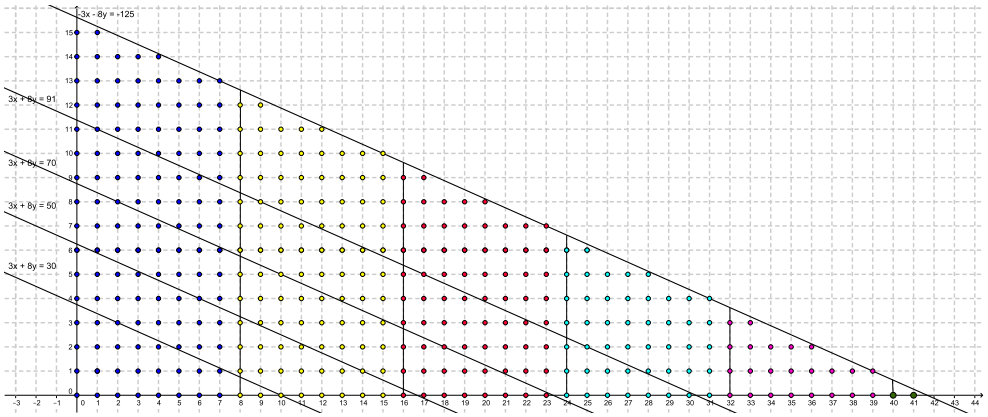


Para el triángulo más pequeño, limitado por $3x+7y=59$ la fórmula nos da 99 puntos.

El siguiente triángulo, que tiene por hipotenusa $3x+7y=92$ nos da, sustituyendo en la fórmula, la cantidad de 226 puntos con coordenadas enteras.

Por último el mayor, limitado por $3x+7y=122$, nos da según la fórmula una cantidad de 387. El lector puede comprobar mediante el dibujo anterior, que el resultado obtenido mediante la fórmula coincide exactamente con los puntos enteros encerrados.

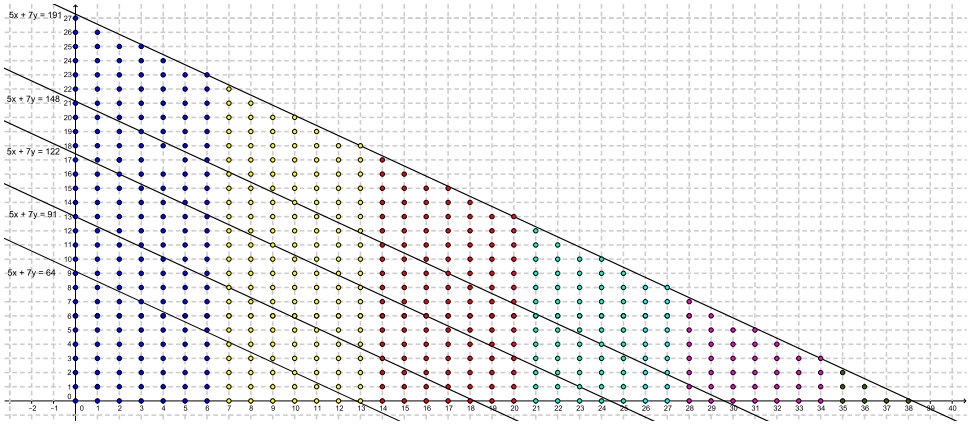
Ejemplo 3.3 *Veremos algunos ejemplos más, para empezar limitados por la hipotenusa $3x+8y=\gamma$ con $\gamma = 30, 50, 70, 91, 125$.*



La fórmula (y el recuento manual) nos da los siguientes resultados:

- *Para* $3x + 8y = 30$*, encierra* 27 *puntos.*
- *Para* $3x + 8y = 50$*, tiene* 65 *puntos.*
- *Para* $3x + 8y = 70$*, tiene* 120 *puntos.*
- *Para* $3x + 8y = 91$*, tiene* 196 *puntos.*
- *Para* $3x + 8y = 125$*, tiene* 357 *puntos.*

Ejemplo 3.4 *Al igual que en el ejemplo anterior veamos ahora que nos da la fórmula para los triángulos limitados por* $5x + 7y = \gamma$ *con* $\gamma = 64, 91, 122, 148, 191$*.*



- *Para* $5x + 7y = 64$*, tiene* 71 *puntos.*
- *Para* $5x + 7y = 91$*, tiene* 136 *puntos.*
- *Para* $5x + 7y = 122$*, tiene* 236 *puntos.*
- *Para* $5x + 7y = 148$*, tiene* 341 *puntos.*
- *Para* $5x + 7y = 191$*, tiene* 557 *puntos.*

Notemos cómo en estos ejemplos encontramos casuísticas variadas relativas a los puntos enteros que hay (o no hay) sobre la hipotenusa.

3.3 Generalización a dimensiones superiores.

El tipo de fórmula que hemos obtenido en la sección anterior hace que resulte particularmente sencillo generalizar el resultado a dimensiones superior. Veamos primero, por fijar ideas, cómo funcionaría en dimensión 3.

Supongamos que queremos hallar el cardinal del siguiente conjunto:

$$T_3 = \left\{(y_1, y_2, y_3) \in \mathbb{Z}^3_{\geq 0} \mid a_1y_1 + a_2y_2 + a_3y_3 \leq \gamma_3\right\},$$

con, pongamos $a_1 \leq a_2 \leq a_3$, $\gcd(a_1, a_2, a_3) = \gcd(a_1, a_2) = 1$.

Claramente bastará para con contar los puntos de T_3 en cada plano $y_3 = i_3$, donde i_3 recorre el intervalo $[0, \lfloor \gamma_3/a_3 \rfloor]$.

De esta forma en un plano $y_3 = i_3$, tendríamos el triángulo

$$T_2 = \left\{(y_1, y_2) \in \mathbb{Z}^2_{\geq 0} \mid a_1y_1 + a_2y_2 \leq \gamma_2\right\}$$

siendo $\gamma_2 = \gamma_3 - a_3i_3$.

Por lo que utilizando la fórmula de la sección anterior es claro que:

$$\sharp\, T_3 = \sum_{i_3=0}^{\lfloor \gamma_3/a_3 \rfloor} \left[\sum_{i=0}^{k-1} \left(\frac{(a_1 + a_2) - (1 + 2i)a_1a_2 + 1}{2} + \gamma_2 \right) + \right.$$
$$\left. + \sum_{i=0}^{\left\lfloor \frac{\gamma_2 - ka_1a_2}{a_2} \right\rfloor} \left(\left\lfloor \frac{\gamma_2 - ka_1a_2 - ia_2}{a_1} \right\rfloor + 1 \right) \right]$$

donde $k = \left\lfloor \frac{\gamma_2/a_1}{a_2} \right\rfloor$ y $\gamma_2 = \gamma_3 - a_3i_3$.

Observación 3.3 *El caso* $\gcd(a_1, a_2) = d > 1$ *habría que estudiarlo aparte, ya que en este caso el teorema 3.1. no puede aplicarse. No es nuestra intención hacer aquí un desarrollo exhaustivo de las diferentes casuísticas.*

El cálculo para dimensión 4 no reviste mayor dificultad. Tenemos

$$T_4 = \{(y_1, y_2, y_3, y_4) \in \mathbb{Z}^4_{\geq 0} \mid a_1y_1 + a_2y_2 + a_3y_3 + a_4y_4 \leq \gamma_4\}$$

con $\gcd(a_1, a_2, a_3, a_4) = \gcd(a_1, a_2, a_3) = \gcd(a_1, a_2) = 1$.

Podemos hacer que la variable y_4 recorra los enteros desde 0 hasta $\left\lfloor \frac{\gamma_4}{a_4} \right\rfloor$. En el plano $y_4 = i_4$ con $i_4 = 0, ..., \left\lfloor \frac{\gamma_4}{a_4} \right\rfloor$, tenemos el conjunto de puntos

$$T_3 = \{(y_1, y_2, y_3) \in \mathbb{Z}^3_{\geq 0} \mid a_1y_1 + a_2y_2 + a_3y_3 \leq \gamma_3 = \gamma_4 - i_4a_4\}$$

Y aplicando la fórmula anterior en cada plano $y_4 = i_4$ con $i_4 = 0, ..., \left\lfloor \frac{\gamma_4}{a_4} \right\rfloor$, obtenemos:

$$\begin{aligned} \sharp\, T_4 \;=\; \sum_{i_4=0}^{\lfloor \gamma_4/a_4 \rfloor} \sum_{i_3=0}^{\lfloor \gamma_3/a_3 \rfloor} \Bigg[\sum_{i=0}^{k-1} \left(\frac{(a_1 + a_2) - (1 + 2i)a_1a_2 + 1}{2} + \gamma_2 \right) + \\ + \sum_{i=0}^{\left\lfloor \frac{\gamma_2 - ka_1a_2}{a_2} \right\rfloor} \left(\left\lfloor \frac{\gamma_2 - ka_1a_2 - ia_2}{a_1} \right\rfloor + 1 \right) \Bigg], \end{aligned}$$

donde $k = \left\lfloor \frac{\gamma_2/a_1}{a_2} \right\rfloor$ y $\gamma_2 = \gamma_3 - a_3i_3$ y $\gamma_3 = \gamma_4 - i_4a_4$. Por tanto $\gamma_2 = \gamma_4 - i_4a_4 - a_3i_3$.

Este mismo razonamiento se puede seguir, como ya es obvio, para calcular el cardinal del siguiente conjunto;

$$T_n = \left\{(y_1, ..., y_n) \in \mathbb{Z}^n_{\geq 0} \mid a_1y_1 + ... + a_ny_n \leq \gamma_n\right\}$$

ya que razonando de manera reiterada, basta con contar los puntos en cada hiperplano $y_i = i_n$, con $i_n = 0, ..., \lfloor \gamma_n/a_n \rfloor$.

Teorema 3.4 *En las condiciones anteriores se tiene que:*

$$\sharp\, T_n = \sum_{i_n=0}^{\lfloor \gamma_n/a_n \rfloor} \cdots \sum_{i_4=0}^{\lfloor \gamma_4/a_4 \rfloor} \sum_{i_3=0}^{\lfloor \gamma_3/a_3 \rfloor} \left[\sum_{i=0}^{k-1} \left(\frac{(a_1+a_2)-(1+2i)a_1a_2+1}{2} + \gamma_2 \right) + \sum_{i=0}^{\left\lfloor \frac{\gamma_2 - ka_1a_2}{a_2} \right\rfloor} \left(\left\lfloor \frac{\gamma_2 - ka_1a_2 - ia_2}{a_1} \right\rfloor + 1 \right) \right]$$

donde $k = \left\lfloor \frac{\gamma_2/a_1}{a_2} \right\rfloor$ *y*

$$\gamma_i = \gamma_{i+1} - a_{i+1}i_{i+1},$$

en particular

$$\gamma_2 = \gamma_n - i_n a_n .... - i_4 a_4 - a_3 i_3.$$

Final remarks

N.B.: Esta parte de la tesis está redactada en inglés de cara a cumplir con la normativa vigente de la Universidad de Sevilla relativa a la Mención Internacional en el Título de Doctor.

This final part of the thesis will be devoted to point out some of the problems that our results have arisen. These problems (some explicit, some vague) are expected to represent an interesting set of challenges for our near future work, where the use of Groebner bases for the study of numerical semigroups may be expanded and reinforced.

Chapter 1.

Open Problem 1.– *Find a tight bound for $n(S)$ in terms of $f(S)$ and a set of generators of S.*

Open Problem 2.– *Find a lower bound for $n(S)$ in terms of $f(S)$ and a set of generators of S.*

In this direction, we believe that we need to understand better the precise combinatorial structure of the set $N(S)$, as our approach in chapter 1 is too coarse. Maybe a more precise (or a more intelligent) choice of monomial ordering may be of great help for this matter.

Chapter 2.

Open Problem 3.– *Prove or disprove the conjecture that links the Gorenstein condition with the property of the Apéry set being a $(k-1)$–cuboid.*

The partial ordering $\leq_S$ seems to play a key role here, as the ordered tree it induces seems to resemble the structure of $Ap(S, a_k)$. We think this will be probably be the first problem to be paid attention from the present list.

Chapter 3.

Open Problem 4.– *Relate the formulas obtained for the number of points in an n–tetrahedron to the Ehrhart pseudo–polynomials. In particular, try to give explicit terms of the Ehrhart pseudo–polynomials for cases with small dimension.*

Open Problem 5.– *Relate the formulas obtained for the number of points in an n–tetrahedron to the denumerant function ($n = 3$ may be a real difficulty already).*

A bit more elusive, these two problems represent major challenges to test the Groebner bases approach against. The Ehrhart polynomials, pseudo–polynomials and series have proved to be very fruitful tools in the recent past (see for instance [4]). The denumerant, on the other hand, has a well–deserved reputation as a source of many interesting problems, as one can check in the open problems appendix to [24].

Apéndice: Bases de Groebner.

Las bases de Groebner tienen en la actualidad un espectro de aplicación muy amplio. Su origen, o mejor dicho, uno de sus orígenes, fue sin embargo intentar resolver un problema natural en el ámbito de ideales de anillos de polinomios. El problema en cuestión no era otro que el problema de la pertenencia: averiguar, dado un sistema de generadores de un ideal (en un anillo de polinomios), cuándo un determinado polinomio está en el ideal.

Parece curioso que, a pesar de que se conocía el concepto de ideal desde hacía bastante tiempo, este problema no se resolvió hasta la década de los sesenta, donde las herramientas que estudiaremos a continuación fueron introducidas, de manera independiente, por Buchberger[6] e Hironaka[14] (éste último con una motivación completamente distinta: la resolución de singularidades en característica cero).

El material de este apéndice puede encontrarse en la actualidad incluso entre las materias que se imparten cursos de grado, dado que se ha popularizado y ha pasado en poco tiempo, de tratarse como algo altamente especializado y de escaso interés fuera del ámbito del Álgebra Computacional a convertirse en un recurso prácticamente ubicuo en cualquier aplicación o modelización que utilice anillos de polinomios.

A pesar de esto, intentaremos en este apéndice ser exhaustivos, al menos en la presentación de resultados y en la introducción de la nomenclatura y la notación que se utiliza a lo largo de la memoria.

Consideremos K, un cuerpo, $X_1, \ldots, X_n$ indeterminadas algebraicamente independientes, en principio; y sea $A = K[X_1, \ldots, X_n]$. A es un anillo de polinomios, además de un K–espacio vectorial, i.e. es una K–álgebra.

Como K–espacio vectorial es bien sabido que A tiene dimensión infinita,

siendo una base el conjunto $\mathcal{M}$ de los monomios;

$$\mathcal{M} = \{X_1^{\alpha_1} \dots X_n^{\alpha_n} \mid \alpha_i \in \mathbb{Z}_{\geq 0};\ \forall i, 1 \leq i \leq n\}\,.$$

Usualmente denotaremos $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ por X^α. En esta situación conviene observar que $\mathcal{M} \simeq \mathbb{Z}_{\geq 0}^n$, en el sentido de que existe una biyección (además natural) entre ellos.

Vamos a estudiar entonces algunas propiedades de $\mathbb{Z}_{\geq 0}^n$ que después aplicaremos en A.

Definición 3.1 *Un subconjunto $E \subset \mathbb{Z}_{\geq 0}^n$ se dice que es estable para la suma (también lo denominaremos escalera) si $\forall \alpha \in E$ y $\forall \beta \in \mathbb{Z}_{\geq 0}^n$ se tiene que $\alpha + \beta \in E$.*

El primer resultado importante es el siguiente, conocido como Lema de Dickson:

Lema 3.1 *Sea E una escalera en $\mathbb{Z}_{\geq 0}^n$. Entonces existe un número finito de elementos de $\mathbb{Z}_{\geq 0}^n$, únicos, que llamaremos $\alpha_1, \dots, \alpha_r$ tales que*

$$E = \bigcup_{i=1}^{r} \left[\alpha_i + \mathbb{Z}_{\geq 0}^n\right],$$

mientras que

$$E \neq \bigcup_{i \in J} \left[\alpha_i + \mathbb{Z}_{\geq 0}^n\right],$$

para todo J subconjunto propio de $\{1, \dots, r\}$. En otras palabras, los α_i son un conjunto minimal, denominados vértices de la escalera y denotados por $V(E)$.

Demostración: Lo haremos por inducción sobre n, siendo el caso $n = 1$ trivial (basta con usar la buena ordenación de $\mathbb{Z}_{\geq 0}$).

Supuesto cierto para $\mathbb{Z}_{\geq 0}^{n-1}$, consideremos la aplicación

$$\begin{array}{rcl} p_i : \mathbb{Z}_{\geq 0}^n & \longrightarrow & \mathbb{Z}_{\geq 0}^{n-1} \\ (\alpha_1, \dots, \alpha_n) & \longmapsto & (\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_n) \end{array}$$

Consideremos, así mismo, la aplicación

$$\begin{array}{rcl} q_{ij} : \mathbb{Z}_{\geq 0}^{n-1} & \longrightarrow & \mathbb{Z}_{\geq 0}^n \\ (\alpha_1, \dots, \alpha_{n-1}) & \longmapsto & (\alpha_1, \dots, \alpha_{i-1}, j, \alpha_{i+1}, \dots, \alpha_n) \end{array}$$

Vamos a fijar entonces un elemento del conjunto E, al que llameremos $\alpha = (\alpha_1, \ldots, \alpha_n)$. Sean

$$E_{ij} = p_i \left[\; E \cap \left(\mathbb{Z}_{\geq 0}^{i-1} \times \{j\} \times \mathbb{Z}_{\geq 0}^{n-i} \right) \; \right]$$

con $1 \leq i \leq n$; $\quad j = 0, \ldots, \alpha_i - 1$. Vamos a ver que E_{ij} es una escalera en $\mathbb{Z}_{\geq 0}^{n-1}$.

En efecto, sea $\beta \in E_{ij}$. Entonces existe un $\gamma \in E \cap \left(\mathbb{Z}_{\geq 0}^{i-1} \times \{j\} \times \mathbb{Z}_{\geq 0}^{n-i} \right)$ tal que $p_i(\gamma) = \beta$, con lo que $\beta = (\gamma_1, \ldots, \gamma_{i-1}, \gamma_{i+1}, \ldots, \gamma_n)$.

Sea ahora $\delta \in \mathbb{Z}_{\geq 0}^{n-1}$ y demostremos que $\beta + \delta \in E_{ij}$:

$$\beta + \delta = p_i(\gamma + (\delta_1, \ldots, \delta_{i-1}, 0, \delta_{i+1}, \ldots, \delta_{n-1})).$$

Pero obsérvese que el segundo sumando puede escribirse como $q_{i0}(\delta) \in \mathbb{Z}_{\geq 0}^{n}$ y, por tanto, la suma sobre la que opera p_i es un elemento de $E \cap \left(\mathbb{Z}_{\geq 0}^{i-1} \times \{j\} \times \mathbb{Z}_{\geq 0}^{n-i} \right)$. Esto último se basa en que las coordenadas distintas de i se quedan en E por ser γ de E y ser E escalera, y la coordenada i–ésima es claramente j por construcción.

Por ser entonces E_{ij} escalera existen (de la hipótesis de inducción) conjuntos finitos de vértices $F_{ij} = V\left(E_{ij}\right) \subset \mathbb{Z}_{\geq 0}^{n-1}$. Por tanto $q_{ij}(F_{ij}) \subset \mathbb{Z}_{\geq 0}^{n}$ también es un conjunto finito.

Consideremos ahora el conjunto

$$F = \left[\bigcup_{i,j} q_{ij}(F_{ij}) \right] \; \cup \; \{\alpha\}.$$

Vamos a demostrar a continuación que

$$E = \bigcup_{\gamma \in F} \left[\gamma + \mathbb{Z}_{\geq 0}^{n} \right],$$

y, para la minimalidad, basta con desechar las n-uplas redundantes; esto es, las que estén en la escalera inducida por las anteriores. Tendremos entonces demostrada la existencia de $V(E)$.

Sea pues $\beta \in E$. Si $\beta \in \alpha + \mathbb{Z}_{\geq 0}^{n}$ no tenemos nada que probar; por lo tanto, supondremos que no sucede esto. Por no estar β en $\alpha + \mathbb{Z}_{\geq 0}^{n}$ existe un i tal que $\beta_i < \alpha_i$. Sea $j = \beta_i$. Entonces

$$\beta \in E \cap (\mathbb{Z}_{\geq 0}^{i-1} \times \{j\} \times \mathbb{Z}_{\geq 0}^{n-i}),$$

con lo cual $p_i(\beta) \in E_{ij}$. En consecuencia $\exists \gamma \in F_{ij}$ tal que $p_i(\beta) \in \gamma + \mathbb{Z}_{\geq 0}^{n-1}$.

De aquí ya es claro que $\exists \delta$ con $\gamma + \delta = p_i(\beta)$. Por tanto se tiene que $q_{ij}(\gamma)+q_{i0}(\delta) = \beta$. Como el primer elemento pertenece a F, tengo demostrada la existencia.

Para ver la unicidad sólo es necesario escribir E en función de dos conjuntos de vértices distintos y aplicar que cada vértice de un conjunto ha de estar en la escalera generada por uno del otro conjunto. Así se llega rápidamente a que ambos conjuntos son, en realidad, el mismo. ■

Observación.– El Lema de Dickson se puede leer de la siguiente manera: todo ideal de A generado por monomios admite un sistema generador finito, resultado ya conocido por el Teorema de la base de Hilbert, que es mucho más general.

Para una correcta comprensión y fundamentación del concepto de base de Groebner es necesario acudir a los órdenes en $\mathbb{Z}_{\geq 0}^n$. En consecuencia vamos a estudiar brevemente algunos conceptos de utilidad en este sentido.

Definición 3.2 *Una relación de orden $<_{ord}$ se dice estable para la suma cuando verifica que es total y compatible con la adición i.e.:*

$$\alpha <_{ord} \beta \iff \left(\forall \gamma \in \mathbb{Z}_{\geq 0}^n,\ \alpha + \gamma <_{ord} \beta + \gamma \right).$$

Existen numerosos ejemplos de órdenes estables y no estables para la suma. Nosotros veremos a continuación dos ejemplos de los primeros, y uno de los segundos.

Ejemplo 3.5 *Se define el orden lexicográfico en $\mathbb{Z}_{\geq 0}^n$ como:*

$$\alpha <_{lex} \beta \iff \exists i,\ 1 \leq i \leq n \mid \alpha_1 = \beta_1, \ldots, \alpha_i = \beta_i,\ \alpha_{i+1} < \beta_{i+1}.$$

Este orden es estable para la suma.

Se define el orden lexicográfico inverso en $\mathbb{Z}_{\geq 0}^n$ como:

$$\alpha <_{lexinv} \beta \iff \exists i,\ 1 \leq i \leq n-1 \mid \alpha_n = \beta_n, \ldots, \alpha_i = \beta_i,\ \alpha_{i-1} < \beta_{i-1}.$$

Este orden también es estable para la suma.

Ejemplo 3.6 *Se define el orden producto en $\mathbb{Z}_{\geq 0}^n$ como:*

$$\alpha < \beta \iff \forall i, \alpha_i \leq \beta_i \ y\ \exists i_0 \mid \alpha_{i_0} < \beta_{i_0}.$$

Este orden no es total, luego no es estable para la suma. Este orden tiene la curiosa propiedad de que, si E es una escalera, $V(E)$ es el conjunto de elementos minimales para el orden producto.

Definición 3.3 *Sea $f \in A \setminus \{0\}$. Se define el diagrama de Newton de f, y se denota $DN(f)$ como el conjunto de todos los exponentes de los monomios de f distintos de cero.*

Sea $<_{ord}$ un orden estable para la suma y sea $f \in A \setminus \{0\}$. Entonces f se puede expresar en la forma

$$f = \sum_{\alpha \in DN(f) \subset \mathbb{Z}^n_{\geq 0}} a_\alpha X^\alpha.$$

Llamaremos exponente de f al elemento α, máximo para el orden $<_{ord}$ en el diagrama de Newton de f. Lo denotaremos por $exp(f)$.

Obsérvese que $exp(f)$ siempre existe (no ocurre si f es nulo),y es un elemento de $\mathbb{Z}^n_{\geq 0}$, porque $DN(f)$ ha de ser un conjunto finito.

Definición 3.4 *Se dice que un orden estable para la suma $<_{ord}$ es de eliminación en las variables $X_1, ..., X_i$ cuando se verifica que el exponente de todo monomio donde aparezcan estas variables es mayor que el exponente de cualquier monomio donde no aparezcan.*

Estos órdenes son especialmente útiles en nuestras aplicaciones a semigrupos numéricos. De los ejemplos anteriores, es sencillo ver que el orden lexicográfico es un orden de eliminación en las i primeras variables, para cualquier i. Por lo general esto se expresa diciendo que tomamos el orden lexicográfico $X_1 > X_2 > ... > X_n$.

Definición 3.5 *Sea $I \subset A$ un ideal no nulo. Se define el conjunto $E(I)$ como:*

$$E(I) = \{exp(f) \mid f \in I \setminus \{0\}\}.$$

Lema 3.2 *$E(I)$ es una escalera, para todo I ideal no nulo de $K[X_1, \ldots, X_n]$.*

Demostración: Sea $\alpha \in E(I)$. Hemos de probar que $\forall \beta \in \mathbb{Z}^n_{\geq 0}$, se tiene que $\alpha + \beta \in E(I)$. Pero, como $\alpha \in E(I)$, ha de existir $f \in I$ tal que $exp(f) = \alpha$. Considerando entonces el polinomio $X^\beta f$ para todo β de $\mathbb{Z}^n_{\geq 0}$ hallamos un elemento de I que tiene a $\alpha + \beta$ como exponente. ■

Llegamos por fin al concepto de base de Groebner (o base de Gröbner) aunque, en un principio, la definición no parece muy próxima a nuestros primeros objetivos.

Definición 3.6 *Dado I, ideal de A; diremos que $\{f_1, \ldots, f_k\} \subset I$ es una base de Groebner de I si verifica que:*

$$V(E(I)) \subset \{exp(f_1), \ldots, exp(f_k)\}.$$

Hay que observar algunos detalles importantes tras esta definición. En primer lugar, las bases *dependen del orden considerado*. Éste es, por tanto, uno de los puntos más delicados que hay que tener en cuenta al trabajar con bases de Groebner.

Ejemplo 3.7 *Sea el anillo $\mathbb{Q}[X, Y, Z]$ y el ideal $I = \langle XY + Y^2, X^2 \rangle$. ¿Forma este sistema de generadores una base de Groebner? Veremos cómo esta pregunta tiene diferentes respuestas en función del orden considerado. En primer lugar vamos a tomar el orden lexicográfico. Los exponentes de los elementos del sistema generador son*

$$\begin{array}{rcl} exp(XY + Y^2) & = & exp(f_1) = (1,1). \\ exp(X^2) & = & exp(f_2) = (2,0). \end{array}$$

Podemos dibujar la escalera generada por los exponentes del sistema generador, que no contiene puntos sobre el eje de ordenadas. Sin embargo véase que $Y^3 \in I$, ya que

$$Y^3 = Y f_2 + (Y - X) f_1.$$

Sin embargo $exp(Y^3)$ no se encuentra en la escalera generada por $exp(f_1)$ y $exp(f_2)$. Por lo tanto, el sistema generador no es una base de Groebner.

Vamos a considerar ahora el orden lexicográfico inverso. Los exponentes cambian en esta ocasión a

$$\begin{array}{rcl} exp(XY + Y^2) = & exp(f_1) & = (0,2). \\ exp(X^2) = & exp(f_2) & = (2,0). \end{array}$$

A diferencia del caso anterior, podemos observar ahora que, en la escalera inducida por $exp(f_1)$ y $exp(f_2)$, sólo dejamos fuera los términos (1,0), (0,1), (1,1) y (0,0). Pero si un polinomio tiene alguno de estos pares como exponente es sencillo comprobar que no puede pertencer al ideal. En consecuencia el sistema generador sí que es una base de Groebner.

En realidad, más adelante veremos un procedimiento menos artesanal para comprobar si un conjunto de polinomios es o no una base de Groebner del ideal que genera, pero este ejemplo es lo suficientemente ilustrativo como para resaltar la importancia del orden.

Otro detalle a tener en cuenta es el hecho, ya ilustrado por el ejemplo anterior, de que no cualquier sistema de generadores es una base de Groebner. En consecuencia, debemos intentar resolver dos problemas a continuación:

1. Cuándo un sistema generador es una base de Groebner.
2. Supuesto que no lo sea, cómo ampliar el conjunto a una base de Groebner.

Además tenemos aún pendiente el problema cuya resolución motivó el nacimiento de las bases de Groebner: cómo decidir si un polinomio dado está o no en un ideal generado por un conjunto conocido.

Para resolver estos problemas hemos de restringirnos un poco más en los órdenes que tomamos. Aunque las bases de Groebner se definen para una clase de órdenes más general, son los órdenes multiplicativos los que realmente nos van a servir para resolver los problemas propuestos.

Definición 3.7 *Llamamos orden multiplicativo en $\mathbb{Z}_{\geq 0}^n$ a un orden $<_{ord}$ tal que es estable para la suma y además verifica que*

$$\alpha <_{ord} \alpha + \beta, \quad \forall \beta \in \mathbb{Z}_{\geq 0}^n.$$

Se tiene entonces el siguiente resultado de cierta importancia:

Lema 3.3 *Los órdenes multiplicativos son buenos órdenes.*

Demostración: Supongamos que existe una sucesión estrictamente decreciente para un orden multiplicativo $<$ en $\mathbb{Z}_{\geq 0}^n$:

$$\alpha_1 > \alpha_2 > \ldots > \alpha_n > \ldots$$

Consideremos entonces E definido por

$$E = \bigcup_{p \in \mathbb{Z}_{\geq 0}} \left[\alpha_p + \mathbb{Z}_{\geq 0}^n\right].$$

Al ser E, por propia definición, una escalera, podemos aplicar el Lema de Dickson y sabemos que existen unos vértices $\{\beta_1, \ldots, \beta_s\}$ tales que

$$E = \bigcup_{i=1}^{n} \left[\beta_i + \mathbb{Z}_{\geq 0}^n\right].$$

Como $\{\alpha_p\}$ es infinito existe una $i,\ 1 \leq i \leq s$ tal que en $\beta_i + \mathbb{Z}_{\geq 0}^n$ hay infinitos α_p. Pero por ser único el conjunto de vértices minimales (ver prueba del Lema de Dickson) β_i ha de ser uno de los α_p, por ejemplo $\beta_i = \alpha_{p_0}$.

Por lo tanto, mayores que β_i sólo hay p_0 de los α_p, con lo cual llegamos a contradicción porque, hay infinitos α_p en $\beta_i + \mathbb{Z}_{\geq 0}^n$ y cada uno de ellos, por ser el orden multiplicativo, habría de ser mayor que β_i. ■

De los órdenes que hemos manejado tanto el lexicográfico como el lexicográfico inverso son multiplicativos.

Definición 3.8 *En $\mathbb{Z}_{\geq 0}^n$ definimos la siguiente partición:*

$$\begin{aligned}
\Delta_1 &= exp(f_1) + \mathbb{Z}_{\geq 0}^n. \\
\Delta_i &= \left[exp(f_i) + \mathbb{Z}_{\geq 0}^n\right] \setminus \left(\bigcup_{j<i} \Delta_j\right),\ 2 \leq j \leq t. \\
\overline{\Delta} &= \mathbb{Z}_{\geq 0}^n \setminus \left(\bigcup_{j=1}^{t} \Delta_j\right).
\end{aligned}$$

El siguiente resultado es fundamental y contiene toda la información necesaria para resolver los problemas que nos planteamos hace un momento. Para posteriores referencias lo llamaremos Teorema de la División.

Teorema 3.5 *Sea $<$ un orden multiplicativo en $\mathbb{Z}_{\geq 0}^n$, donde consideramos la partición anterior. Sean $f_1, \ldots, f_t \in A$, ninguno de ellos cero. Sea f un polinomio de A. Entonces existen $q_1, \ldots, q_t \in A$ y $h \in A$, únicos, verificando*

1. $f = q_1 f_1 + \ldots + q_t f_t + h$.
2. $DN(h) \subset \overline{\Delta}$.
3. $\forall i,\ 1 \leq i \leq t, \quad q_i \neq 0 \implies DN\left(q_i X^{exp(f_i)}\right) \subset \Delta_i$.

Demostración: Por ser $<$ un buen orden vamos a poder aplicar un procedimiento inductivo sobre $exp(f)$.

El caso $exp(f) = (0, \ldots, 0)$ es muy fácil, ya que en ese caso $f = a \in K$. Tomo entonces $q_i = 0$, $\forall i$, y $h = a$, en el caso de que ningún f_i sea constante. Estos polinomios verifican claramente 1, 2 y 3. Obsérvese que es necesario que no sea constante ningún f_i para que $N(h) \in \overline{\Delta}$. Caso de que algún f_i sea constante (llamémosle a_i), tomamos $h = q_j = 0$, para todo $j \neq i$ y $q_i = 1/a_i$. En este caso el apartado 2 del teorema queda vacío de contenido, ya que $\overline{\Delta} = \emptyset$ y $N(h)$ no existe propiamente.

La solución es única, en este caso, porque, si tomo $h \neq a$ y tengo unos ciertos q_i tales que

$$q_1 f_1 + \ldots + q_t f_t = f - h,$$

se tiene que, por un lado, como $f \in K$,

$$exp(f - h) = exp(h) \in \overline{\Delta};$$

pero también

$$exp(f - h) = exp(q_1 f_1 + \ldots + q_t f_t) = exp(q_i f_i),$$

para un determinado i. Esto es debido a que, por 3, los exponentes de la suma no pueden cancelarse entre sí, ya que los Δ_j son disjuntos.

En consecuencia

$$exp(f - h) \in \overline{\Delta} \bigcap \Delta_i,$$

de donde tenemos la contradicción buscada.

Supuesto demostrado el enunciado para todos los exponentes menores que el $exp(f)$ vamos a proceder a demostrarlo para éste.

Sea $\alpha = exp(f)$. Se sabe entonces que f es de la forma

$$f = aX^\alpha + \ldots,$$

y entonces podemos tener varias posibilidades.

Caso 1. Supongamos que $\alpha \in \overline{\Delta}$. Entonces consideremos el polinomio

$$g = f - aX^\alpha,$$

que verifica que $exp(f) > exp(g)$. Por hipótesis de inducción se tiene que

$$f - aX^\alpha = g = f_1 g_1 + \ldots + f_t g_t + h,$$

con los polinomios $g_1, \ldots, g_t, h$ únicos verificando el teorema. A partir de aquí es elemental ver que

$$f = q_1 f_1 + \ldots + q_t f_t + (h + aX^{\alpha})$$

es una expresión que verifica todas las condiciones del teorema. Además es sencillo ver que es única porque, de no serlo, encontramos otra expresión para g.

Caso 2. Supongamos por fin que $\alpha \in \Delta_i$, para un i único, por ser los Δ_i disjuntos dos a dos. En este caso sabemos entonces que existe un β tal que

$$\alpha = exp(f_i) + \beta.$$

Expresando entonces f_i en la forma

$$f_i = bX^{exp(f_i)} + \ldots,$$

podemos hacer entonces:

$$f - \frac{a}{b} X^{\beta} f_i = g; \text{ con } exp(g) < exp(f) \Rightarrow$$

$$f - \frac{a}{b} X^{\beta} f_i = q_1 f_1 + \ldots + q_t f_t + h \Rightarrow$$

$$f = q_1 f_1 + \ldots + \left(q_i + \frac{a}{b} X^{\beta}\right) f_i + \ldots + q_t f_t + h.$$

Análogamente a el caso anterior, tenemos que la expresión verifica las exigencias del teorema y, de no ser única, no lo sería la expresión de g, con lo cual debe serlo, por hipótesis de inducción. ■

Al procedimiento anterior se le suele denominar también reducción. Para fijar ideas vamos a ilustrar el procedimiento de manera más precisa con dos polinomios, f y g.

Decimos que g es reducible con respecto a f cuando el monomio líder de f (aquél que ostenta como expoenente $exp(f)$), que denotaremos por f_0 es un factor de un monomio m de g. Entonces sabemos que f es de la forma

$$f = c_0 f_0 + f_1,$$

donde $c_0 \in K$, y así mismo, m verifica que

$$m = p f_0.$$

Entonces vamos a reemplazar m en g por la expresión

$$\frac{-pf_1}{c_0},$$

con vistas a obtener un polinomio g_1. Entonces se verifica que

$$g - g_1 = m - \frac{-pf_1}{c_0} = \frac{mc_0 + pf_1}{c_0} = \frac{p(c_0 f_0 + f_1)}{c_0} \in \langle f \rangle.$$

Si g_1 también es reducible, repetimos el proceso y así hasta llegar a un g_s que no sea reducible, cosa que debe ocurrir porque estamos rebajando el exponente en cada paso.

Éste es, a grandes rasgos, el procedimiento que se usa para dividir de forma efectiva. Para un caso práctico hay que ir reduciendo primero con respecto a f_1, luego con respecto a f_2 y así sucesivamente hasta llegar al polinomio que hemos llamado h, que habrá de ser reducido con respecto a $f_1, \ldots, f_t$.

Definición 3.9 *El polinomio h se denomina forma normal de f respecto de $D = \{f_1, \ldots, f_t\}$ y se denotará por $N(f)$, cuando no haya lugar a la ambiguedad acerca del conjunto de divisores, o $N_D(f)$ cuando la haya.*

Al respecto de la unicidad del Teorema de la División hay que decir que, evidentemente, un cambio de orden entre las f_i induce un cambio entre las Δ_i pero se entiende que la unicidad se considera salvo permutaciones.

Ya podemos resolver entonces el problema que nos motivó al principio, mediante el siguiente resultado.

Proposición 3.1 *Sea I un ideal no nulo de A, $f_1, \ldots, f_t$ elementos de I. Son entonces equivalentes:*

1. *$\mathcal{B} = \{f_1, \ldots, f_t\}$ es una base de Groebner de I.*
2. *Para todo f de A; $f \in I \iff N_{\mathcal{B}}(f) = 0$.*

Demostración:

$1 \Leftarrow 2$. Sabemos que el conjunto de los f_i es base de Groebner, en consecuencia;

$$E(I) = \bigcup_{i=1}^{t} \left[exp(f_i) + \mathbb{Z}^n_{\geq 0} \right].$$

Sea entonces $h = N_{\mathcal{B}}(f)$, con $f \in I$. Vamos a demostrar que $h = 0$. Para ello hemos de observar que

$$N(h) = f - \sum_{i=1}^{t} q_i f_i,$$

con lo cual tenemos, por un lado, que $h \in I$ y, por tanto, $exp(h) \in E(I)$. Sin embargo, el Teorema de la División asegura que

$$exp(h) \in \overline{\Delta} = \mathbb{Z}_{\geq 0}^n \setminus \bigcup_{i=1}^{t} \Delta_i = \mathbb{Z}_{\geq 0}^n \setminus E(I),$$

con lo cual la única posibilidad para h es $h = 0$.

$2 \Leftarrow 1$. Vamos a suponer que el conjunto no es base de Groebner. Entonces, por definición

$$E(I) \setminus \bigcup_{i=1}^{t} \left[exp(f_i) + \mathbb{Z}_{\geq 0}^n\right] \neq \emptyset.$$

Por tanto hay un elemento α en ese conjunto. Pero, como $\alpha \in E(I)$ existe una f tal que $exp(f) = \alpha$. De aquí se deduce que $N_{\mathcal{B}}(f) \neq 0$, porque $exp(f) \in \overline{\Delta}$, con lo cual llegamos a contradicción con 2. ■

Observación.– Conviene notar que, de 2, es inmediato que toda base de Groebner es un sistema generador. El inverso ya sabemos que no es necesariamente cierto.

Ya tenemos entonces la respuesta a una de las preguntas que nos formulamos. Ahora nos queda resolver las otras dos, cosa que haremos construyendo un proceso algorítmico que, por un lado, verifique si el conjunto dado es o no una base de Groebner y, por otro lado, caso de no serlo, construya otro conjunto con más garantías de que lo sea.

Definición 3.10 *Dados f y g, polinomios de A, con $exp(f) = \alpha$, $exp(g) = \beta$, notemos*

$$f = aX^{\alpha} + \ldots, \quad g = bX^{\beta} + \ldots;$$

llamaremos término líder de f al sumando aX^{α}, notado $lt(f)$.

Llamaremos polinomio sicigia de f y g (o simplemente sicigia), y lo notaremos $S(f,g)$, al polinomio

$$bX^{\gamma-\alpha}f - aX^{\gamma-\beta}g;$$

donde $\gamma = (\gamma_1, \ldots, \gamma_n)$ con $\gamma_i = \max\{\alpha_i, \beta_i\}$.

Teorema 3.6 *Sea $(f_1, \ldots, f_t)$ ideal de A. Son equivalentes:*

1. *$\mathcal{B} = \{f_1, \ldots, f_t\}$ es base de Groebner.*
2. *$N_{\mathcal{B}}(S(f_i, f_j)) = 0$ para cualquier i y j en $\{1, \ldots, t\}$.*

Demostración: La implicación $1 \Rightarrow 2$ es inmediata, dado que las sicigias están, por su definición en el ideal. En consecuencia hay que demostrar la otra impicación. Lo haremos probando que la forma normal de un polinomio del ideal con respecto al sistema de generadores $\{f_1, \ldots, f_t\}$ es cero. Supongamos que tenemos un polinomio $f \in I$, siendo

$$g = N_{\mathcal{B}}(f) \neq 0,$$

con lo cual podemos escribir

$$g = \sum c_\alpha X^\alpha, \text{ con } X^\alpha \in \mathbb{Z}^n_{\geq 0} \setminus \bigcup_{i=1}^{t} \left[exp(f_i) + \mathbb{Z}^n_{\geq 0}\right],$$

cuando $c_\alpha \neq 0$, caso que se da en, al menos, un α.

Dado que el polinomio g pertenece también al ideal I, tenemos que g es de la forma

$$g = H_1 f_1 + \ldots + H_t f_t,$$

para ciertos polinomios H_j. Sea, en estas condiciones,

$$\omega = \max_{i \,|\, H_i \neq 0} exp(H_i f_i) \in \mathbb{Z}^n_{\geq 0}.$$

Si existiese un único i_0 tal que $\omega = exp(H_{i_0} f_{i_0})$, entonces tendríamos que ω es el exponente de g, con lo cual

$$exp(g) = \omega = exp(H_{i_0} f_{i_0}) \in exp(f_{i_0}) + \mathbb{Z}^n_{\geq 0},$$

lo cual contradice el Teorema de la División.

Por tanto han de existir unos números $i_0 < i_1 < \ldots < i_s$, con $s \geq 1$, tales que, para todo i de $\{i_0, i_1, \ldots, i_s\}$, se tenga que $exp(H_i f_i) = \omega$.

Sean, entonces,

$$\begin{array}{rclcrcl} lt(f_{i_0}) & = & \lambda_{i_0} X_1^{\alpha_1} \ldots X_n^{\alpha_n}, & & lt(H_{i_0}) & = & \nu_{i_0} X_1^{u_1} \ldots X_n^{u_n}, \\ lt(f_{i_1}) & = & \lambda_{i_1} X_1^{\beta_1} \ldots X_n^{\beta_n}, & & lt(H_{i_1}) & = & \nu_{i_1} X_1^{v_1} \ldots X_n^{v_n}. \end{array}$$

Sabemos, por hipótesis, que

$$(\alpha_1, \ldots, \alpha_n) + (u_1, \ldots, u_n) = (\beta_1, \ldots, \beta_n) + (v_1, \ldots, v_n) = \omega.$$

Definamos ahora

$$\gamma_i = \text{máx}(\alpha_i, \beta_i),$$

que verifica de forma inmediata que

$$\begin{array}{rcl} u_i \geq & \gamma_i - \alpha_i, & \forall 1 \leq i \leq n, \\ v_i \geq & \gamma_i - \beta_i, & \forall 1 \leq i \leq n. \end{array}$$

Consideremos a continuación

$$p_i = u_i - (\gamma_i - \alpha_i) = v_i - (\gamma_i - \beta_i),$$

igualdad que se demuestra simplemente considerando las dos posibilidades de γ_i.

Entonces se tiene que

$$S\left(X_1^{p_1} \ldots X_n^{p_n} f_{i_0}, f_{i_1}\right) = \lambda_{i_1} X^u f_{i_0} - \lambda_{i_0} X^v f_{i_1} = \frac{\lambda_{i_1}}{\nu_{i_0}} lt(H_{i_0}) f_{i_0} - \frac{\lambda_{i_0}}{\nu_{i_1}} lt(H_{i_1}) f_{i_1}.$$

Y, por consiguiente, podemos reescribir g de esta manera

$$\begin{array}{rcl} g & = & lt(H_{i_0}) f_{i_0} + lt(H_{i_1}) f_{i_1} + (H_{i_0} - lt(H_{i_0})) f_{i_0} + \\ & & \quad + (H_{i_1} - lt(H_{i_1})) f_{i_1} + \displaystyle\sum_{j \geq 2} f_{i_j} H_{i_j} + \sum_{i \neq i_0, \ldots, i_s} f_i H_i \\ & = & S\left(\dfrac{\nu_{i_0}}{\lambda_{i_1}} X^p f_{i_0}, f_{i_1}\right) + \left(1 + \dfrac{\nu_{i_0} \lambda_{i_0}}{\nu_{i_1} \lambda_{i_1}}\right) ML(H_{i_1}) f_{i_1} + (H_{i_0} - lt(H_{i_0})) f_{i_0} + \\ & & \quad + (H_{i_1} - lt(H_{i_1})) f_{i_1} + \displaystyle\sum_{j \geq 2} f_{i_j} H_{i_j} + \sum_{i \neq i_0, \ldots, i_s} f_i H_i. \end{array}$$

Para facilitar la notación vamos a renombrar algunos de los polinomios que nos han aparecido. Sean, para ello,

$$\begin{aligned} H'_{i_0} &= H_{i_0} - lt(H_{i_0}), \\ H'_{i_1} &= \frac{\nu_{i_0}\lambda_{i_0}}{\nu_{i_1}\lambda_{i_1}} lt(H_{i_1}) + H_{i_1}, \\ H'_i &= H_i \quad \text{para todo } i \neq i_0, i_1. \end{aligned}$$

En estas condiciones, veamos cómo han variado los exponenetes. En efecto, se tiene que

$$\begin{aligned} exp(H'_{i_0} f_{i_0}) &< \omega, \\ exp(H'_{i_1} f_{i_1}) &\leq \omega, \\ exp(H'_{i_j} f_{i_j}) &= \omega,\ j \geq 2, \\ exp(H'_i f_i) &< \omega,\ i \neq i_0, \ldots, i_s. \end{aligned}$$

Además, podemos escribir g en la forma

$$g = \frac{\nu_{i_0}}{\lambda_{i_1}} X^p S\left(f_{i_0}, f_{i_1}\right) + \sum H'_i f_i,$$

y hemos de hacer notar que

$$exp\left(X^p S\left(f_{i_0}, f_{i_1}\right)\right) = p + exp\left(S\left(f_{i_0}, f_{i_1}\right)\right) < p + \gamma = \omega,$$

donde la desigualdad se obtiene de manera elemental, dada la definición del polinomio sicigia. Pueden darse ahora varios casos:

1. $H'_i = 0$, para $i = 1, \ldots, t$, o
2. $\omega' = \text{máx}\{exp(H'_i f_i) \mid H'_i \neq 0\} < \omega$, o bien
3. $\omega' = \omega$.

Si se da el tercer caso, análogamente a la situación del comienzo de la demostración, se demuestra que han de existir $i', j' \in i_2, \ldots, i_s$ distintos, tales que

$$exp(H'_{i'} f_{i'}) = exp(H'_{j'} f_{j'}) = \omega = \omega'.$$

En cualquier caso, podemos asegurar que, tras una serie de cálculos semejantes a los hasta ahora efectuados (una serie finita porque el conjunto $i_0, \ldots, i_s$ es finito), hemos de llegar a poder escribir g en la forma

$$g = \sum_{i<j, i,j \in \{i_0,\ldots,i_s\}} \lambda_{ij} X^{q_{ij}} S(f_i, f_j) + \sum_i \tilde{H}_i f_i,$$

donde se verifica que, por un lado,

$$exp\left(X^{q_{ij}} S(f_i, f_j)\right) < \omega,$$

y, además, cuando $\tilde{H}_i \neq 0$, también se tiene que

$$\max_{i \,|\, \tilde{H}_i \neq 0} exp(\tilde{H}_i f_i) < \omega.$$

Dado que $S\left(f_i, f_j\right) \in (f_1, \ldots, f_t)$, tenemos que existen unos polinomios h_{ij}^l tales que

$$S\left(f_i, f_j\right) = \sum_{l=1}^{t} h_{ij}^l f_l,$$

de forma que

$$exp\left(S\left(f_i, f_j\right)\right) \geq exp(h_{ij}^l f_l),$$

y, por tanto, tenemos que

$$\omega > exp\left(X^{q_{ij}} S\left(f_i, f_j\right)\right) \geq exp(X^{q_{ij}} h_{ij}^l f_l).$$

Recapitulando, hemos obtenido una expresión de g en la forma

$$g = \sum \bar{H}_i f_i,$$

donde se tiene que

$$\omega_1 = \max_{i \,|\, \bar{H}_i \neq 0} exp(\bar{H}_i f_i) < \omega.$$

Por consiguiente, podemos crear una sucesión infinita decreciente de elementos de $\mathbb{Z}_{\geq 0}^n$, aplicando iteradamente este razonamiento. Dado que esto es imposible, tenemos demostrado lo que buscábamos. ■

En consecuencia, tenemos ya un procedimiento como el que queríamos. Este proceso, conocido como el algoritmo de Buchberger, permite obtener una base de Groebner a partir de un sistema generador dado. El algoritmo es el siguiente:

1. `INPUT`: $\mathcal{B} = \{f_1, \ldots, f_t\}$ sistema generador de I.
2. Considerar el conjunto $S = \{S\left(f_i, f_j\right) \mid 1 \leq i, j \leq t\}$.
3. Si $N_{\mathcal{B}}(f) = 0$ para todo $f \in S$, entonces $\mathcal{B}$ es base de Groebner.

4. `OUTPUT`: $\mathcal{B}$.

5. Caso contrario considerar el conjunto

$$\mathcal{B} \cup \{N_{\mathcal{B}}(f) \ : \ f \in S\},$$

y volver a 2.

El proceso debe terminar ya que, de lo contrario, existiría una cadena $\alpha_1 > \alpha_2 > \ldots$ infinita en $\mathbb{Z}^n_{\geq 0}$, lo cual es claramente imposible.

Como anotación final al algoritmo hemos de hacer notar que, en lenguaje de escaleras, sólo añadimos las formas normales de los polinomios sicigias porque son tan informativas como los polinomios completos y más sencillas (pues tienen menos términos) que éstos. El hecho de que sean tan informativas quiere decir que la diferencia entre un polinomio y su forma normal siempre va a estar (por el Teorema de la División) en la escalera inducida por G y, por consiguiente, no aporta nada nuevo a dicha escalera.

Observación.– El algoritmo bien puede devolvernos elementos de la base que sean redundantes; esto es, tales que al quitarlos seguimos teniendo una base de Groebner. Cuando retiramos estos elementos nos encontramos con una base de Groebner *minimal* (en algunos textos se considera minimal una base de Groebner cuyos términos líder tienen todos coeficiente 1). Al igual que las bases de Groebner en general, no existe una única base de Groebner minimal.

Teorema 3.7 *Sea I un ideal no nulo de A. Fijado un orden monomial multiplicativo $<$ existe una única base de Groebner $\mathcal{B}$ verificando las siguientes propiedades:*

- *Es minimal.*
- *Los términos líder de los elementos de $\mathcal{B}$ tienen coeficiente* 1.
- *Dado $g \in \mathcal{B}$ ningún monomio de f está en el ideal $\langle X^{exp(f)} \mid f \in \mathcal{B} \setminus \{g\}\rangle$.*

Esta base se denomina base de Groebner reducida para el orden $<$.

Demostración: Se puede ver en [9], 2.7. ∎

Observación.– La base reducida de Groebner es la que calculan, por defecto, la mayoría de los paquetes de cálculo simbólico, y por tanto la que aparece en toda la memoria cada vez que se realiza algún ejemplo concreto.

Observación.– Para terminar, ya que hablamos de las implementaciones de las bases de Groebner, hacemos notar que en muchos casos, los posibles órdenes se codifican en función de matrices, y nosotros así lo haremos ocasionalmente.

Sea $<_{ord}$ un orden en $\mathbb{N}^n$. Entonces decimos que la matriz $A \in \mathcal{M}(n \times m, \mathbb{Z}_{\geq 0})$ representa a $<_{ord}$ si y sólo si

$$\forall \alpha, \beta \in \mathbb{N}^n \text{ se tiene que } \alpha <_{ord} \beta \iff A \cdot \alpha^t <_{lex} A \cdot \beta^t,$$

donde $<_{lex}$ es el orden lexicográfico usual en $\mathbb{N}^m$.

Claramente la matriz identidad representa al orden $<_{lex}$, mientras que, por ejemplo, la matriz

$$A = \begin{pmatrix} 1 & 1 & ... & 1 & 1 \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 \end{pmatrix} \in \mathcal{M}(n \times n; \mathbb{Z}_{\geq 0})$$

representa el orden lexicográfico graduado.

Bibliografía

[1] Adams, W.W.; Loustaunau, Ph.: *An introduction to Gröbner bases.* American Mathematical Society, 1994.

[2] Apéry, R.: Sur les branches superlinéaires des courbes algébriques. *C. R. Acad. Sci. Paris* **222** (1946) 1198–1200.

[3] Beck, M.: Counting lattice points by means of the residue theorem. *Ramanujan J.* **4** (2000, 299–310.

[4] Beck, M.; Robins, S.: *Computing the continuous discretely. Integer-point enumeration in polyhedra.* Springer, 2007.

[5] Bras-Amorós, M.: Fibonacci–like behavior of the number of numerical semigroups of a given genus. *Semigroup Forum* **76** (2008) 379–384.

[6] Buchberger, B.: Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math.* **4** (1970) 374–383.

[7] Cortadellas, T.; Jafari, R.; Zarzuela, S.: On the Apéry sets of monomial curves. *Semigroup Forum* **86** (2013) 289–320.

[8] Cortadellas, T.; Zarzuela, S.: Apéry and micro–invariants of a one–dimensional Cohen–Macaulay local ring and invariants of its tangent cone. *J. Algebra* **328** (2011) 94–113.

[9] Cox, D.; Little, J.; O'Shea, D.: *Ideals, varieties and algorithms.* Springer, 1992.

[10] Eisenbud, D.; Sturmfels, B.: Binomial ideals. *Duke Math. J.* **84** (1996) 1–45.

[11] Ehrhart, E.: Sur les polyèdres rationnels homothétiques à n dimensions. C. R. Acad. Sci. Paris **254** (1962) 616–618.

[12] García–Sánchez, P.A.; Rosales, J.C.: *Numerical semigroups*. Springer, 2009.

[13] Hardy, G. H.; Littlewood, J. E.: Some problems of Diophantine approximation: The lattice-points of a right-angled triangle. *Abh. Math. Sem. Univ. Hamburg* **1** (1922) 211–248.

[14] Hironaka, H.: Resolution of singularities of an algebraic variety over a field of characteristic zero (I–II). *Ann. of Math. (2)* **79** (1964) 109–326.

[15] Kaplan, N.: Counting numerical semigroups by genus and some cases of a question of Wilf. *J. Pure Appl. Algebra* **216** (2012) 1016–1032.

[16] Kunz, A.: The value–semigroup of a one-dimensional Gorenstein ring. Proc. Amer. Math. Soc. **25** (1970) 748–751.

[17] Lin, K.P.; Yau, S.T.: Analysis of sharp polynomial upper estimate of number of positive integral points in 4–dimensional tetrahedra. *J. Reine Angew. Math.* **547** (2002) 191–205.

[18] Lin,K.P.; Yau, S.T.: Analysis of sharp polynomial upper estimate of number of positive integral points in 5–dimensional tetrahedra. *J. Number Theory* **93** (2002) 207–234.

[19] Lin, K.P.; Yau, S.S.T.: Counting the number of integral points in general n–dimensional tetrahedra and Bernoulli polynomials. *Canad. Math. Bull.* **24** (2003) 229–241.

[20] Madero–Craven, M.; Herzinger, K.: Apéry sets of numerical semigroups. *Comm. Algebra* **33** (2005) 3831–3838.

[21] Nijenhuis, A.; Wilf, H.S.: Representations of integers by linear forms in nonnegative integers. *J. Number Theory* **4** (1972) 98–106.

[22] Pick, G.A.: Geometrisches zur Zahlenlehre, Sitzungsber. Lotos (Prague) **19** (1989) 311–319.

[23] Ramírez–Alfonsín, J.L.: Complexity of the Frobenius problem. *Combinatorica* **16** (1996) 143–147.

[24] Ramírez–Alfonsín, J.L.: *The Diophantine Frobenius problem.* Oxford University Press, 2005.

[25] Ramrez–Alfonsín, J.L.; Rodseth, O.J.: Numerical semigroups: Apéry sets and Hilbert series. *Semigroup Forum* **79** (2009) 323–340.

[26] Reeve, J.E.: On the volume of the lattice polyhedra. Proc. London Math. Soc. **7** (1957) 378–395.

[27] Rosales, J.C.; García–Snchez, P.A.; García–García, J.I.; Branco, M. B.: Numerical semigroups with a monotonic Apéry set. *Czechoslovak Math. J.* **55** (2005) 755–772.

[28] Sammartano, A.: Numerical semigroups with large embedding dimension satisfy Wilf's conjecture. *Semigroup Forum* **85** (2012) 439–447.

[29] Sylvester, J.J.: Problem 7382. *Educational Times* **37** (1884) 26.

[30] Van der Poorten, A.: A proof that Euler missed. *The Mathematical Intelligencer* **1** (1979) 195–203.

[31] Wang, X.; Yau, S.S.T.: On the GLY conjecture of upper estimate of positive integral points in real right-angled simplices. *J. Number Theory* **122** (2007) 184–210.

[32] Wilf, H.S.: A circle–of–lights algorithm for the money changing problem. *Amer. Math. Monthly* **85** (1978) 562–565.

[33] Xu, Y.J.; Yau, S.S.T.: A sharp estimate of number of integral points in a tetrahedron. *J. Reine Angew. Math.* **423** (1992) 199–219.

[34] Xu, Y.J.; Yau, S.S.T.: Durfee conjecture and coordinate free characterization of homogeneous singularities. *J. Differential Geom.* **37** (1993) 375–396.

[35] Xu, Y.J.; Yau, S.S.T.: A sharp estimate of number of integral points in a 4–dimensional tetrahedra. *J. Reine Angew. Math.* **473** (1996) 1–23.

[36] Yau, S.S.T.; Zhang, L.: An upper estimate of integral points in real simplices with an application to singularity theory. *Math. Res. Lett.* **13** (2006) 911–921.