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

Tesis de Licenciatura

Polítopos y Funciones Generatrices Racionales

Martín Mereb
mmereb@promail.com.ar

Directora: Dra. Alicia M. Dickenstein
Codirector: Dr. Matías A. Graña

Agosto de 2006

Agradecimientos:

Antes que nada, quiero agradecer al jurado por saltearse esta parte.

A mi directora Alicia y a mi co-director Matías, por la increíble paciencia y buena onda que muestran.

A mi familia por bancarme siempre, incluso cuando ni yo me aguanto.

A Dano, mi mejor amigo, por ayudarme a superar mi pánico a los polinomios, porque siempre estuvo y siempre estará.

A Jonny, compañero de aventuras, por darme una mano en todo momento. A Enzo, por prestarme sus apuntes y transmitir siempre esa calma que lo caracteriza. A Angie, por sus palabras, por su tiempo, y por aceptarme como soy.

A la OMA, en especial a Flora y Patricia, por permitirme descubrir a temprana edad lo lindo de esta ciencia.

Al Huergo y todo su staff, por las oportunidades que me dieron y los buenos momentos que me hicieron pasar. Al personal docente, por todo lo que aprendí. Y en especial a Gustavo, por enseñarme más de lo que cree.

A ORT y sus alumnos, por abrirme las puertas y darme tantas alegrías.

A Willie, Juan, Gabriel, Carlos, Eduardo, Fernando, Ariel, Gabriela, Teresa, Lisi y Silvia, por sus charlas extracurriculares, sus consejos de vida y por recordarme todo lo que hago mal.

A Matilde por su asesoramiento a distancia. A Flavia, por explicarme algo de grafos. Y a Irene Loiseau por conseguirme un paper.

A Michele Vergne, Matthias Beck, Sinai Robins y Kádár István, no sólo por no haber tirado mis e-mails a la carpeta de SPAM, sino por haberlos contestado.

Y a mis amigos Lean, Eduardo, Vicky, José Luis, Magui, Lau, Isa, Silvia, Abi, Juliana, Mara, Ezequiel, Seba, Nico, Pablo, Martín, Sergio, Pancho, Matías, Quique, Gaby, Vale, Caro, Santiago y Juan Pablo, por sus preguntas molestas, su sinceridad, por escoltarme en esta travesía y por hacer que todo sea más fácil.

Índice general

Capítulo 0

Introducción.

En el presente trabajo abordamos problemas relacionados con sistemas de inecuaciones lineales, cantidad de soluciones enteras y el comportamiento de las funciones que calculan dichas cantidades para ciertas familias de sistemas parametrizados. Nos proponemos demostrar que en varios ejemplos concretos, dichas funciones se pueden describir con polinomios y estudiar las maneras conocidas de hallarlos.

La riqueza de la Matemática moderna permite atacar estos problemas integrando herramientas de Geometría, Aritmética, Combinatoria y Análisis, brindando diferentes perspectivas de un mismo tema.

También estudiamos una manera muy importante en la actualidad de representar el conjunto de soluciones enteras de un sistema dado, siguiendo el resultado de Brion [14] y las cuestiones técnicas de la implementación del algoritmo de Barvinok (ver [22] y [20]).

Comenzaremos mencionando algunos problemas famosos de enumeración, de un planteo netamente elemental.

Coloreo de mapas y grafos

Supongamos que queremos colorear un mapa con 4 colores sin que países limítrofes tengan el mismo color: ¿de cuántas maneras podemos hacerlo? ¿y el mismo mapa con 5 colores? ¿y en general con $n \in \mathbb{N}$?

Sin detenernos acá, dado un *grafo*[1] $G = (V, E)$ y un número $n \in \mathbb{N}$, es bien sabido que el número de coloreos de G que no pintan del mismo color los vértices de ninguna arista, viene dado por un polinomio $\chi(n)$ denominado *polinomio cromático* de G. Cabe destacar que existen interpretaciones de los valores que alcanza dicho polinomio en los enteros negativos (por ejemplo, $|\chi(-1)|$ coincide con la cantidad de orientaciones acíclicas del grafo G).

Cuadrados semi-mágicos

Todos vimos alguna vez un arreglo cuadrado de 3×3 con los números del 1 al 9 donde las filas columnas y diagonales sumaban 15, y acordamos en llamarlo "mágico". Pidiendo un poco menos, se define *cuadrado semi-mágico* de $k \times k$ a una matriz de $\mathbb{Z}^{k\times k}$ tal que sus filas y columnas suman lo mismo. Fijando k y dado $n \in \mathbb{N}$, nos preguntamos cuántos cuadrados semi-mágicos se pueden conseguir con sus coordenadas en $\{0, 1, \ldots, n\}$. Llamando $Csm_k(n)$ a dicho número, veremos que también es un polinomio en n (de grado $(k-1)^2$). Y si notamos $Csm_k^\circ(n)$ a la cantidad de cuadrados semi-mágicos con coordenadas positivas, menores o iguales que n, si bien está claro que $Csm_k^\circ(n) = Csm_k(n-k)$, también concluiremos que $Csm_k^\circ(n) = (-1)^{(k-1)^2} Csm_k(-n)$, es decir, se tiene una interpretación combinatoria de los valores de $Csm_k(n)$ en números negativos.

El problema de Frobenius del cambio con monedas

Tenemos monedas de $1, 5, 10, 25, 50$ y 100 centavos. Si queremos dar un vuelto de 50 centavos, tenemos varias maneras de hacerlo (con una moneda de 50, diez de 5, o una de 25 y el resto de 1, etc.). ¿Cuántas formas hay?

Más en general, el problema de Frobenius del cambio con monedas consiste en contar la cantidad de maneras distintas de pagar n centavos, teniendo una cantidad indiscriminada de monedas de ciertos valores $\{a_1, a_2, \ldots, a_k\} = A \subseteq \mathbb{N}$. Llamando $p_A(n)$ a dicha cantidad, se tienen $p_{\{1,5,10,25,50,100\}}(50)$ formas de dar un vuelto de 50 centavos.

Siendo precisos: $p_A(n) = \sharp\{m \in \mathbb{N}_0^k / \sum_{i=1}^k a_i m_i = n\}$, que puede interpretarse como la cantidad de puntos enteros de $P = \{x \in \mathbb{R}^k / x_i \geq 0, \sum_{i=1}^k a_i x_i = n\}$.

[1] es decir, un conjunto V de vértices y otro $E \subseteq G \times G$ de aristas

Observemos que $p_A(n)$ en general *NO* es un polinomio en n. Por ejemplo, si sólo tenemos monedas de 5 no podremos pagar 32 centavos. Se tiene que:

$$p_{\{5\}}(n) = \begin{cases} 1 & \text{si } \frac{n}{5} \in \mathbb{N} \\ 0 & \text{si } \frac{n}{5} \notin \mathbb{N} \end{cases}$$

que es una función periódica en n.

Llegamos así a la:

Definición 0.0.1 *Llamaremos* cuasi-polinomio de período n y grado d *a una sucesión* $f(t)$ *de la forma* $f(t) = \sum_{j=0}^{d} p_j(t)t^j$ *donde los coeficientes* p_j *son funciones periódicas, de período* $n \in \mathbb{N}$*, y* $p_d \not\equiv 0$*.*

Observación 0.0.2 *Las funciones periódicas son casos particulares de cuasi-polinomios.*

Polítopos y Programación lineal entera

Inspirados en el problema de Frobenius, llegamos a uno de los problemas clásicos de Programación Lineal Entera. Nos preguntamos si, dado un sistema de desigualdades, éste admite solución entera, y en dicho caso cuántas.

Podemos interpretar al sistema como un convexo $P = \{x \in \mathbb{R}^d / Ax \leq b\} \subseteq \mathbb{R}^d$ con $b \in \mathbb{R}^m$ y $A \in \mathbb{R}^{m \times d}$ y $Ax \leq b$ debe entenderse como como una desigualdad coordenada a coordenada. Nuestro problema ahora sería hallar $\sharp(P \cap \mathbb{Z}^d)$.

A menudo se tiene que P es compacto y, siendo $\mathbb{Z}^d$ discreto, $P \cap \mathbb{Z}^d$ será un conjunto finito de puntos (eventualmente vacío).

Definición 0.0.3 *Un* polítopo $P \subseteq \mathbb{R}^d$ *es un subconjunto compacto de* $\mathbb{R}^d$ *dado por un sistema de inecuaciones* $P = \{x \in \mathbb{R}^d / Ax \leq b\}$*.*

Observación 0.0.4 *Un polítopo puede darse o bien por un sistema de inecuaciones, o bien como la clausura convexa de un subconjunto finito de* $\mathbb{R}^d$ *(ver [40], para detalles). El primer modo tiene como desventaja el no saber a priori si dicho sistema describe o no un subconjunto acotado.*

Los problemas de enumeración antes mencionados, pueden llevarse a contar puntos enteros en un polítopo P y sus dilatados $nP = \{nx/x \in P\}$.

- El problema de los cuadrados semi-mágicos consiste en hallar $Csm_k(n) = \sharp(nP \cap \mathbb{Z}^{k\times k})$ donde P es el polítopo descripto por $\{M \in \mathbb{R}^{k\times k}/\mathbf{1}M = \mathbf{1}M^t = \mathbf{1}, M_{ij} \geq 0\}$, siendo $\mathbf{1} = (1, 1, \ldots, 1)$. Está claro que P resulta compacto, pues todas sus coordenadas quedan entre 0 y 1. También puede verse como la clausura convexa de las matrices de permutación.

- El problema de Frobenius se plantea como $p_A(n) = \sharp\{m \in \mathbb{N}_0^k/\sum_{i=1}^k a_i m_i = n\}$, pero $\{m \in \mathbb{N}_0^k/\sum_{i=1}^k a_i m_i = n\} = nP \cap \mathbb{Z}^k$ con $P = \{x \in \mathbb{R}^k/x_i \geq 0, \sum_{i=1}^k a_i x_i = 1\}$, que resulta acotado pues suponemos que los a_i son positivos.

- El caso del polinomio cromático de $G = (V, E)$ es un poco más rebuscado, pero puede verse a $\chi(n)$ como $\sharp(\mathbb{Z}^{\sharp V} \cap (n-1)P)$ con $P = \{x \in \mathbb{R}^V/0 \leq x_v \leq 1, x_v \neq x_w \forall (v, w) \in E\}$. Si bien no es un polítopo, puede pensarse como el cubo $[0, 1]^V$ menos los polítopos $[0, 1]^V \cap \{x_v = x_w\}$ para toda arista $(v, w) \in E$.

En el Capítulo 1 veremos algunas consecuencias del resultado de Ehrhart [23], que asegura que el número de puntos enteros en los dilatados de un polítopo dado por inecuaciones a coeficientes enteros, viene dado por un cuasi-polinomio, dando también condiciones suficientes para que dicho cuasi-polinomio resulte ser un polinomio.

En el Capítulo 2 veremos una demostración del Teorema de Ehrhart, que involucra el uso de funciones generatrices. También veremos que los valores del cuasi-polinomio evaluado en los números negativos, coinciden (salvo signo) con el número de puntos enteros en el interior relativo del polítopo P.

En el Capítulo 3 damos una demostración elemental del Teorema de Brion. Antes de ella vemos algunos hechos que surgen de explotar este resultado. Entre otras cosas, deducimos la fórmula (3.3) para calcular volúmenes de polítopos simples a partir del Teorema de Brion, y basándonos en las ideas de Barvinok [4] damos otra forma de llegar a la misma.

En el Capítulo 4 centramos la atención en el algoritmo de Barvinok, escencial para el cálculo efectivo de las funciones generatrices, así como los detalles que hicieron posible la implementación de dicho algoritmo en el sistema LattE [20].

En el Capítulo 5 mencionamos otro punto de vista, que surge al generalizar las fórmulas de Euler-MacLaurin a mayores dimensiones, permitiendo así considerar problemas de enumeración de naturaleza más complicada.

Y en el Capítulo 6 mencionamos un paralelo a la Teoría de Ehrhart, algo más geométrica, que considera el cálculo de volúmenes discretos en lugar de cantidad de puntos enteros, y goza de una serie de resultados análogos.

En el Apéndice A, de sucesiones recursivas lineales, establecemos las herramientas y la notación que usamos en el Capítulo 3 para deducir el Teorema de Ehrhart a partir del de Brion, y cómo usar esa idea para generalizar el resultado a sumas de Minkowski de varios Polítopos (Corolario 3.1.2).

En el Apéndice B repasamos las bases de la Teoría de problemas $NP-$completos (siguiendo el enfoque de [26]), explicando la importancia de la hipótesis de dimensión fija en el algoritmo de Barvinok.

Por último, en el Apéndice C describimos el algoritmo LLL [33], herramienta sugerida por Dyer y Kannan en [22], y usada por los autores de [20] en la implementación del algoritmo de Bravinok.

Entre la bibliografía consultada, los libros más importantes son el de Beck y Robins [11] y el de A. Barvinok [5]. El primero engloba la mayoría de los temas teóricos, desde un punto de vista combinatorio y elemental, y el segundo trata las cuestiones geométricas y algorítmicas.

Capítulo 1

Polinomios de Ehrhart

En el presente capítulo, deduciremos algunas propiedades elementales que se desprenden del resultado de Ehrhart. Usaremos la siguiente notación:

Definición 1.0.5 *Sea P un polítopo, llamamos $relint(P) = P^\circ$ al interior de P relativo al subespacio afín que genera. Si P es un punto, consieramos $P^\circ = P$.*

Las caras *de un polítopo $P \subseteq \mathbb{R}^d$ son los subconjuntos de P donde se maximiza algún funcional $\phi(x) =< u, x >$.*

La dimensión *$dim(F)$ de una cara F se define como la dimensión del espacio afín generado por F.*

Observemos que P es la cara de P donde se maximiza el funcional nulo.

Como casos particulares tenemos los vértices*, que son las caras puntuales, o sea las de dimensión* 0*. Notamos $Vert(P)$ al conjunto de vértices.*

Llamamos aristas *a las caras de dimensión* 1 *y* facetas *a las de codimensión* 1 *(es decir, aquellas tales que su dimensión es uno menos que la de P).*

Definición 1.0.6 *Un polítopo $P \subseteq \mathbb{R}^d$ se dice* entero *si sus vértices tienen coordenadas enteras. Se dice* racional *si sus vértices tienen coordenadas racionales, o equivalentemente, si puede describirse como las soluciones de un sistema de inecuaciones $\{Ax \leq b\}$ donde los*

coeficientes de A y de b están en $\mathbb{Q}$. Llamamos denominador *de P a algún $n \in \mathbb{N}$ tal que nP es entero.*

Definición 1.0.7 *Un* cono centrado en 0 *es un semigrupo de $\mathbb{R}^d$ cerrado por la multiplicación de $\mathbb{R}^+ = \{r \in \mathbb{R} / r \geq 0\}$.*

Extendemos la definición de cono, permitiendo trasladar el origen a otro vector $v \in \mathbb{R}^d$, tomando por ejemplo $K + v$ con K un cono centrado en 0.

Diremos que el cono es poliedral *si está generado por finitos vectores, y que es* racional poliedral *si se pueden elegir dichos vectores en $\mathbb{Q}^d$.*

El cono se dirá simplicial *si está generado por un conjunto de vectores linealmente independiente.*

Se dice que el cono K centrado en 0 es punteado *si no contiene subespacios de dimensión mayor a cero, es decir si $K \cap -K = \{0\}$.*

Se definen dimensión, cara *y* faceta *para conos poliedrales de manera análoga a los polítopos. Denominamos* rayos *a las aristas del cono.*

Definición 1.0.8 *Dado un punto p del polítopo P, se define el* cono sobre p *como $K_p = p + \mathbb{R}^+(P - p)$. Más generalmente, dada una cara F llamamos* cono sobre F *al cono $K_F = K_p$, para algún*[1] *$p \in relint(F)$. Se dice que un polítopo P es* simple *si los conos sobre sus vértices resultan simpliciales.*

Definición 1.0.9 *Una* triangulación *de un polítopo P es un conjunto de símplices tales que su unión da P, sólo pueden intersecarse en caras comunes y no utilizan otros vértices salvo los de P. Análogamente, una* triangulación *de un cono poliedral punteado K es un conjunto de conos simpliciales tales que su unión da K, sólo se intersecan en caras comunes y no se usan nuevos rayos.*

Nos será de utilidad saber que podemos triangular polítopos y conos racionales (para más detalles ver [40], [5] o [11]).

[1] es fácil ver que no depende del punto p elegido.

Sea P un polítopo en $\mathbb{R}^d$ y supongamos de momento que es entero y de dimensión d. Para cada $t \in \mathbb{N}$ consideramos

$$L_P(t) = \sharp(tP \cap \mathbb{Z}^d),$$

la cantidad de puntos con coordenadas enteras del $t-$ésimo dilatado de P. En el próximo capítulo veremos que la función L_P depende polinomialmente de t. Se la llama *polinomio de Ehrhart de* P en honor a su descubridor E. Ehrhart [23].

Veamos primero que dicho polinomio necesariamente debe tener grado d y su coeficiente principal ser $vol(P)$.

Está claro que P contiene a un $(d+1)-$simplex entero (no degenerado), por lo que $(d+1)P \cap \mathbb{Z}^d$ contendrá al menos un punto interior a $(d+1)P$. Dilatanto más, de ser necesario, podemos suponer que existe un $k \in \mathbb{N}$ tal que kP contiene un cubo de lado 1 centrado en un $p \in kP$, es decir $B^{\|\cdot\|_\infty}(p, \frac{1}{2}) \subseteq kP$ (la bola abierta respecto de la norma infinito, de centro p y radio $1/2$).

Como P es convexo, para cada $t \in \mathbb{N}$ tenemos que $(t+k)P = tP + kP$. Entonces, para cada punto $q \in tP$ tendremos $B^{\|\cdot\|_\infty}(p+q, \frac{1}{2}) \subseteq (t+k)P$. En particular $p + tP \subseteq (t+k)P$ y haciendo a q recorrer los puntos de $tP \cap \mathbb{Z}^d$ tendremos un conjunto

$$C_t = \bigcup_{q \in tP \cap \mathbb{Z}^d} \overline{B}^{\|\cdot\|_\infty}(p, \frac{1}{2})$$

que verifica $tP \subseteq C_t \subseteq (t+k)P$ y, por ende, $vol(tP) \leq vol(C_t) \leq vol((t+k)P)$.

Como C_t tiene un cubo por cada punto de entero de tP, se tiene que $vol(C_t) = L_P(t)$ de donde:

$$\begin{aligned} vol(tP) \leq &\quad vol(C_t) &&\leq vol((t+k)P) \\ vol(P)t^d \leq &\quad vol(C_t) &&\leq vol(P)(t+k)^d \\ vol(P)t^d \leq &\quad L_P(t) &&\leq vol(P)(t+k)^d \end{aligned}$$

para todo $t \in \mathbb{N}$, por lo que $L_P(t) = vol(P)t^d + o(t^d)$. Sabiendo que $L_P(t)$ es un polinomio en t, llegamos a que su grado es d y su coeficiente principal $vol(P)$.

También veremos en el Capítulo 2 que los valores que toma $L_P(t)$ para $t < 0$ tienen también una interpretación combinatoria dada por la llamada *Reciprocidad de Ehrhart-MacDonald* (cfr. Teorema 2.2.5): $L_P(-t) = (-1)^d L_P^\circ(t)$, donde $L_P^\circ(t) = \sharp(tP^\circ \cap \mathbb{Z}^d)$.

Como consecuencia de dicha reciprocidad tenemos una caracterización del coeficiente de grado $d-1$ de $L_P(t)$.

Sea $\mathcal{F}$ el conjunto de caras de P, y $\mathcal{F}_m$ el de caras de dimensión m. Como $P = \bigcup_{F\in\mathcal{F}} F^\circ$ y se tiene la misma descomposición para los dilatados de P, llegamos a que $L_P(t) = \sum_{F\in\mathcal{F}} L_F^\circ(t)$ para todo $t \in \mathbb{N}$ y por lo tanto, dicha igualdad pasa a ser una identidad polinomial.

Por la reciprocidad del Teorema 2.2.5, llegamos a $L_P(t) = \sum_{F\in\mathcal{F}} (-1)^{dimF} L_F(-t)$. Los únicos términos de grado $d-1$ en el miembro derecho provienen de los polinomios de Ehrhart de P y sus facetas. Llamando c_{d-1} al coeficiente de grado $d-1$ de $L_P(t)$ tenemos que:

$$\begin{aligned}
c_{d-1} &= (-1)^{dimP} c_{d-1}(-1)^{d-1} + \sum_{F\in\mathcal{F}_{d-1}} (-1)^{dimF} vol(F)(-1)^{d-1} \\
c_{d-1} &= (-1)^{d+d-1} c_{d-1} + \sum_{F\in\mathcal{F}_{d-1}} (-1)^{d-1+d-1} vol(F) \\
c_{d-1} &= -c_{d-1} + \sum_{F\in\mathcal{F}_{d-1}} vol(F) \\
2c_{d-1} &= \sum_{F\in\mathcal{F}_{d-1}} vol(F) \\
c_{d-1} &= \frac{1}{2} \sum_{F\in\mathcal{F}_{d-1}} vol(F) = \frac{1}{2} vol(\partial P)
\end{aligned}$$

donde $vol(F)$ representa al volumen de F relativo al subespacio afín y la última igualdad debe tomarse como definición de $vol(\partial P)$.

Otra consecuencia importante es la fórmula:

$$vol(P) = \frac{1}{d!} \sum_{k=0}^{d} (-1)^{d-k} \binom{d}{k} \sharp((k+n)P \cap \mathbb{Z}^d) \tag{1.1}$$

donde n es cualquier entero y $(-m)P$ debe interpretarse aquí[2] como mP° y $0P = \{0\}$, que proviene de observar que ambos miembros son el coeficiente principal de $L_P(t) = \sharp(tP \cap \mathbb{Z}^d)$

[2] recordar que, en general $\lambda P = \{\lambda p / \ p \in P\}$ para cualquier $\lambda \in \mathbb{R}$

(ver Apéndice A, fórmulas (A.2) y (A.1)).

Reescribiendo obtenemos:

$$vol(P) = \frac{1}{d!}\sum_{k=0}^{d}(-1)^{d-k}\binom{d}{k}\sharp(P \cap \frac{1}{k+n}\mathbb{Z}^d), \tag{1.2}$$

donde $\frac{1}{m}\mathbb{Z}^d$ es un lattice de $\mathbb{R}^d$ más fino que $\mathbb{Z}^d$, si $m > 0$, y para $m < 0$ debe interpretarse $P \cap \frac{1}{m}\mathbb{Z}^d$ como $P^\circ \cap \frac{1}{-m}\mathbb{Z}^d$, y tomamos $P \cap \frac{1}{0}\mathbb{Z}^d = \{0\}$ como notación.

En el caso particular de $\mathbb{R}^2$ con $n = -1$ tenemos:

$$\begin{aligned} A(P) = vol(P) &= \frac{1}{2}\sum_{k=0}^{2}(-1)^{2-k}\binom{2}{k}\sharp((k-1)P \cap \mathbb{Z}^d) \\ &= \frac{1}{2}\binom{2}{0}\sharp((-1)P \cap \mathbb{Z}^d) - \frac{1}{2}\binom{2}{1}\sharp(0P \cap \mathbb{Z}^d) + \frac{1}{2}\binom{2}{2}\sharp(P \cap \mathbb{Z}^d) \\ &= \frac{1}{2}\sharp(P^\circ \cap \mathbb{Z}^d) - 1 + \frac{1}{2}\sharp(P \cap \mathbb{Z}^d) \\ &= \sharp(P^\circ \cap \mathbb{Z}^d) - 1 + \frac{1}{2}\sharp(\partial P \cap \mathbb{Z}^d), \end{aligned}$$

que es la conocida fórmula de Pick.

Es oportuno mencionar que unos pocos años antes de publicarse el resultado de Ehrhart, ya había generalizaciones del Teorema de Pick para dimensión 3 ([35] y [36]) que consideraban lattices más finos que $\mathbb{Z}^3$, similares a la fórmula (1.2).

Capítulo 2

Funciones generatrices

En este capítulo hablaremos de funciones generatrices de conjuntos de $\mathbb{R}^d$ y cómo utilizarlas para dar una demostración del Teorema de Ehrhart, a raíz del Teorema de Positividad de Stanley 2.2.1 y de la Recipricidad de Ehrhart-MacDonald 2.2.5.

Antes de hablar de funciones generatrices de subconjuntos de $\mathbb{R}^d$ veamos cómo asociar series formales de Laurent a funciones racionales en varias variables.

Notamos $\mathbb{C}[z] = \mathbb{C}[z_1, \ldots, z_d]$ al anillo de polinomios y $C[z^{\pm}] = \mathbb{C}[z_1^{\pm}, \ldots, z_d^{\pm}]$ al de polinomios de Laurent.

Llamamos $\mathbb{C}[[z]] = \mathbb{C}[[z_1, \ldots, z_d]]$ a la $\mathbb{C}-$álgebra de series de potencias, o series formales, compuesta por sumas $f = \sum_{\alpha \in \Omega} k_\alpha z^\alpha$ con $k_\alpha \in \mathbb{C}$, $sop(f) = \{\alpha \in \Omega / k_\alpha \neq 0\} \subseteq \mathbb{N}_0^d$ es el soporte de f y si $\alpha = (\alpha_1, \ldots, \alpha_d)$ notamos z^α al monomio $z_1^{\alpha_1} \ldots z_d^{\alpha_d}$, con la suma y producto definidas de la manera natural.

En el caso de $\mathbb{C}[[z^{\pm}]] = \mathbb{C}[[z_1^{\pm}, \ldots, z_d^{\pm}]]$ (definido de manera similar, permitiendo $\Omega \subseteq \mathbb{Z}^d$), el producto podría no estar definido (a diferencia de la suma, que sigue teniendo sentido). Por ejemplo, en $\mathbb{C}[[t^{\pm}]]$ el producto $(\sum_{n<0} t^n)(\sum_{n>0} t^n)$ no puede calcularse distribuyendo, pues tendríamos infinitos términos de grado 0.

Sin embargo, se puede considerar el producto de una $f \in \mathbb{C}[[z^{\pm}]]$ por una $g \in \mathbb{C}[z^{\pm}]$ dando a $\mathbb{C}[[z^{\pm}]]$ estructura de $\mathbb{C}[z^{\pm}]-$módulo.

Dados dos elementos $f_1, f_2 \in \mathbb{C}[[z^{\pm}]]$, diremos que pueden multiplicarse si al distribuir sólo tenemos que sumar finitos términos para cada monomio, es decir, siendo $f = \sum_{\beta\in\Omega_1} k_\beta z^\beta$ y $g = \sum_{\gamma\in\Omega_2} \lambda_\gamma z^\gamma$, en la expresión

$$fg = (\sum_{\beta\in\Omega_1} k_\beta z^\beta)(\sum_{\gamma\in\Omega_2} \lambda_\gamma z^\gamma) = \sum_{\alpha\in\Omega_1+\Omega_2} \sum_{\beta+\gamma=\alpha} k_\beta\lambda_\gamma z^\alpha$$

cada suma $\sum_{\beta+\gamma=\alpha} k_\beta\lambda_\gamma$ involucra finitos términos.

Esto puede darse, por ejemplo, si los soportes Ω_1, Ω_2 están contenidos en un mismo cono racional poliedral punteado.

Notamos $\mathbb{C}(z) = \mathbb{C}(z_1, \ldots, z_d)$ al cuerpo de cocientes de $\mathbb{C}[z_1, \ldots, z_d]$, siendo sus elementos funciones racionales $\frac{f}{g}$ con $f, g \in \mathbb{C}[z_1, \ldots, z_d]$. Claramente $\mathbb{C}[z^{\pm}] \subseteq \mathbb{C}(z)$.

Dada una función racional $\frac{f}{g}$, hay en general varias formas de verla como serie formal $h = \sum_{\alpha\in\Omega} k_\alpha z^\alpha \in \mathbb{C}[[z^{\pm}]]$, donde entendemos que $\frac{f}{g} = h$ si el producto[1] gh coincide con f.

Por ejemplo, podemos representar a $\frac{1}{1-t} \in \mathbb{C}(t)$ como $\sum_{n\geq 0} t^n$, pero también podemos verlo como $\frac{1}{1-t} = \frac{-1}{t}\frac{1}{(1-\frac{1}{t})} = \sum_{n<0} -t^n$.

Por este motivo es útil considerar el submódulo $\mathcal{Z} = \mathcal{Z}(z_1, \ldots, z_d) \subseteq \mathbb{C}[[z_1^{\pm}, \ldots, z_d^{\pm}]]$ dado por

$$\mathcal{Z} = \{h \in \mathbb{C}[[z^{\pm}]] \,/\, \exists f \in \mathbb{C}[z^{\pm}] \setminus \{0\} : fh = 0\},$$

es decir, la torsión de $\mathbb{C}[[z^{\pm}]]$ visto como $\mathbb{C}[z^{\pm}]-$módulo.

Del ejemplo anterior concluimos que $\sum_{n\in\mathbb{Z}} t^n \in \mathcal{Z}$.

Más generalmente, dado cualquier $\alpha \in \mathbb{Z}^d$, la serie formal multivariada $\sum_{n\in\mathbb{Z}} z^{n\alpha}$ pertenece a $\mathcal{Z}$, pues se anula al multiplicarla por $1 - z^\alpha$.

Veamos cómo asignar alguna serie formal a $\frac{f}{g}$. Dicha asignación no estará bien definida en $\mathbb{C}[[z_1^{\pm}, \ldots, z_d^{\pm}]]$ pero sí sobre el cociente $\mathbb{C}[[z_1^{\pm}, \ldots, z_d^{\pm}]]/\mathcal{Z}$.

Lo haremos para $\frac{1}{g}$ y luego multiplicaremos por f.

Sea $P = \mathcal{P}_{New}(g)$ *el polítopo de Newton de* g (es decir, la envoltura convexa del soporte de g), v uno de sus vértices y $\omega \in \mathbb{Z}^d$ un vector tal que el funcional lineal $\langle x, \omega\rangle$, restringido a P, se minimiza en $x = v$. Notamos con K_v al cono sobre v del polítopo P.

[1] bien definido, pues g es sólo un polinomio

Multiplicando por un escalar no nulo, podemos suponer que $g = z^v - \sum_{\alpha\in\Omega'} k_\alpha z^\alpha$ con $v \notin \Omega'$.

Reescribiendo $g = z^v(1 - \sum_{\alpha\in\Omega'} k_\alpha z^{\alpha-v})$ podemos asignarle el "inverso"

$$\frac{1}{g} = z^{-v} \sum_{n\geq 0} (\sum_{\alpha\in\Omega'} k_\alpha z^{\alpha-v})^n.$$

La serie tiene sentido, dado que en la expansión cada monomio aparece un número finito de veces. Para verlo, basta observar que el funcional $\langle x, \omega\rangle$ evaluado en los exponentes de $(\sum_{\alpha\in\Omega'} k_\alpha z^{\alpha-v})^n$ da entre n y nM donde $M = \text{máx}_{x\in P}\langle x, \omega\rangle$.

Observación 2.0.10 *El soporte de dicha expresión queda contenido en el cono* $-2v + K_v$.

Observación 2.0.11 *El "inverso" así fabricado, depende de la elección de* v.

Ejemplo 2.0.12 $g = 1 + x + y$

Eligiendo $v = (0, 0)$ tendremos

$$\frac{1}{g} = \sum_{a,b\in\mathbb{N}_0} (-1)^{a+b} \binom{a+b}{a} x^a y^b.$$

En cambio, eligiendo $v = (1, 0)$

$$\frac{1}{g} = (1 + x + y)^{-1} = x^{-1}(1 + x^{-1} + x^{-1}y)^{-1} = x^{-1} \sum_{(a,b)\in(-\mathbb{N}_0)\times\mathbb{N}_0} (-1)^a \binom{-a}{b} x^a y^b.$$

En general, el número de posibles desarrollos de Laurent de una función racional $\frac{f}{g}$ está ligado al polítopo de Newton de g. Según vimos, por cada vértice de dicho polítopo tendremos un desarrollo distinto, pero puede haber más. No nos detendremos a estudiar este tema, pero dicha cantidad está acotada por el número de puntos enteros del polítopo (ver [27] y [25]).

2.1. La función generatriz de un cono

Definición 2.1.1 *Dado un subconjunto $S \subseteq \mathbb{R}^d$, la* función generatriz *de S es la serie formal de Laurent dada por*

$$\sigma_S(z) = \sum_{v \in S \cap \mathbb{Z}^d} z^v.$$

Si S es un cono o un polítopo, notamos $\sigma_S^\circ(z) = \sigma_{S^\circ}(z)$.

En esta sección demostraremos que para K un cono racional poliedral, $\sigma_K(z)$ tiene un representante en $\mathbb{C}(z)$. Más adelante veremos cómo escribirlo de manera "corta" siguiendo las ideas de Barvinok [4].

Si el cono K no es punteado (recordar Definición 1.0.7), contiene alguna recta $v + \mathbb{R}w$ con $w \in \mathbb{Z}^d$, de donde $(1 - z^w)\sigma_K = 0$ y σ_K está en la torsión de $\mathbb{C}[[z^{\pm}]]$, o sea que su representante es 0 (para detalles ver [5] pg. 338).

Supongamos de momento que $K = v + \sum_{i=1}^k \mathbb{R}^+ w_i$ con $w_i \in \mathbb{Z}^d$ linealmente independientes (o sea que $k \leq d$). No será necesario en este caso, pero supongamos adicionalmente que también son *primitivos* (es decir, el *mcd* de las coordenadas de cada w_i es 1).

Sea $\Pi = \sum_{i=1}^k [0,1)w_i$ el paralelepípedo fundamental asociado a $\{w_1, \ldots, w_k\}$, y $\sigma_{v+\Pi}(z) = \sum_{p \in (v+\Pi)\cap\mathbb{Z}^d} z^p$ la función generatriz de $v + \Pi$.

Cualquier $p \in K \cap \mathbb{Z}^d$ se escribe de manera única como suma de un vector en $(v+\Pi)\cap\mathbb{Z}^d$ con uno del lattice $\Lambda = \sum_{i=1}^k \mathbb{Z}w_i$ y coordenadas no negativas, es decir $p = q + \sum_{i=1}^k c_i w_i$ con $q \in (v + \Pi) \cap \mathbb{Z}^d$ y los $c_i \geq 0$ enteros.

Tenemos entonces que:

$$\begin{aligned}
\sigma_K(z) &= \sum_{p \in K\cap\mathbb{Z}^d} z^p = \sum_{q \in (v+\Pi)\cap\mathbb{Z}^d} \sum_{c \in {\mathbb{Z}_{\geq 0}}^k} z^{q+\sum_{i=1}^k c_i w_i} = \\
&= \sigma_{v+\Pi}(z) \sum_{c \in {\mathbb{Z}_{\geq 0}}^k} z^{\sum_{i=1}^k c_i w_i} = \\
&= \sigma_{v+\Pi}(z) \prod_{i=1}^k \sum_{c_i=0}^{\infty} (z^{w_i})^{c_i} = \frac{\sigma_{v+\Pi}(z)}{\prod_{i=1}^k (1 - z^{w_i})}. \qquad (2.1)
\end{aligned}$$

Similarmente, para hallar $\sigma_{K^\circ}(z)$ consideramos $\Pi' = \sum_{i=1}^k (0,1]w_i$ en lugar de Π y llegamos a

$$\begin{aligned}\sigma_{K^\circ}(z) &= \sum_{q\in(v+\Pi')\cap\mathbb{Z}^d}\ \sum_{c\in\mathbb{Z}_{\geq 0}{}^k} z^{q+\sum_{i=1}^k c_i w_i} = \\ &= \frac{\sigma_{v+\Pi'}(z)}{\prod_{i=1}^k (1-z^{w_i})}.\end{aligned}$$

Como

$$\Pi' = \sum_{i=1}^k (0,1]w_i = \sum_{i=1}^k (1-[0,1))w_i = \sum_{i=1}^k w_i - \sum_{i=1}^k [0,1)w_i = \sum_{i=1}^k w_i - \Pi,$$

tenemos que $\sigma_{v+\Pi'}(z) = z^w \sigma_{-v+\Pi}(\frac{1}{z})$ con $w = \sum_{i=1}^k w_i$.

Tenemos entonces la identidad:

$$\sigma_{K^\circ}(z) = \frac{\sigma_{v+\Pi'}(z)}{\prod_{i=1}^k (1-z^{w_i})} = \frac{z^w \sigma_{-v+\Pi}(z^{-1})}{\prod_{i=1}^k (1-z^{w_i})} = \frac{\sigma_{-v+\Pi}(z^{-1})}{\prod_{i=1}^k (z^{-w_i}-1)} = (-1)^k \sigma_{-2v+K}(z^{-1}),$$

o, de manera más simétrica, si tomamos $K = \sum_{i=1}^k \mathbb{R}^+ w_i$ resulta:

$$\sigma_{v+K^\circ}(z) = (-1)^k \sigma_{-v+K}(z^{-1}).$$

Si $K = \sum_{i=1}^m \mathbb{R}^+ w_i$ es un cono racional poliedral con vértice en cero, no necesariamente simplicial, de dimensión k, podemos triangularlo, es decir, escribirlo como unión disjunta de conos simpliciales K_j° relativamente abiertos de dimensiones a lo sumo k, sin usar nuevos generadores. Por lo que $\sigma_K(z) = \sum_j \sigma_{K_j^\circ}(z)$ tiene un representante en $\mathbb{C}(z)$ con denominador $\prod_{i=1}^m (1-z^{w_i})$ y numerador en $\mathbb{C}[z^\pm]$.

De $\sigma_{v+K^\circ}(z) = (-1)^d \sigma_{-v+K}(z^{-1})$ sale que $\sigma_{v+K}(z^{-1}) = (-1)^d \sigma_{-v+K}(z)$ si v se elige de manera tal que $v + \partial K \cap \mathbb{Z}^d = \emptyset$. Salvo un conjunto de medida nula, cualquier v genérico funciona.

Éste es uno de los llamados *métodos irracionales* en donde una perturbación genérica v (posiblemente pequeña en algunos casos) se suma a los conos o símplices involucrados para evitar problemas con los puntos del borde (ver [12]).

Dado un cono racional poliedral K con vértice en el origen, de dimensión d, podemos triangularlo y elegir ahora un $v \in K^\circ$ suficientemente pequeño y genérico, tal que al perturbar

a todos los conos de la triangulación no haya puntos enteros en las caras de los conos de dimensión d, y que $(v+K)\cap\mathbb{Z}^d = K^\circ\cap\mathbb{Z}^d$ y $(-v+K)\cap\mathbb{Z}^d = K\cap\mathbb{Z}^d$.

Entonces

$$\sigma_K^\circ(z^{-1}) = \sigma_{v+K}(z^{-1}) = (-1)^d\sigma_{-v+K}(z) = (-1)^d\sigma_K(z) \tag{2.2}$$

pues la identidad del medio se deduce del caso simplicial sumando las funciones generatrices de los conos de la división de K.

2.2. Serie de Ehrhart

Dado un polítopo racional $P\subseteq\mathbb{R}^d$ se define $C(P)\subseteq\mathbb{R}^{d+1}$ el *cono sobre* P como el generado por $P\times\{1\}$ con vértice en el 0 (ver fig. 2.1).

Para $t\in\mathbb{N}$, tendremos en altura t que $tP\times\{t\} = C(P)\cap(\mathbb{R}^d\times\{t\})$.

El cono $C(P)$ será racional poliedral, y si P es entero, su función generatriz $\sigma_{C(P)}(z,x) = \sum_{t\geq 0}\sigma_{tP}(z)x^t$ tiene como denominador al producto $\prod_{v\in Vert(P)}(1-xz^v)$.

Evaluando en $z=\mathbf{1}$ nos queda la serie:

$$\sigma_{C(P)}(z,x)|_{z=\mathbf{1}} = \sum_{t\geq 0}\sigma_{tP}(z)|_{z=\mathbf{1}}x^t = \sum_{t\geq 0}L_P(t)x^t = \frac{f(x)}{(1-x)^V}$$

para cierto polinomio $f\in\mathbb{C}[x]$ y $V = \sharp(Vert(P))$. Definimos así la *serie de Ehrhart* de P como $Ehr_P(x) = \sum_{t\geq 0}L_P(t)x^t$, donde $L_P(0)=1$ por convención.

Si P no es entero, repitiendo el razonamiento se llega a que $Ehr_P(x)$ es una función racional en la que puede tomarse como denominador a $(1-x^n)^V$ donde n es algún denominador de P.

Cuando P es un $d-$simplex entero, tiene $d+1$ vértices y su serie de Ehrhart puede tomarse con denominador $(1-x)^{d+1}$.

En el caso de P entero, como podemos subdividirlo en simplices de dimensión a lo sumo d, su serie de Ehrhart se escribe como suma y resta de series de Ehrhart de simplices, por lo que es una suma de funciones racionales cuyos denominadores dividen a $(1-x)^{d+1}$, lo que implica que podemos tomar $Ehr_P(x)$ de la forma $\frac{f(x)}{(1-x)^{d+1}}$.

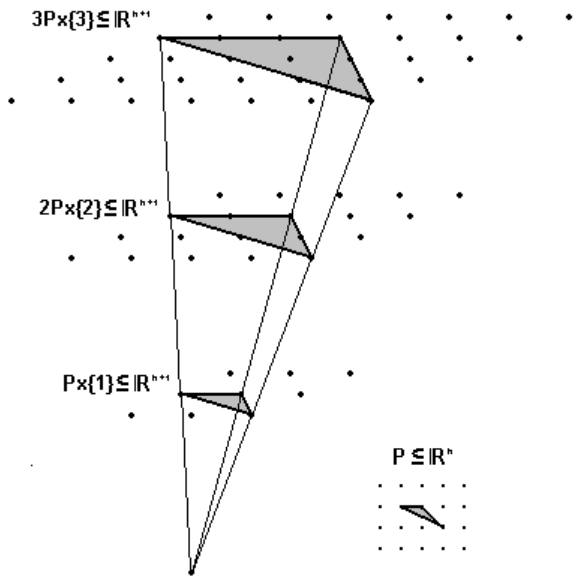

Figura 2.1: Ejemplo de C(P)

Teorema 2.2.1 *(de Positividad , Stanley [11]) Sea P un polítopo entero de dimensión d, entonces $Ehr_P(x) = \frac{f(x)}{(1-x)^{d+1}}$ donde los coeficientes de f son enteros no negativos, y f tiene grado $\leq d$.*

Demostración. Cuando P es un simplex, el cono $C(P)$ es simplicial y su función generatriz tiene la forma : $\frac{\sigma_\Pi(z,x)}{\prod(1-xz^v)}$ y al evaluar $z = \mathbf{1}$ en el numerador nos queda una suma de varios monomios x^t con $t < d+1$ (pues el paralelepípedo Π es el generado por los $d+1$ vectores $(v,1)$ con $v \in Vert(P)$). Tenemos entonces que $f(x) = \sigma_\Pi(\mathbf{1}, x)$ tiene grado a lo sumo d y su coeficiente de grado t es la cantidad de puntos enteros de Π con última coordenada t, que es un entero no negativo.

El caso general se obtiene de éste, triangulando $C(P)$ en conos simpliciales $K_1, \ldots, K_l$ y tomando una pequeña perturbación $v \in \mathbb{R}^{d+1}$ que garantice $C(P) \cap \mathbb{Z}^{d+1} = (v + C(P)) \cap \mathbb{Z}^{d+1}$ y que ninguna cara de la triangulación contenga puntos enteros.

La idea de correr al cono $C(P)$ sumando un v, es evitar la superposición de puntos enteros en las caras de la triangulación, pudiendo sumar las funciones generatrices sin necesidad de

llevar la cuenta de las caras de menor dimensión y aplicar el principio de inclusión-exclusión. Éste es otro ejemplo de los métodos irracionales de [12].

Podemos escribir a la función generatriz de $C(P)$ como la suma de las funciones generatrices de los conos simpliciales $v + K_i$, luego evaluar en $z = \mathbf{1}$ y llegar a que la serie de Ehrhart de P es suma de funciones racionales de la forma $\frac{f_i(x)}{(1-x)^{d+1}}$ con f_i de grado $\leq d$ y coeficientes no negativos, lo que implica el resultado buscado. Q.E.D.

Observación 2.2.2 *Como el desarrollo de Taylor de* $\frac{x^j}{(1-x)^{d+1}}$ *es*

$$\sum_{t\geq 0} \binom{t+d-j}{d} x^t,$$

si escribimos a $f(x)$ *como* $\sum_{j=0}^{d} c_j x^j$ *llegamos a que*

$$L_P(t) = \sum_{j=0}^{d} c_j \binom{t+d-j}{d},$$

con los c_k *enteros no negativos.*

Observación 2.2.3 *Si* P *es racional con denominador* n*, imitando el razonamineto de esta sección llegamos a que*

$$Ehr_P(x) = \frac{f(x)}{(1-x^n)^{d+1}},$$

con $f(x)$ *de grado menor que* $n(d+1)$ *y coeficientes no negativos. Por los resultados del Apéndice A, tendremos que* $L_P(t)$ *satisface una recursión lineal cuyo polinomio característico es* $Char(T) = (T^n - 1)^{d+1}$*. Como sus raíces están en* $\mathbb{G}_n$*, resulta que* $L_P(t)$ *es un cuasi-polinomio de período* n *y grado* $\leq d$ *(recordar Definición 0.0.1).*

En particular, tenemos el

Teorema 2.2.4 *(Ehrhart [23]) Sea* P *un polítopo racional de dimensión* d*, entones* $L_P(t)$ *es un cuasi-polinomio en* t *de grado* d*, y su período divide al denominador de* P*.*

Como consecuencia de este Teorema y la idetidad (2.2), tenemos el siguiente:

Teorema 2.2.5 *(Reciprocidad de Ehrhart-MacDonald) Sea $P \subseteq \mathbb{R}^d$ un polítopo racional de dimensión d, entonces:*

$$L_P(-t) = (-1)^d L_{P^\circ}(t).$$

Demostración. Sólo hay que observar que

$$\begin{aligned}\sum_{t\geq 1} L_{P^\circ}(t)x^t &= \sigma^\circ_{C(P)}(z,x)|_{z=\mathbf{1}} = \\ &= (-1)^{d+1}\sigma_{C(P)}(\frac{1}{z},\frac{1}{x})|_{z=\mathbf{1}} = \\ &= (-1)^{d+1}Ehr_P(\frac{1}{x}) = (-1)^d \sum_{t\geq 1} L_P(-t)x^t,\end{aligned}$$

usando en la última igualdad que $\sum_{t\leq 0} L_P(-t)x^t = -\sum_{t\geq 1} L_P(-t)x^t$, lo que equivale a decir que $F(x) = \sum_{t\in\mathbb{Z}} L_P(-t)x^t$ está en la torsión de $\mathbb{C}[[x^{\pm}]]$. Veamos que así es. Como L_P es un cuasipolinomio, $\{L_P(t)\}_{t\in\mathbb{Z}}$ satisface una recursividad lineal de polinomio característico $Char(T) = (T^n - 1)^{d+1}$, por lo que $(x^n - 1)^{d+1}F(x) = 0$. Q.E.D.

2.3. Cotas para las raíces de L_P

Antes de querer calcular el polinomio de Ehrhart de un polítopo, es bueno saber en qué formato es razonable escribirlo (éste es el problema de querer escribir la función generatriz de un polítopo de manera densa). Listar sus coeficientes es viable siempre y cuando se tenga alguna cota "buena" para el tamaño de los mismos.

Dado que éstos se calculan a partir de las raíces, nos interesaría acotarlas.

En [10] se exhiben cotas superiores e inferiores para la raíz de mayor valor absoluto, la mayor y la menor de las raíces reales, y algunas ideas de cómo acotar la parte real de las raíces complejas. En el reciente paper [13], se presenta una demostración elemental de una cota de orden cuadrático en la dimensión, mejorando las cotas anteriores.

Proposición 2.3.1 *Sean $c_k \geq 0$, con $0 \leq k \leq d$ no todos nulos. Las raíces de $f(t) = \sum_{k=0}^{d} c_k \binom{t+d-k}{d} \in \mathbb{R}[t]$ caen dentro de la bola $B(-1/2, d(d-\frac{1}{2})) \subseteq \mathbb{C}$.*

Demostración. La idea es bastante geométrica. Veamos que para $z \in \mathbb{C}$ fuera de la bola, todos los valores $\binom{z+d-k}{d}$ se encuentran en un mismo cono punteado.

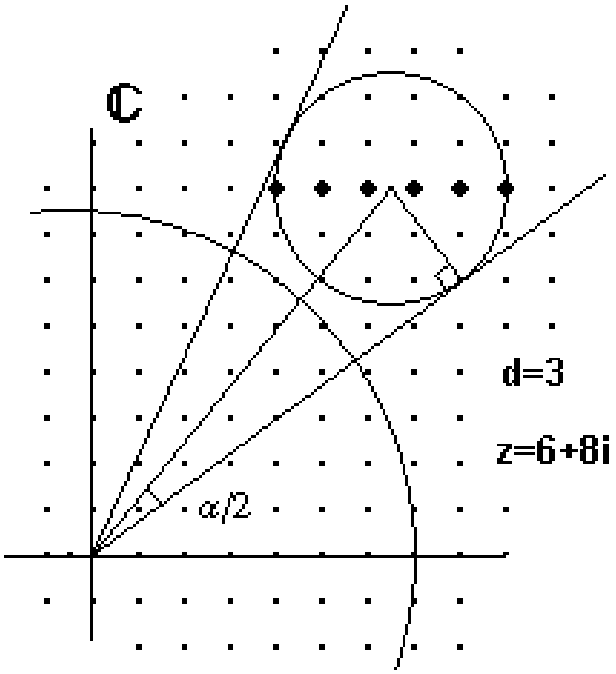

Figura 2.2: El cono de ángulo $\alpha < \frac{\pi}{d}$, en un ejemplo concreto.

Los números $\{z-d+1, z-d+2, \ldots, z+d\}$ se encuentran en la bola de centro $z+\frac{1}{2}$ y radio $d-\frac{1}{2}$. Las tangentes a dicha bola desde el origen forman un ángulo α que verifica:

$$\sin(\frac{\alpha}{2}) = \frac{d-\frac{1}{2}}{|z+\frac{1}{2}|} < \frac{d-\frac{1}{2}}{d(d-\frac{1}{2})} = \frac{1}{d}.$$

Como $\frac{2x}{\pi} \leq \sin(x)$ para x en $[0, \frac{\pi}{2}]$ tenemos $\frac{\alpha}{\pi} < \frac{1}{d}$, luego $\alpha < \frac{\pi}{d}$. O sea que los complejos $\{z-d+1, z-d+2, \ldots, z+d\}$ caen dentro de un cono centrado en el origen cuyo ángulo es menor a $\frac{\pi}{d}$ (ver fig. 2.2), por lo que los puntos $\{\binom{z+d-k}{d}\}_{0\leq k\leq d}$ se encuentran en un cono de ángulo estrictamente menor a π. Q.E.D.

Capítulo 3

Teorema de Brion

A continuación hablaremos de cómo codificar el conjunto de puntos enteros de un polítopo P, en lugar de preocuparnos simplemente por la cantidad. La idea es escribir la función generatriz de P de alguna manera "corta". Si lo hiciésemos listando el conjunto de monomios, ésto podría ocupar mucho lugar y llevarnos mucho tiempo. El Teorema de Brion [14] nos permite escribir a σ_P como suma de funciones racionales (una por cada vértice de P). Comenzaremos viendo algunos corolarios del Teorema y luego presentamos una demostración elemental del mismo. En el capítulo siguiente veremos cómo calcular dichas funciones racionales de manera eficiente.

Dado un polítopo $P \subseteq \mathbb{R}^d$, consideramos para cada vértice $v \in Vert(P)$ su cono $K_v = v + \mathbb{R}^+(P - v)$, y llamando $\sigma_P, \sigma_v \in \mathbb{C}(z_1, \ldots, z_d)$ a las funciones generatrices de P y los conos K_v (resp.) se tiene:

Teorema 3.0.2 *(Brion, 1988 [14])*

$$\sigma_P = \sum_{v \in Vert(P)} \sigma_v. \tag{3.1}$$

Antes de su demostración, veremos primero algunas aplicaciones.

3.1. Consecuencias

Como primer Corolario, podemos demostrar el Teorema de Ehrhart 2.2.4, usando algunas herramientas del Apéndice A.

Corolario 3.1.1 *(Ehrhart) Sea $P \subseteq \mathbb{R}^d$ un polítopo racional, entonces $L_P(t) = \sharp(tP \cap \mathbb{Z}^d)$ es un cuasi-polinomio para los valores de $t \in \mathbb{N}$. Su período divide al mínimo común múltiplo de los denominadores de las coordenadas de los vértices de P, en particular si P es entero, L_P es un polinomio.*

Demostración. Lo haremos primero para P entero y después deduciremos el caso general.

Si $v \in Vert(P)$, resulta que $tv \in Vert(tP)$ $(t \in \mathbb{N})$ y $K_{tv} = tK_v = (t-1)v + K_v$, por lo que $\sigma_{tP} = \sum_{v \in Vert(P)} z^{(t-1)v}\sigma_v = \sum_{v \in Vert(P)} z^{tv}\sigma_{-v+K_v}$.

Tenemos que la sucesión $\{\sigma_{tP}\}_{t\in\mathbb{N}} \subseteq \mathbb{C}(z_1, \ldots, z_d)$ es una suma de exponenciales de base z^v. Entonces satisface cierta recursividad lineal cuyo polinomio característico viene dado por $Char(T) = \prod_{v \in Vert(P)}(T - z^v)$, en particular, verifica cierto vector, cuyas coordenadas son polinomios de Laurent.

Como $L_P(t) = \sigma_{tP}(\mathbf{1})$ (evaluar en $z_i = 1$), la sucesión $\{L_P(t)\}_{t\in\mathbb{N}}$ satisface una recursividad lineal que se obtiene de la anterior, evaluando los z_i en 1 (podemos hacer esto pues el vector que verifica $\{\sigma_{tP}\}_{t\in\mathbb{N}}$ está en $\mathbb{C}[z_1^{\pm}, \ldots, z_d^{\pm}]$). Entonces, como su polinomio característico se obtiene del anterior especializando z en $\mathbf{1}$, deberá ser

$$Char(T)(\mathbf{1}) = \prod_{v \in Vert(P)} (T-1) = (T-1)^{\sharp Vert(P)},$$

de donde $\{L_P(t)\}_{t\in\mathbb{N}}$ tiene que ser un polinomio de grado menor que $\sharp Vert(P)$ [1].

Para el caso más general, sea n el menor denominador de P. Alcanzará con probar que $\{L_P(t)\}_{t\in\mathbb{N}}$ es una suma de sucesiones polinomiales multiplicadas por exponenciales cuyas bases son raíces $n-$ésimas de la unidad (esto hace que $\{L_P(t)\}_{t\in\mathbb{N}}$ sea un cuasi-polinomio de período n, aunque también podría tener períodos menores, cfr. Prop. A.0.34).

[1] ver Apéndice A

Observando que $\sharp(tP \cap \mathbb{Z}^d) = \sharp(tnP \cap n\mathbb{Z}^d)$, nos concentraremos en hallar

$$\widetilde{\sigma}_{tP} = \sum_{p \in tnP \cap n\mathbb{Z}^d} z^p = \sigma_{tp}(z_1^n, \ldots, z_d^n)$$

a partir de la función generatriz de tnP.

En general, si $f(x) = \sum_{k=-N}^{N} c_k x^k \in \mathbb{K}[x^{\pm}]$ es un polinomio de Laurent en una sola variable con $\mathbb{C} \subseteq \mathbb{K}$, y queremos quedarnos sólo con los términos de subíndice múltiplo de n, calculamos el promedio:

$$\frac{1}{n} \sum_{\xi \in \mathbb{G}_n} f(\xi x) = \sum_{k=-N, n|k}^{N} c_k x^k.$$

En el caso multivariado, deberíamos aplicar este promedio para cada variable, y obtener:

$$\widetilde{\sigma}_{tP}(z_1, \ldots, z_d) = \sum_{p \in tnP \cap n\mathbb{Z}^d} z^p = \frac{1}{n^d} \sum_{\xi \in \mathbb{G}_n^d} \sigma_{tnP}(\xi_1 z_1, \ldots, \xi_d z_d).$$

Siguiendo el razonamiento anterior, ahora tenemos que $\{\sigma_{tP}\}_{t \in \mathbb{N}}$ es una combinación lineal de sucesiones exponenciales de bases $\xi^v z^v$ con $v \in Vert(P)$ y $\xi \in \mathbb{G}_n$. El polinomio característico de la recursión tendrá como raíces a dichos $\xi^v z^v$, y el polinomio característico de la recursividad de $\{L_P(t)\}_{t \in \mathbb{N}}$ tendrá como raíces a los números $(\xi^v z^v)(\mathbf{1}) = \xi^v = \prod_{i=1}^{d} \xi_i^{v_i} \in \mathbb{G}_n$, es decir, raíces $n-$ésimas de la unidad, de donde $\{L_P(t)\}_{t \in \mathbb{N}}$ es una combinación de polinomios multiplicados por exponenciales de bases ξ. Q.E.D.

Considerando multisucesiones recursivas en lugar de simples sucesiones, podemos generalizar este resultado a sumas de Minkowski de varios polítopos:

Corolario 3.1.2 *Sean $P_1, \ldots, P_m \subseteq \mathbb{R}^d$ polítopos enteros, entonces la función*

$$L_{P_1,\ldots,P_m}(t_1, \ldots, t_m) = \sharp(t_1 P_1 + \ldots + t_m P_m \cap \mathbb{Z}^d)$$

es un polinomio en los $t_1, \ldots, t_m$ naturales.

Demostración. Basta observar que para cada $v \in Vert(t_1 P_1 + \ldots + t_m P_m)$ existen vértices $v_i \in Vert(P_i)$ tales que $v = t_1 v_1 + \ldots + t_m v_m$ y que $-v + K_v = \sum_{i=1}^{m} -v_i + K_{v_i}$, y que

esto implica que $\sigma_{t_1P_1+\ldots+t_mP_m}$ es una suma de multisucesiones de la forma $z^{t_1v_1+\ldots+t_mv_m} = \prod_{i=1}^{m} z^{t_iv_i}$ multiplicadas por funciones racionales fijas, por lo que satisface en cada variable t_i una recursión lineal de raíces z_i^v, que al evaluar $z = \mathbf{1}$ pasan a ser recursiones de raíz 1 con multiplicidad, lo que da como resultado un polinomio en varias variables. Q.E.D.

Con la misma línea de razonamiento también se tiene el siguiente resultado:

Corolario 3.1.3 *Si $P_1, \ldots, P_m \subseteq \mathbb{R}^d$ son polítopos racionales, $L_{P_1,\ldots,P_m}(t_1, \ldots, t_m)$ es un cuasi-polinomio multivariado, es decir, una suma de polinomios multiplicados por exponenciales $\xi_1^{t_1}\xi_2^{t_2}\ldots\xi_m^{t_m}$ con $\xi_i^n = 1$, con n denominador común a los P_i.*

Observación 3.1.4 *Supongamos $P \subseteq \mathbb{R}^d$ de dimensión d. Recordemos que el coeficiente principal de L_P es el volumen, y que dicho coeficiente puede calcularse como la derivada discreta $d-$ésima de L_P dividido $d!$ (ver Apéndice A y (1.1)). Más aún, no es necesario decir en dónde se evalua, pues dicha derivada discreta da un polinomio de grado cero. Por lo tanto, como $L_P(t) = \sigma_{tP}(\mathbf{1}) = (\sum_{v\in Vert(P)} z^{tv}\sigma_{-v+K_v})(\mathbf{1})$ se tiene que:*

$$\begin{aligned} d!Vol(P) &= (\Delta^d\sigma_{tP})(\mathbf{1}) = \left(\sum_{i=0}^{d}(-1)^i\binom{d}{i}\sigma_{(t+i)P}\right)(\mathbf{1}) \qquad (3.2)\\ &= \left(\sum_{i=0}^{d}(-1)^i\binom{d}{i}\sum_{v\in Vert(P)} z^{(t+i)v}\sigma_{-v+K_v}\right)(\mathbf{1})\\ &= \left(\sum_{v\in Vert(P)}\sum_{i=0}^{d}(-1)^i\binom{d}{i}z^{(t+i)v}\sigma_{-v+K_v}\right)(\mathbf{1})\\ &= \left(\sum_{v\in Vert(P)}(z^v-1)^d z^{tv}\sigma_{-v+K_v}\right)(\mathbf{1}), \end{aligned}$$

donde t es cualquier entero.

Supongamos ahora que P es simple, y para cada $v \in Vert(P)$ sean $\{w_{v1}, \ldots, w_{vd}\}$ los vectores primitivos de los rayos de $K_v - v$. Entonces

$$\sigma_{-v+K_v}(z) = \frac{\sigma_{\Pi_v}(z)}{\prod_{i=1}^{d}(1-z^{w_{vi}})}$$

donde Π_v es el paralelepípedo fundamental de la base $\{w_{v1}, \ldots, w_{vd}\}$.

En este caso nos queda:

$$d!Vol(P) = \left(\sum_{v \in Vert(P)} \frac{(z^v - 1)^d z^{tv} \sigma_{\Pi_v}(z)}{\prod_{i=1}^{d}(1 - z^{w_{vi}})} \right) (\mathbf{1}).$$

Observemos que la evaluación $z = \mathbf{1}$ que anula d factores del denominador, también anula d factores del numerador. Veamos que es posible salvar la indeterminación, pudiendo hacer la evaluación en cada término.

Para ello elegimos un vector $x \in \mathbb{R}^d$ que no sea ortogonal a ninguno de los w_{vi}, evaluamos en $z = \exp(\epsilon x)$ (es decir, $z_i = \exp(\epsilon x_i)$) y luego hacemos tender ϵ a cero:

$$\begin{aligned}
\lim_{\epsilon \longrightarrow 0} \frac{(\exp(\epsilon x)^v - 1)^d \exp(\epsilon x)^{tv} \sigma_{\Pi_v}(\exp(\epsilon x))}{\prod_{i=1}^{d}(1 - \exp(\epsilon x)^{w_{vi}})} &= \\
\lim_{\epsilon \longrightarrow 0} \frac{(\exp(\epsilon < x, v >) - 1)^d \exp(\epsilon t < x, v >) \sigma_{\Pi_v}(\exp(\epsilon x))}{\prod_{i=1}^{d}(1 - \exp(\epsilon < x, w_{vi} >))} &= \\
\lim_{\epsilon \longrightarrow 0} \sigma_{\Pi_v}(\mathbf{1}) \prod_{i=1}^{d} \frac{\exp(\epsilon < x, v >) - 1}{1 - \exp(\epsilon < x, w_{vi} >)} &= \frac{\sigma_{\Pi_v}(\mathbf{1}) < x, -v >^d}{\prod_{i=1}^{d} < x, w_{vi} >}.
\end{aligned}$$

Llamando W al sublattice de $\mathbb{Z}^d$ generado por los $\{w_{vi}\}_{i=1}^{d}$ tenemos que

$$\sigma_{\Pi_v}(e) = \sharp(\Pi_v \cap \mathbb{Z}^d) = \sharp(\mathbb{Z}^d / W) = |det(w_{v1}, \ldots, w_{vd})|.$$

Y así hemos probamos la siguiente:

Proposición 3.1.5 *Sea $P \subseteq \mathbb{R}^d$ simple de dimensión n, y sean $\{w_{vi}\}$ los vectores primitivos de los rayos de $-v + K_v$ para cada $v \in Vert(P)$. Entonces:*

$$Vol(P) = \frac{1}{d!} \sum_{v \in Vert(P)} \frac{|det(w_{v1}, \ldots, w_{vd})| < x, -v >^d}{\prod_{i=1}^{d} < x, w_{vi} >} \tag{3.3}$$

para culaquier $x \in \mathbb{R}^d$ que no sea ortogonal a ninguna de las aristas de P.

Observación 3.1.6 *Como la fórmula (3.3) siguie valiendo si multiplicamos a los w_{vi} por cualquier escalar positivo, podemos obviar la hipótesis de "primitivos" y considerar simplemente los w_{vi} en las direcciones de las aristas de v.*

Observación 3.1.7 *Si P es un polítopo racional de denominador n, nP es entero y sus vértices son $\{nv\}_{v\in Vert(P)}$. Aplicando la fórmula (3.3) a nP y dividiendo ambos lados por n^d, obtendremos la misma fórmula para P, relajando así de la condición de "entero" por la de "racional".*

Observación 3.1.8 *Es posible extender dicha fórmula aún para los P no racionales, mediante un argumento de aproximación.*

A continuación veremos otra forma de llegar a esta fórmula.

En [6], A. Barvinok presentó algoritmos polinomiales para estimar el volumen de un polítopo P con un error menor a un $\epsilon > 0$ dado, basándose en la fórmula:

$$\int_P \exp(< z, x >)dz = (-1)^d \sum_{v\in Vert(P)} \frac{|det(w_{v1}, \ldots, w_{vd})| \exp(< x, v >)}{\prod_{i=1}^d < x, w_{vi} >},$$

tomando un vector $x \in \mathbb{R}^d$ suficientemente pequeño.

Existen varias maneras de llegar a esta fórmula. Barvinok presentó una inductiva, usando el Teorema de Stokes para reducir la integral sobre P a una integral sobre sus facetas, y luego éstas a integrales sobre las caras de codimensión 2, etc., hasta llegar a la suma sobre los vértices.

En [11] la demuestran a partir del Teorema de Brion.

Veamos cómo deducir (3.3) a partir de esta otra fórmula, dando lugar así a algoritmos exactos para el cálculo de $vol(P)$.

Desarrollando las series de Taylor de las funciones exponenciales en dicha fórmula obtenemos:

$$\sum_{k\geq 0} \int_P \frac{< z, x >^k}{k!} dz = \sum_{k\geq 0} (-1)^d \sum_{v\in Vert(P)} \frac{|det(w_{v1}, \ldots, w_{vd})| < x, v >^k}{k! \prod_{i=1}^d < x, w_{vi} >}.$$

Igualando los términos homogéneos en x de grado k de ambos lados llegamos a que, para $k < d$:

$$(-1)^d \sum_{v\in Vert(P)} \frac{|det(w_{v1}, \ldots, w_{vd})| < x, v >^k}{\prod_{i=1}^d < x, w_{vi} >} = 0$$

y si $k \geq 0$

$$\int_P \frac{< z, x >^k}{k!} dz = \frac{(-1)^d}{(k+d)!} \sum_{v \in Vert(P)} \frac{|det(w_{v1}, \ldots, w_{vd})| < x, v >^{k+d}}{\prod_{i=1}^d < x, w_{vi} >}.$$

Notemos que para $k = 0$ recuperamos la fórmula (3.3).

Observación 3.1.9 *La fórmula (3.3) se obtuvo a partir del Teorema 3.0.2, la identidad (3.2), componiendo las funciones generatrices con la exponencial* $\exp(\epsilon x)$ *para cierto* $x \in \mathbb{R}^d$ *genérico, y tomando límite cuando* ϵ *tiende a* 0*.*

Si P *no fuese simple, podríamos escribir las* σ_v *como combinación lineal de funciones generatrices de conos simpliciales (por ejemplo, triangulando a* P*), y proceder de la misma manera.*

Si bien no llegaremos a una fórmula explícita, en cada vértice v *nos quedará una función racional en* x*, cuya suma da idénticamente* $vol(P)$*, y cada una de ellas se escribe como combinación lineal de funciones de la forma*

$$\frac{|det(w_{v1}, \ldots, w_{vd})| < x, -v >^d}{\prod_{i=1}^d < x, w_{vi} >},$$

fabricadas a partir de v *y alguna triangulación fija de* $-v + K_v$*. Suponiendo* $-v + K_v$ *fijo, dichas funciones racionales varían polinomialmente en* v*.*

Concluimos así la versión continua del Corolario 3.1.2:

Corolario 3.1.10 *Dados los polítopos* $P_1, \ldots, P_m \subseteq \mathbb{R}^d$*, entonces la función*

$$V_{P_1,\ldots,P_m}(t_1, \ldots, t_m) = vol(t_1 P_1 + \ldots + t_m P_m)$$

es un polinomio en los valores positivos de $t_1, \ldots, t_m$*.*

Demostración. Como en el Corolario 3.1.2, los vértices de las sumas de Minkowski $t_1 P_1 + \ldots + t_m P_m$ dependen linealmente de los los $t_1, \ldots, t_m$ y los respectivos conos $-v + K_v$ (centrados en el origen) sólo dependen de los conos de ciertos vértices fijos $v_i \in P_i$. Concluímos la demostración escribiendo al volumen $vol(t_1 P_1 + \ldots + t_m P_m)$ como suma de funciones racionales definidas por sus vértices (como en la Observación 3.1.9) y observando que dichas funciones dependen polinomialmente de los t_i. Q.E.D.

3.2. Demostración del Teorema de Brion

Lo demostraremos primero para el caso de $P^\circ = relint(P)$ un simplex relativamente abierto, es decir P es la cápsula convexa de $n+1$ puntos $\{u_0, \ldots, u_n\}$ tales que los vectores $\{u_1 - u_0, \ldots, u_n - u_0\}$ son linealmente independientes (entonces $n \leq d$), y queremos ver que $\sigma_P^\circ = \sum_{i=0}^n \sigma_{K_i}^\circ$, donde los K_i son los conos de P sobre sus vértices.

Restringiéndonos de ser necesario al espacio afín generado por P, podemos suponer $n = dim(P) = d$.

Las caras $\{F\}$ de P serán también símplices, y están determinados por todos los subconjuntos no vacíos de $\{u_0, \ldots, u_d\}$. Denotemos por $\{F_0, \ldots, F_d\}$ a las facetas de P.

Está claro que P° es la intersección de todos los conos abiertos $K_{F_i}^\circ$ (que son semiespacios). Más generalmente, el cono abierto K_F° sobre cualquier cara F de S es la intersección de los conos $K_{F_i}^\circ$ correspondientes a las facetas F_i que contienen a F.

Llamando $[K]$ a la función característica de un cono K, tenemos que $1-[K]$ es la función característica del complemento de K, y como el producto de funciones características da la función característica de la intersección, tenemos:

$$\prod_{i=0}^{d}(1 - [K_{F_i}^\circ]) = [\bigcap_{i=0}^{d}(K_{F_i}^\circ)^c] = 1 - [(\bigcup_{i=0}^{d} K_{F_i}^\circ)] = 0,$$

pues $\bigcup_{i=0}^d K_{F_i}^\circ = \mathbb{R}^d$ como puede verse fácilmente en el caso de $P = \{x \in \mathbb{R}^d / x_i \geq 0, \sum_{i=0}^d x_i \leq 1\}$ y demostrando el caso general aplicando una tranformación afín.

Distribuyendo el producto y pasando de lado el término $\prod_{i=0}^d(-[K_{F_i}^\circ])$ tenemos:

$$1 + \sum_{0 \leq j_1 < \ldots < j_k \leq d,\ k \leq d+1} (-1)^k [\bigcap_{l=1}^{k} K_{F_{j_l}}^\circ] = (-1)^d \prod_{i=0}^{d} [K_{F_i}^\circ] = (-1)^d [\bigcap_{i=0}^{d} K_{F_i}^\circ],$$

o sea

$$[P^\circ] = [\bigcap_{i=0}^{d} K_{F_i}^\circ] = (-1)^d + \sum_{0 \leq j_1 < \ldots < j_k \leq d,\ k \leq d+1} (-1)^{d-k} [\bigcap_{l=1}^{k} K_{F_{j_l}}^\circ] = \sum_{F \subsetneq S} (-1)^{dim(F)} [K_F^\circ],$$

donde F recorre las caras de P, incluyendo al propio P (y observando que $[K_P^\circ] = 1$), que no es más que una suerte de fórmula de *inclusión-exclusión*.

Como esta fórmula no involucra tomar complementos, sigue valiendo en el caso $d \neq n$. De aquí que

$$\sigma_P^\circ = \sum_{F \subsetneq P} (-1)^{dim(F)} \sigma_{K_F}^\circ,$$

y podemos eliminar las funciones generatrices correspondientes a conos no punteados (por estar en la torsión) llegando a

$$\sigma_P^\circ = \sum_{v \in Vert(P)} \sigma_{K_v}^\circ.$$

El caso general, cuando P no es necesariamente un simplex abierto, se deduce de éste triangulando a P, es decir, descomponiéndolo como unión disjunta de simplices relativamente abiertos, sin involucrar vértices nuevos. Los conos en los vértices se escribirán como unión de los conos abiertos correspondientes a los simplices de la triangulación y reagrupando los términos llegamos a

$$\sigma_P = \sum_{v \in Vert(P)} \sigma_{K_v},$$

para cualquier polítopo P cerrado.

Observación 3.2.1 *Otra demostración posible consiste en probarlo primero para símplices no abiertos y generalizarlo con el truco de los métodos irracionales. Sumando pequeños vectores a los hiperplanos que aparecen en una triangulación de P, podemos llegar del caso general a uno perturbado donde las caras que aparecen como intersecciones en la triangulación no contengan puntos enteros (ver [11]).*

Capítulo 4

Algoritmo de Barvinok

En [4] A. Barvinok presentó un algoritmo para escribir la función generatriz de un polítopo P como suma de funciones racionales, que corre en un tiempo polinomial en el tamaño de la entrada (suponiendo la dimensión d fija), resolviendo de esta manera varios problemas de Programación Lineal Entera [7]. Veremos cómo los autores de [20] implementaron el Algoritmo de Barvinok en el sistema LattE [19], siguiendo los métodos porpuestos en [22]. Comenzaremos con la idea de la descomposición unimodular de Barvinok, su versión efectiva, y finalizaremos con el truco de la polarización de Brion y algunas conclusiones.

4.1. Descomposición Unimodular

Dado un cono punteado $K = \sum_{i=1}^{k} \mathbb{R}^+ w_i \subseteq \mathbb{R}^d$, con $w_i \in \mathbb{Z}^d$, el principal problema que surge a la hora de hallar una forma "corta" de escribir σ_K es el de encontrar los puntos enteros dentro de un paralelepípedo fundamental (cfr. fórmula (2.1)).

Siempre podemos escribir a K como unión de conos simpliciales y reducir el problema a hallar $\sigma_K(z) = \frac{\sigma_\Pi(z)}{\prod_{i=1}^{k}(1-z^{w_i})}$ donde $\Pi = \sum_{i=1}^{k}[0,1)w_i$.

El polinomio de Laurent σ_Π tiene un monomio por cada punto entero de Π. Cuando $k = d$, dicha cantidad coincide con $|det(w_1, \ldots, w_d)|$, lo que nos dice que el número de puntos enteros de Π puede ser exponencial en el tamaño de la entrada, aún fijando la dimensión.

Por todo esto no resulta buena idea hallar σ_Π mediante un búsqueda exhaustiva.

Notemos que no habría problema en encontrar σ_Π si $|det(w_1, \ldots, w_d)| = 1$, es decir, si $\{w_1, \ldots, w_d\}$ fuese una base para el lattice $\mathbb{Z}^d$, dado que el 0 siempre está en $\Pi \cap \mathbb{Z}^d$, y el numerador buscado sería $\sigma_\Pi(z) = 1$. En general, si $\{w_1, \ldots, w_k\}$ es una base para el lattice $(K - K) \cap \mathbb{Z}^d$, sólo tendremos el monomio $1 = \sigma_\Pi(z)$.

La idea de Barvinok [7] consiste en escribir para el cono K una *descomposición unimodular* formada por conos unimodulares $\{K_1, \ldots, K_l\}$ junto con $\{\epsilon_1, \ldots, \epsilon_l\} \subseteq \{-1, 1\}$ tales que $[K] = \sum_{i=1}^{l} \epsilon_i [K_i]$, donde decimos que el cono K_i es *unimodular* si los vectores primitivos de sus rayos forman una base para $\mathbb{Z}^d \cap (K_i - K_i)$ (esto equivale a pedir que su paralelepípedo fundamental Π tenga un solo punto entero, el 0 y σ_Π sea igual a 1).

Luego $\sigma_K = \sum_{i=1}^{l} \epsilon_i \sigma_{K_i}$ y esta escritura será "corta" si mostramos que l puede tomarse pequeño.

Sea $K = \sum_{i=1}^{d} \mathbb{R}^+ w_i$ de dimensión d y $w_i \in \mathbb{Z}^d$, y llamemos $ind(K) = |det(w_1, \ldots, w_d)|$.

Denotemos con $\gamma = ind(K)^{-1/d}$, el volumen del conjunto convexo y simétrico $\Gamma = \sum_{i=1}^{d} [-\gamma, \gamma] w_i$ es 2^d. Por el Teorema de Minkowski ([5], pg. 294) existe un $w \in \Gamma \cap \mathbb{Z}^d \setminus \{0\}$. Se tiene que $w = \sum_{i=1}^{d} \alpha_i w_i$ con $|\alpha_i| \leq ind(K)^{-1/d}$.

Tomamos ahora los conos $K_i = \mathbb{R}^+ w + \sum_{j=1, j \neq i}^{d} \mathbb{R}^+ w_j$, y observamos que $ind(K_i) = |det(w_1, \ldots, w_{i-1}, w, w_{i+1}, \ldots, w_d)| \leq ind(K)^{\frac{d-1}{d}}$.

Hay que llevar la cuenta de los polítopos de menor dimensión que aparecen como intersecciones, y sumarlos alternadamente según el principio de inclusión-exculsión.

En el peor de los casos, la cantidad de conos se multiplica por una constante (suponiendo que d permanece fijo), y los índices se elevan a la $\frac{d-1}{d}$. En un número de pasos acotado por un doble logaritmo iterado de $ind(K)$, todos los índices serán 1 y habremos terminado. Al final, la cantidad de conos queda de orden polinomial en $log(ind(K))$, que es polinomial en el tamaño de la entrada.

4.2. Versión efectiva del Teorema de Minkowski

Queda la cuestión de hallar explícitamente el vector w. En [20], los autores siguen el enfoque propuesto por Dyer y Kannan [22].

La idea es conseguir un vector "corto" para que esté en Γ, es decir, todas sus coordenadas en la base $\{w_1, \ldots, w_d\}$ deben ser pequeñas.

Llamando A a la matriz cuyas columnas son los $\{w_1, \ldots, w_d\}$, usan el algoritmo LLL de reducción de base [1] para hallar una base de vectores cortos del lattice generado por las columnas de la matriz A^{-1}.

Es decir, logran escribir $A^{-1}U = A'$ con $U \in \mathbb{Z}^{d\times d}$ unimodular tal que las columnas de A' son "casi" ortogonales y relativamente cortas para la métrica Euclídea. Pero se quiere minimizar la norma infinito de los vectores no nulos del lattice que estas columnas generan (consiguiendo así un vector dentro de Γ).

Éste es el paso más costoso del algoritmo. Se puede hallar el vector $\lambda = A'z$ que minimice la norma infinito, probando con todas las combinaciones lineales enteras de las columnas de A' (i.e. $z \in \mathbb{Z}^d$) con coordenadas menores que cierta cota explícita (ver [22]).

En la práctica se trata de evitar este paso, tomando simplemente la columna de A' de menor norma infinito. No suele ser el vector de menor norma del lattice, pero a los hechos prácticos, la mayoría de las veces resulta casi tan útil.

Por último, el vector $w = A\lambda = Uz$ resulta ser el buscado, pues escrito en la base $\{w_1, \ldots, w_d\}$ minimiza a la mayor de sus coordenadas.

4.3. Polarización de Brion

Se puede evitar llevar la cuenta de los conos de dimensiones menores modificando un poco el algoritmo, aplicándoselo al cono dual $K^* = \{x / < x, y > \leq 0 \ \forall y \in K\}$ en lugar de K, y luego tomando los conos duales de los de mayor dimensión de la descomposición de K^*.

[1] ver apéndice C

Este es el llamado *truco de polarización de Brion [7].*

Si uno tiene $[K] = \sum \epsilon_i [K_i]$, y considera las funciones características de los duales de los K_i, llega a $[K^*] = \sum \epsilon_i [K_i^*]$ ([5] pg.147 Teo. 1.5 y Coro. 1.6).

Como los duales de conos de menor dimensión son conos que contienen subespacios, y por lo tanto sus funciones generatrices son nulas en el cociente, podemos obviarlos a la hora de implementar el algoritmo. Y como el dual de un cono unimodular también es unimodular, este truco permite escribir a la función generatriz del cono K como suma signada de funciones generatrices de conos unimodulares.

Ejemplo 4.3.1 Sea $K = \mathbb{R}^+(1,3) + \mathbb{R}^+(4,1)$. Podemos descomponerlo como

$$[K] = [K_1] - [K_2] - [K_3] + [K_4] + [K_5]$$

donde $K_1 = \mathbb{R}^+(1,0) + \mathbb{R}^+(0,1)$, $K_2 = \mathbb{R}^+(1,3) + \mathbb{R}^+(0,1)$, $K_3 = \mathbb{R}^+(1,0) + \mathbb{R}^+(4,1)$, $K_4 = \mathbb{R}^+(1,3)$ y $K_5 = \mathbb{R}^+(4,1)$ (ver fig.4.1) de donde obtenemos:

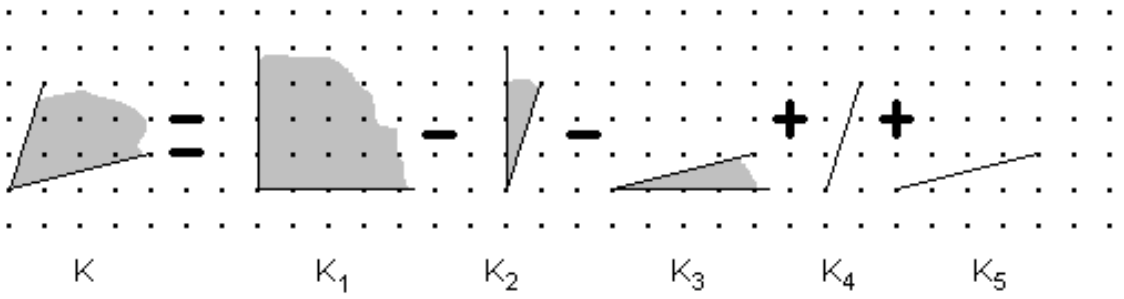

Figura 4.1: Descomponiendo a K

$$\sigma_K(x,y) = \frac{1}{(1-x)(1-y)} - \frac{1}{(1-xy^3)(1-y)} - \frac{1}{(1-x)(1-x^4y)} + \frac{1}{(1-xy^3)} + \frac{1}{(1-x^4y)}.$$

Pero también podríamos haber considerado el dual $K^* = \mathbb{R}^+(-3,1) + \mathbb{R}^+(1,-4)$, descomponerlo como

$$[K^*] = [K_1'] + [K_2'] + [K_3'] - [K_4'] - [K_5']$$

con $K_1' = \mathbb{R}^+(0,-1)+\mathbb{R}^+(1,-4)$, $K_2' = \mathbb{R}^+(-1,0)+\mathbb{R}^+(0,-1)$, $K_3' = \mathbb{R}^+(-1,0)+\mathbb{R}^+(-3,1)$, $K_4' = \mathbb{R}^+(-1,0)$ y $K_5' = \mathbb{R}^+(0,-1)$ (ver fig. 4.2). y obtenemos

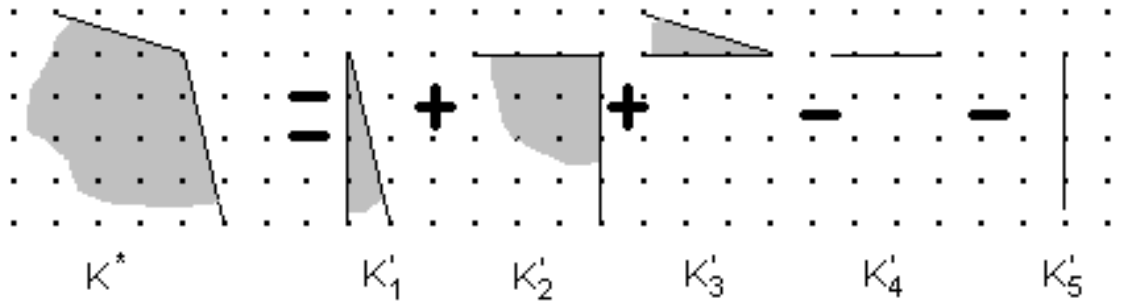

Figura 4.2: Descomponiendo a K^*

$$[K] = [K_1'^*] + [K_2'^*] + [K_3'^*] - [K_4'^*] - [K_5'^*]$$

con $K_1'^* = \mathbb{R}^+(4,1) + \mathbb{R}^+(-1,0)$, $K_2'^* = \mathbb{R}^+(1,0) + \mathbb{R}^+(0,1)$, $K_3'^* = \mathbb{R}^+(1,3) + \mathbb{R}^+(0,-1)$,

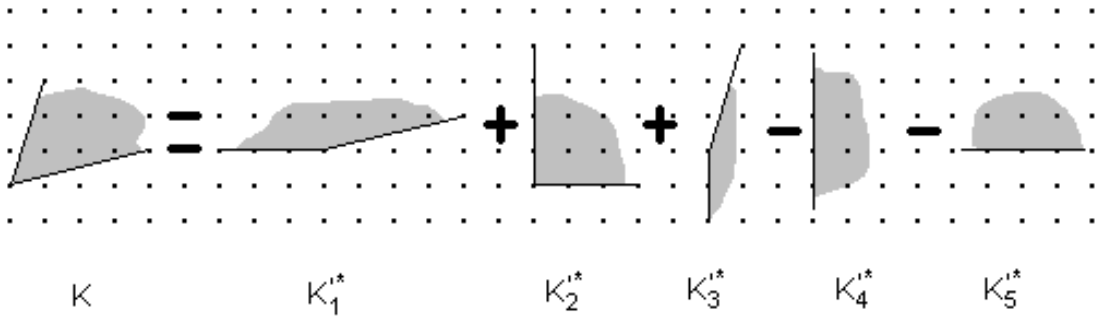

Figura 4.3: Dualizando la descomposición.

$K_4'^* = \mathbb{R}^+(1,0) + \mathbb{R}(0,1)$y $K_5'^* = \mathbb{R}^+(0,1) + \mathbb{R}(1,0)$ (ver fig. 4.3). Las funciones generatrices de los últimos dos conos están en la torsión de $\mathbb{C}[[x^{\pm}, y^{\pm}]]$, por lo que podemos ignorarlas y obtener:

$$\sigma_K(x,y) = \frac{1}{(1-x^{-1})(1-x^4y)} + \frac{1}{(1-x)(1-y)} + \frac{1}{(1-xy^3)(1-y^{-1})}.$$

4.4. Algunas Aplicaciones

Programación Lineal Entera

Veamos cómo el algoritmo de Barvinok resuelve polinomialmente el problema de Programación Lineal Entera en el caso de la dimensión fija.

Dado un polítopo racional $P \subseteq \mathbb{R}^d$, podemos calcular una función racional corta que represente a $\sigma_P(z)$. La cantidad de puntos enteros de P es $\sigma_P(\mathbf{1})$. No podemos hacer esta cuenta en cada término de la forma corta de σ_P, ya que siempre se nos anulan los denominadores (recordemos que son productos de binomios de la forma $(1 - z^w)$). Sin embargo, si lo único que nos interesa es saber si $P \cap \mathbb{Z}^d$ es o no vacío, el problema se reduce a saber si σ_P es o no cero. En caso de no serlo, sería suma de algunos monomios, con coeficientes 1. Basta con evaluar la función generatriz en cualquier vector $v \in \mathbb{R}^d$ con todas sus coordenadas estrictamente positivas (de manera que no anule a ninguno de los denominadores de la forma corta que devuelve el algoritmo) y ver si el resultado es o no 0.

Ehrhart efectivo

Otra consecuencia del Algoritmo de Barvinok, no menos importante, es la existencia de una manera eficiente de calcular $L_P(t)$ (ver [20] y [18]). Veámoslo para $P \subseteq \mathbb{R}^d$ entero.

Por la Observación 2.2.2 alcanza con encontrar $Ehr_P(x) = \frac{f(x)}{(1-x)^{d+1}}$ y tomar $L_P(t) = \sum_{j=0}^{d} c_j \binom{t+d-j}{d}$ donde los c_j son los coeficientes de f.

Pero $Ehr_P(x) = \sigma_{C(P)}(z, x)|_{z=\mathbf{1}}$. Como podemos hallar una representación corta de $\sigma_{C(P)}$ (gracias a Barvinok), querríamos evaluar las primeras variables en 1. Esto podría llegar a cancelar algún denominador de las funciones racionales que aparecen en la representación de $\sigma_{C(P)}$, pero no anula al denominador de $\sigma_{C(P)}$, pues es un producto de binomios de la forma $(1 - xz^w)$ y luego de hacer $z = \mathbf{1}$ quedará un producto de varias copias de $(1 - x)$. El algoritmo de *sustitución monomial* de [8] resuleve precisamente esto, permite componer

una función racional con una aplicación monomial (como puede ser evaluar las primeras coordenadas en 1), en un tiempo polinomial (suponiendo d fijo).

Con ideas similares, se puede recuperar $\sigma_P(z)$ como el coeficiente de grado 1 de $\sigma_{C(P)}(z,x) = \sigma_{C(P)}(z)(x)$.

Observación 4.4.1 *El truco de Brion resulta ser de mucha utilidad para calcular $\sigma_{C(P)}(z,x)$ cuando P tiene muchos vértices y pocas caras.*

Capítulo 5

Fórmulas de Euler MacLaurin

En este capítulo mencionaremos una generalización de la Fórmula de Euler-Maclaurin exacta a varias dimensiones, que discretiza la integral de una función, permitiendo atacar problemas más generales que el de contar puntos enteros en las dilataciones de un polítopo, o de sumas de Minkowski de varios polítopos. Al final mencionamos cómo sirven estas herramientas para tratar el problema de enumerar flujos admisibles enteros en una red.

Definición 5.0.2 *Dado un operador diferencial D, definimos $Td(D)$ el* operador de Todd *asociado a D como:*

$$Td(D) = \frac{D}{1 - e^{-D}} = 1 + \frac{D}{2} + \frac{D^2}{12} - \frac{D^4}{720} + \ldots = \sum_{k \geq 0} \frac{B_k D^k}{k!},$$

siendo $B_k \in \mathbb{Q}$ los números de Bernoulli.

Similarmente, si $G : \mathbb{C} \longrightarrow \mathbb{C}$ es una función holomorfa en un entorno del 0, se define $G(D)$ como el operador diferencial de orden infinito tal que

$$G(D)(f) = \sum_{k \geq 0} \frac{G^k(0)}{k!} D^k(f),$$

para aquellas funciones f donde la serie esté definida y resulte absolutamente convergente.

Recordemos la fórmula exacta de Euler-MacLaurin ([31] y [30]). Sea $f \in \mathbb{C}[t]$ un polinomio en una variable y $a < b \in \mathbb{Z}$. Entonces

$$\sum_{n=a}^{b} f(n) = \left(Td(\frac{\partial}{\partial h_1}) Td(\frac{\partial}{\partial h_2}) \right) \Big|_{h_1=h_2=0} \int_{a-h_1}^{b+h_2} f(t)dt.$$

Como f es un polinomio, la integral $\int_{a-h_1}^{b+h_2} f(t)dt$ es un polinomio en $\mathbb{C}[h_1, h_2]$ y los operadores de Todd se reducen a calcular sumas finitas.

En [30] los autores generalizan la fórmula para más funciones (que incluyen exponenciales de bases pequeñas multplicadas por polinomios) y a más dimensiones.

Ésta última generalización merece ciertos comentarios.

En lugar de hablar de intervalos $[a, b]$, se trabaja sobre polítopos enteros de dimensión máxima. Y, por cuestiones técnicas, se habla de polítopos simples (hecho que siempre se da en dimensión 1 y 2).

Decimos que un polítopo P es *totalmente unimodular*, si es simple y las aristas que salen de los vértices yacen sobre vectores que generan $\mathbb{Z}^d$ (es decir, los conos de sus vértices son unimodulares).

Cabe aclarar que en dimensión 1 todos los polítopos enteros son totalmente unimodulares.

En dimensiones mayores, las fórmulas de Euler-MacLaurin se ven sumamente simplificadas en el caso totalmente unimodular.

Dado un polítopo entero simple $P = \bigcap_{i=1}^{m} \{x/ < x, u_i > +\lambda_i \geq 0\} \subseteq \mathbb{R}^d$ con m facetas y los $u_i \in \mathbb{Z}^d$ primitivos. Consideramos el polítopo dilatado $P(h) = \bigcap_{i=1}^{m} \{x/ < x, u_i > +\lambda_i + h_i \geq 0\}$. Notemos que para pequeñas perturbaciones $h \in \mathbb{R}^m$, $P(h)$ sigue siendo simple.

Notamos a las facetas como $\delta_i = P \cap \partial H_i$, con $H_i = \{x/ < x, u_i > +\lambda_i \geq 0\}$ los semiespacios que definen a P. Para cada cara F existe un único subconjunto de índices $I_F \subseteq \{1, \ldots, m\}$ tales que $F = \cap_{i \in I_F} \delta_i$ (pues P es simple).

Para cada $v \in Vert(P)$, los $\{u_i\}_{i \in I_v}$ forman una base de $\mathbb{R}^d$ y los vectores de su base dual $\{\alpha_{i,v}\}_{i \in I_v}$ apuntan en las direcciones de las aristas que salen de v.

Cada cara F tiene asociado un espacio vectorial normal V_F^* definido como el generado por los $\{u_i\}_{i\in I_F}$ (de hecho, éstos forman una base). Llamamos $\{\alpha_{i,F}\}_{i\in I_v}$ a su base dual.

Definimos entonces el *grupo abeliano finito asociado* a F como

$$\Gamma_F = \frac{V_F^* \cap \mathbb{Z}^d}{\bigoplus_{i\in I_F} \mathbb{Z}u_i}.$$

Tiene sentido entonces calcular $\exp(2\pi i < \gamma, \alpha_{j,F} >)$ para $\gamma \in \Gamma_F$ y $j \in I_F$, pues el producto interno está definido módulo 1.

Como último ingrediente para la fórmula, se tiene un orden natural entre los Γ_F inducido por el orden de las caras. Si $F \subseteq E$ son caras de P, los conjuntos de índices cumplen $I_E \subseteq I_F$, entonces $V_E^* \subseteq V_F^*$ y $V_E^* \cap \bigoplus_{i\in I_F} \mathbb{Z}u_i = \bigoplus_{i\in I_E} \mathbb{Z}u_i$ lo que induce un monomorfismo canónico $\Gamma_E \subseteq \Gamma_F$.

Llamamos entonces $\Gamma_F^\flat = \Gamma_F \setminus \bigcup_{E\supsetneq F} \Gamma_E$ (donde E recorre las caras del polítopo que contienen estrictamente a F).

Ahora sí estamos en condiciones de enunciar la versión multidimensional de las fórmulas de Euler-MacLaurin, debida a Brion y Vergne [16].

Teorema 5.0.3 *Con la notación anterior, si f es un polinomio multivariado, se tiene que:*

$$\sum_{n\in P\cap\mathbb{Z}^d} f(n) = \sum_F \sum_{\gamma\in\Gamma_F^\flat} \left(\prod_{j\notin I_F} \frac{\frac{\partial}{\partial h_j}}{1-e^{-\partial/\partial h_j}} \prod_{j\in I_F} \frac{\frac{\partial}{\partial h_j}}{1-e^{2\pi i<\gamma,\alpha_{j,F}>}e^{-\partial/\partial h_j}} \right) \Bigg|_{h=0} \int_{P(h)} f.$$

Observación 5.0.4 *La misma fórmula se aplica a otras funciones f, como es el caso de las exponenciales de base suficientemente pequeñas.*

Observación 5.0.5 *Cuando P es totalmente unimodular nos queda la elegante fórmula:*

$$\sum_{n\in P\cap\mathbb{Z}^n} f(n) = \left(Td(\frac{\partial}{\partial h_1}) \dots Td(\frac{\partial}{\partial h_d}) \right) \Bigg|_{h=0} \int_{P(h)} f,$$

dado que en este caso, todos los Γ_F resultan triviales, y el único $\Gamma_F^\flat$ no vacío es el que corresponde a $F = P$ con $I_P = \emptyset$.

Lo que nos va a importar de estas fórmula es que valen para $f \equiv 1$, relacionando así el número de puntos enteros de P con ciertos operadores diferenciales aplicados a la función $vol(P(h))$.

Como vimos en la Proposición 3.1.5 podemos escribir a $vol(P(h))$ como una función racional en los vértices y en las aristas de P, una vez fijadas la variable vectorial x de manera genérica (no ortogonal a ninguna arista).

Para h pequeño, el polítopo $P(h)$ sigue siendo simple, y las direciones de las aristas no cambian (ya que son paralelas a las $\alpha_{j,v}$ que se definen a partir de las u_i, o sea, las normales a las facetas).

Observando también que los vértices $v(h)$ de $P(h)$ se consiguen como

$$v(h) = \sum_{i \in I_v} -(\lambda_i + h_i)\alpha_{i,v},$$

tenemos que dependen polinomialmente de h.

Entonces, los denominadores de la fórmula 3.3 no varían, y $vol(P(h))$ resulta ser un polinomio en h (al menos, localmente).

Los operadores de Todd se reducen a sumas finitas de operadores diferenciales aplicados a una función polinomial, por lo que dará también una función polinomial.

Como la fórmula vale para polítopos enteros, sigue valiendo si cambiamos P por $P(b)$ con $b \in \mathbb{Z}^m$ tal que los vértices de $P(b)$ sigan siendo enteros, teniendo en cuenta que $P(b)(h) = P(b+h)$. Esto sucede para cualquier $b \in \mathbb{Z}^m$ en el caso de un polítopo totalmente unimodular.

Antes de sacar conclusiones apresuradas, recordemos que en todo momento suponíamos que la estructura combinatoria de P no se veía alterada. Entre otras cosas, $P(h)$ siempre era simple. Esto puede no pasar para h arbitrario. Pueden desaparecer vértices (ver fig. 5.1), puede elegirse cierto h tal que $P(h)$ se reduzca al 0 (poniendo $h_i = -\lambda_i$), y en todos esos casos la fórmula no sirve. Debemos entonces evitar los h críticos donde estas cosas suceden.

Dichos vectores se caracterizan como aquellos tales que tiene solución alguno de los sistemas $\{< u_i, x >= -\lambda_i - h_i\}_{i \in I}$ con $I \subseteq \{1, \ldots, m\}$ de cardinal $d+1$ (es decir, algún vértice es intersección de más de d caras).

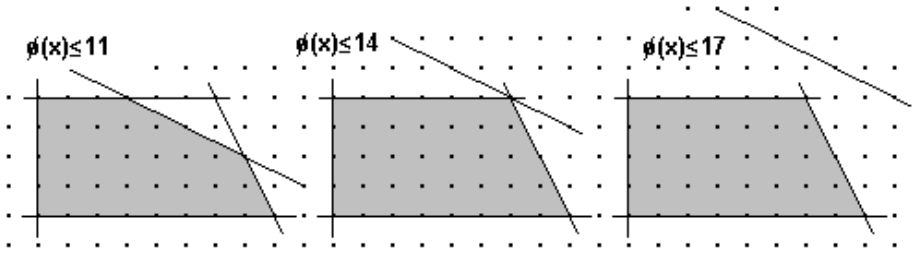

Figura 5.1: Pueden desaparecer vértices.

Para que esto suceda, la matriz del sistema deberá tener el mismo rango que la aumentada, que será menor que $d+1$ (pues los $u_i \in \mathbb{R}^d$).

En particular, el determinante de la matriz aumentada (de dimensiones $(d+1) \times (d+1)$) debe ser 0, y si desarrollamos por la última columna, nos queda una condición lineal homogénea sobre los $h_i + \lambda_i$ con $i \in I$, determinando un hiperplano en $\mathbb{R}^m$, si los $\{u_i\}$ generaban todo $\mathbb{R}^d$, y todo $\mathbb{R}^d$ si el rango r de la matriz del sistema era menor a d.

En este último caso, deberíamos considerar los hiperplanos definidos por los determinantes de los menores $(r+1) \times (r+1)$ que involucran a la última columna.

Eliminando de $\mathbb{R}^m$ dichos hiperplanos (donde pueden aparecer casos degenerados de polítopos no simples), nos queda el espacio dividido en "cámaras" abiertas y conexas (las componentes conexas del complemento de la unión de todos los hiperplanos).

Concluimos entonces (ver [39] y [2]) el siguiente:

Teorema 5.0.6 *Con la notación anterior, si P es un polítopo totalmente unimodular, la función $\sharp(P(h) \cap \mathbb{Z}^n)$ depende polinomialmente de h en cada cámara.*

En [3] se proponen algoritmos para caracterizar dichas funciones considerando residuos totales multivariados.

Comentario Estos polítopos suelen aparecer en problemas de flujos de redes (ver [3]). Éstos consisten en un grafo dirigido $G = (V, E)$ y donde a cada arista $e \in E$ le corresponde una capacidad $c_e \in \mathbb{Z}_{\geq 0}$ y a cada vértice $v \in V$ un exceso $b_v \in \mathbb{Z}$. Un *flujo* en dicha red consiste

en asignar a cada arista $e \in E$ un valor $x_e \leq c_e$ no negativo, tal que para cada vértice $v \in V$, la diferencia entre lo que sale y lo que entra es igual al exceso, es decir:

$$\sum_{e=(v,b)\in E} x_e - \sum_{e=(a,v)\in E} x_e = b_v.$$

Los sistemas de estos problemas dan polítopos totalmente unimodulares (ver [37]), por lo que el número de flujos enteros verifica un comportamiento localmente polinomial en los vectores de excesos y capacidades.

Observación 5.0.7 *En el caso no unimodular, la misma línea de razonamiento lleva a probar que la función* $\sharp(P(h) \cap \mathbb{Z}^n)$ *da un cuasi-polinomio locale (ver [39]).*

Capítulo 6

Volúmenes discretos

Una manera discreta de medir polítopos es contar la cantidad de puntos enteros. Se presenta el inconveniente a la hora de juntar polítopos (e.g., en una triangulación), y no poder simplemente sumar dichas cantidades sin prestar atención a lo que sucede en las intersecciones (a pesar de tratarse de polítopos de menor dimensión). En este capítulo trabajaremos con volúmenes discretos inducidos por normas. Éstos miden cero en polítopos de menor dimensión, comportándose de manera similar al volumen usual. Existen varias familias de polítopos enteros en los que estos volúmenes discretos coinciden con el estándar, por ejemplo los paralelepípedos, los zonotopos, todos los de dimensión ≤ 2, entre otros. A continuación presentaremos teoremas análogos a los vistos para funciones generatrices y terminaremos con una interesante identidad que relaciona entre sí los ángulos sólidos de las caras de un polítopo.

Definición 6.0.8 *Dada una norma* $\|.\| : \mathbb{R}^d \longrightarrow \mathbb{R}$ *definimos el* ángulo sólido inducido $\omega^{\|.\|}$ *como la función que a cada cono* K *de vértice* v*, le asigna el número real*

$$\frac{|B^{\|.\|}(v,1) \cap K|}{|B^{\|.\|}(v,1)|},$$

siendo $|.|$ *la medida de Lebesgue usual de* $\mathbb{R}^d$*.*

Dado un polítopo P *y* $p \in P$*, definimos* $\omega_p^{\|.\|}(P) = \omega^{\|.\|}(K_p)$*.*

La función generatriz inducida *por* $\|.\|$ *se define como*

$$\sigma^{\|\cdot\|}(z) = \sum_{p\in P} \omega_p^{\|\cdot\|}(P) z^p = \sum_{F\subseteq P} \omega_F^{\|\cdot\|}(P)\sigma_F^{\circ}(z),$$

donde $\omega_F^{\|\cdot\|}(P) = \omega_p^{\|\cdot\|}(P)$ *para algun* $p \in F$.

El volumen discreto *inducido por la norma es*

$$VD^{\|\cdot\|}(P) = \sum_{p\in P\cap\mathbb{Z}^d} \omega_p^{\|\cdot\|}(P) = \sigma^{\|\cdot\|}(\mathbf{1}).$$

Observación 6.0.9 *Para puntos interiores a* P*, el ángulo sólido da siempre* 1*, y para los* $p \in relint(F)$ *con* F *una faceta da siempre* $\frac{1}{2}$*, sea cual sea la norma en cuestión.*

Observación 6.0.10 *Es interesante notar que si* $d \leq 2$*, todos los volúmenes discretos inducidos por normas coinciden con el canónico para polítopos enteros.*

Para $d = 1$ es trivial, y para $d = 2$ es una versión del Teorema de Pick.

Si P es un polígono convexo de $\mathbb{R}^2$ con vértices enteros, su área, según Pick, es $I + \frac{B}{2} - 1$ donde $I = \sharp(P^\circ \cap \mathbb{Z}^2)$ y $B = \sharp(\partial P \cap \mathbb{Z}^2)$. Cuando calculamos $VD^{\|\cdot\|}(P)$, cada punto interior aporta 1 a la suma, y los de la frontera aportan $\frac{1}{2}$, salvo los vértices, cuyos ángulos sólidos son menores. Como la suma de todos los ángulos complementarios da un giro completo (ver fig. 6.1) , la suma de sus ángulos sólidos del borde dará precisamente $\frac{B}{2} - 1$.

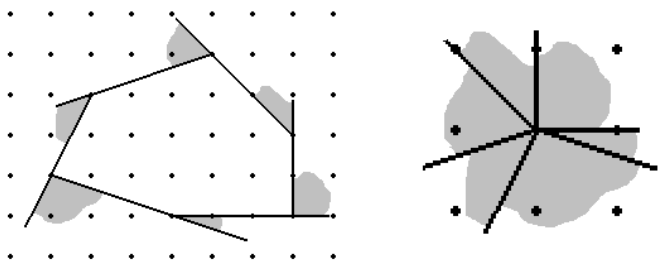

Figura 6.1: Los ángulos complementarios suman un giro completo.

Observación 6.0.11 *Sin embargo, para $d \geq 3$ no podemos esperar un resultado tan simpático. Consideremos $d = 3$ y para cada $n \in \mathbb{N}$ el tetraedro P_n de vértices e_1, e_2, ne_3 y $e_1+e_2+ne_3$ (ver fig. 6.2).*

Los únicos puntos enteros de P_n son los vértices y $Vol(P_n) = \frac{n}{3}$. Para n grande, dicho volumen no puede coincidir con el discreto inducido por ninguna norma, ya que cada ángulo sólido está acotado superiormente por 1, y los volúmenes de estos tetraedros crecen con n.

Similarmente se construyen contraejemplos para $d \geq 4$ considerando $P_n \times [0,1]^{d-3}$.

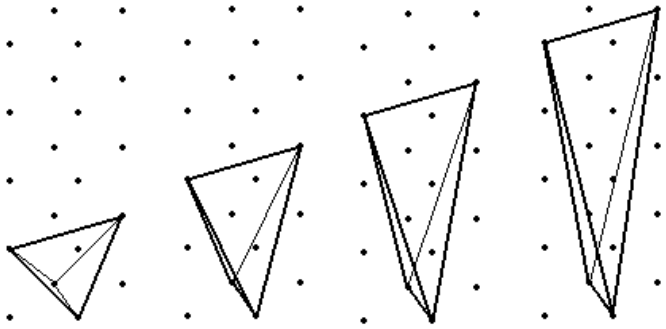

Figura 6.2: P_1, P_2, P_3 y P_4

Se tiene un paralelo a la teoría de Ehrhart para los volúmenes discretos.

Teorema 6.0.12 *(ver [11]) Si P es un polítopo racional, tenemos*

$$\sigma_P^{\|\cdot\|}(z) = \sum_{v \in Vert(P)} \sigma_{K_v}^{\|\cdot\|}(z).$$

Se demuestra aplicando las identidades del Teorema de Brion a cada cara abierta de P, recordando que $\sigma_P^{\|\cdot\|}(z) = \sum_{F \subseteq P} \omega_F^{\|\cdot\|}(P)\sigma_F^\circ(z)$.

Llamando $A_P^{\|\cdot\|}(t) = VD^{\|\cdot\|}(tP) = \sum_{F \subseteq P} \omega_F^{\|\cdot\|}(P)L_F^\circ(z)$, está claro que dicha función es un cuasi-polinomio en t, cuyo período divide al denominador de P.

Teorema 6.0.13 *Siendo K un cono racional con vértice en el origen y $v \in \mathbb{R}^d$, entonces*

$$\sigma_{v+K}^{\|\cdot\|}(z^{-1}) = (-1)^d \sigma_{-v+K}^{\|\cdot\|}(z).$$

Observación 6.0.14 *Si $dim(K) < d$ ambos miembros dan cero.*

La demostración es análoga a la de σ_{v+K}, sólo que más fácil aún, puesto que para dimensiones menores a d los volúmenes discretos dan cero, por lo que basta probarlo para los conos simpliciales de dimensión d que aparecen en la triangulación de K y sumar las funciones generatrices inducidas por $\|.\|$.

De acá se deduce el siguiente:

Teorema 6.0.15 *(Reciprocidad de MacDonald [11]) Sea $P \subseteq \mathbb{R}^d$ un polítopo racional, entonces*

$$A_P^{\|.\|}(-t) = (-1)^d A_P^{\|.\|}(t).$$

Demostración. Si P es entero, $A_P^{\|.\|}(t) = \sigma_{tP}^{\|.\|}(\mathbf{1}) = \sum_{v \in Vert(P)} z^{tv} \sigma_{-v+K_v}^{\|.\|}(\mathbf{1})$ para $t \geq 1$. Queremos ver que sigue valiendo para el resto de los $t \in \mathbb{Z}$ para deducirlo del Teorema anterior.

Para ello alcanza con ver que el miembro de la derecha es un polinomio en t, aún para $t \leq 0$. Y esto es por el mismo motivo de antes, se trata de una sucesión recursiva lineal en t, con raíces no nulas, por lo que sigue verificando el mismo vector para subíndices negativos.

Para los polítopos P no enteros, se procede igual que en el caso de los polinomios de Ehrhart. Llamando n al denominador común, tenemos $A_P^{\|.\|}(t) = (\sum_{p \in n\mathbb{Z}^d} \omega_p^{\|.\|}(nP) z^p)(\mathbf{1})$ se obtiene evaluando en $z = \mathbf{1}$ el polinomio de Laurent que se obtiene quedándonos con los monomios de $\sigma_{nP}^{\|.\|}$ cuyos grados son múltiplos de n, es decir, $A_P^{\|.\|}(t)$ se consigue promediando todos los $\sigma_{nP}^{\|.\|}(\xi z)$ con $\xi \in \mathbb{G}_n^d$, y luego evaluando $z = \mathbf{1}$.

Queda así que $A_P^{\|.\|}(t)$ satisface una recursividad lineal cuyas raíces están en $\mathbb{G}_n$ (por ser un cuasi-polinomio de período n) y se escribe como

$$\sigma_{tnP}^{\|.\|}(\xi z)(\mathbf{1}) = \frac{1}{n^d} \sum_{\xi \in \mathbb{G}_n^d} \sum_{v \in Vert(P)} (\xi z)^{tnv} \sigma_{-v+K_v}^{\|.\|}(\mathbf{1}),$$

y para los $t < 0$ el miembro derecho da lo mismo que con $-t$ sólo que multiplicado por $(-1)^d$, que es el efecto que produce en cada $\sigma_{-v+K_v}^{\|.\|}$ componer con z^{-1}. Q.E.D.

Observación 6.0.16 *Si P es entero, el polinomio $A_P^{\|.\|}$ resulta par para valores pares de d e impar para los valores impares.*

Teorema 6.0.17 *Para todo P entero se cumple que $A_P^{\|.\|}(0) = 0$.*

Observación 6.0.18 *Esto equivale a decir que*

$$A_P^{\|.\|}(0) = \sum_{F \subseteq P} \omega_F^{\|.\|}(P) L_F^{\circ}(0) = \sum_{F \subseteq P} \omega_F^{\|.\|}(P)(-1)^{dim(F)} = 0,$$

fórmula conocida como la Relación de Gram. *[28]*

Demostración. Si d es impar esto es obvio pues $A_P^{\|.\|}$ es impar.

Triangulando P y observando que $A_P^{\|.\|}$ es la suma de los polinomios asociados a los simplices de dimensión d de dicha triangulación, alcanza con probar que $A_P^{\|.\|}(0) = 0$ para P un $d-$simplex de dimensión par.

Se deduce del caso impar, considerando en $\mathbb{R}^{d+1}$ el $(d+1)-$simplex P' con base $P \times \{0\}$ y vértice ne_{d+1}, para $n \in \mathbb{N}$ arbitrariamente grande.

Extendemos a $\mathbb{R}^{d+1}$ la norma $\|.\|$ que teníamos definida en $\mathbb{R}^d$, tomando el máximo con el módulo de la nueva coordenada, es decir $\|(v, \lambda)\|' = \text{máx}\{\|v\|, |\lambda|\}$. La suma alternada de los ángulos sólidos de las caras de este simplex (respecto de la norma extendida) debe dar cero, por tratarse del caso de dimensión impar.

El ángulo sólido correspondiente al vértice ne_{d+1} tiende a cero. El resto de las caras de P' se dividen entre las que están contenidas en P y las que se obtienen de caras de P agregándole el vértice ne_{d+1}.

Cuando $n \longrightarrow \infty$, los ángulos sólidos de las caras del primer tipo, respecto de $\|.\|'$ en $\mathbb{R}^{d+1}$, tienden a la mitad de los correspondientes ángulos respecto de $\|.\|$ en $\mathbb{R}^d$. Y para cada cara F de P, el ángulo sólido de la cara de P' que se obtiene agregándole ne_{d+1}, tiende al correspondiente en $\mathbb{R}^d$.

Como en el segundo caso la dimensión de F aumenta en uno, tomando límite cuando $n \longrightarrow \infty$ llegamos a la relación

$$\begin{aligned} 0 &= \frac{1}{2}\sum_{F\subseteq P}\omega_F^{\|.\|}(P)(-1)^{dim(F)} - \sum_{F\subseteq P}\omega_F^{\|.\|}(P)(-1)^{dim(F)} \\ &= \frac{-1}{2}\sum_{F\subseteq P}\omega_F^{\|.\|}(P)(-1)^{dim(F)} \end{aligned}$$

de donde se llega a la relación de Gram para P. Q.E.D.

También se define la serie de los ángulos sólidos como

$$Solid_P^{\|.\|}(x) = \sum_{t\geq 0} A_P^{\|.\|}(t)x^t = \sum_{F\subseteq P}\omega_F^{\|.\|}(P)Ehr_F^{\circ}(x)$$

y como los $\omega_F^{\|.\|}(P) \geq 0$ tenemos que $Solid_P^{\|.\|}(x) = \frac{\sum_{i=1}^{d} a_i x^i}{(1-x)^d}$ con los $a_i \geq 0$, y llegamos a la expresión $A_P^{\|.\|}(t) = \sum_{i=1}^{d} a_i \binom{t+d-i}{d}$, y los razonamientos de [13], usados en la Prop. 2.3.1 se aplican también a $A_P^{\|.\|}(t)$ para acotar sus raíces.

Observación 6.0.19 *Como $A_P^{\|.\|}(t) = \sum_{F\subseteq P}\omega_F^{\|.\|}(P)L_F^{\circ}(t)$ y el único polinomio de la sumatoria con grado d es el correspondiente a $F = P$, y $\omega_P^{\|.\|}(P) = 1$, resulta que el coeficiente principal de $A_P^{\|.\|}$ también es el volumen de P.*

Apéndice A

Sucesiones Recursivas Lineales

Trabajaremos con sucesiones $\{a_i\}_{i\in\mathbb{N}_0}$ contenidas en algún anillo conmutativo A (generalmente $\mathbb{C}$). Varias de las identidades pueden generalizarse a sucesiones indexadas en todo $\mathbb{Z}$.

Cálculo en diferencias:

Definición A.0.20 *Sea S el operador lineal* shift *definido en el A-módulo de sucesiones, que a cada sucesión $a = \{a_i\}_{i\in\mathbb{N}}$ le asigna $Sa = \{Sa_i\}_{i\in\mathbb{N}}$ definida por $Sa_n = a_{n+1}$.*

También podemos definirlo en $A[X]$ como $SP(x) = P(x+1)$.

El operador de diferencia *o* derivada discreta *se define como $\Delta = S - I$, donde I es la identidad, es decir $\Delta a_n = a_{n+1} - a_n$, y para polinomios sería $\Delta P(x) = P(x+1) - P(x)$.*

El operador de sumatoria *o* integral discreta *se define sólo para sucesiones, como $\Sigma a_n = \sum_{i=0}^{n-1} a_i$ y $\Sigma a_0 = 0$. En el caso de sucesiones indexadas en $\mathbb{Z}$ definimos $\Sigma a_{-n} = -\sum_{i=-n}^{-1} a_i$.*

Observación A.0.21 *Se tiene que:*

- $\Delta\Sigma = I$.
- $\Sigma\Delta a_n = a_n - a_0$ *la famosa suma telescópica, que en este contexto hace las veces de Teorema Fundamental del Cálculo.*

- $\Delta(ab) = b\Delta a + Sa\Delta b$ *juega un rol similar al de la regla del producto.*

  Pasando un término y aplicando a ambos lados el operador Σ *obtenemos la identidad de Abel:*

$$a_n b_n - a_0 b_0 - \sum_{i=0}^{n-1} a_{i+1}(b_{i+1} - b_i) = \sum_{i=0}^{n-1} b_i(a_{i+1} - a_i),$$

  que viene a hacer las veces de integral por partes.

Definición A.0.22 *En el contexto discreto nos será de utilidad trabajar con los* exponenciales descendientes

$$x^{(n)} = \prod_{i=0}^{n-1}(x-i) = x(x-1)\dots(x-n+1)$$

donde $n \geq 0$, $x^{(n)}$ *es un polinomio en* x *mónico de grado* n *y* $x^{(0)} = 1$.

Observación A.0.23 *Para* $x \in \mathbb{N}_0$ *tenemos que* $x^{(n)} = n!\binom{x}{n}$. *De la identidad* $\binom{x}{n-1} + \binom{x}{n} = \binom{x+1}{n}$ *obtenemos:*

$$\begin{aligned}
\binom{x}{n-1} + \binom{x}{n} &= \binom{x+1}{n} \\
\binom{x}{n-1} &= \binom{x+1}{n} - \binom{x}{n} \\
(n!)\binom{x}{n-1} &= (n!)\binom{x+1}{n} - (n!)\binom{x}{n} \\
nx^{(n-1)} &= (x+1)^{(n)} - x^{(n)} \\
nx^{(n-1)} &= \Delta x^{(n)}.
\end{aligned}$$

Observación A.0.24 *Los operadores* S *e* I *conmutan, por lo que podemos aplicar la fórmula del binomio de Newton y obtener*

$$\Delta^n = (S-I)^n = \sum_{i=0}^{n} \binom{n}{i} S^i (-I)^{n-i},$$

es decir

$$\Delta^n a_k = \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} a_{k+i}. \tag{A.1}$$

De la misma manera, como Δ y I conmutan obtenemos

$$S^n = (I+\Delta)^n = \sum_{i=0}^{n} \binom{n}{i} \Delta^i (I)^{n-i} = \sum_{i=0}^{n} \binom{n}{i} \Delta^i,$$

o sea

$$a_{k+n} = \sum_{i=0}^{n} \binom{n}{i} \Delta^i a_k = \sum_{i=0}^{n} \frac{\Delta^i a_k}{i!} n^{(i)},$$

que hace las veces de fórmula de Taylor discreta (siempre que $n!$ sea inversible en A).

En el caso de polinomios observamos que si $P(x) = \sum_{i=0}^{n} p_i x^i$ podemos escribirlo como $P(x) = \sum_{i=0}^{n} q_i x^{(i)}$ donde $p_n = q_n$, dado que los $\{x^{(k)}\}_{k\in\mathbb{N}_0}$ son mónicos, y por lo tanto forman una base de $A[X]$.

Entonces $\Delta P(x) = \Delta \sum_{i=0}^{n} q_i x^{(i)} = \sum_{i=0}^{n} q_i \Delta x^{(i)} = \sum_{i=1}^{n} q_i i x^{(i-1)}$. De aquí que el grado disminuye y

$$\Delta^n P(x) = n! p_n \in A \subseteq A[X], \tag{A.2}$$

por lo que podremos recuperar el coeficiente principal de P. Si $k > n$ queda $\Delta^k P(x) = 0$ y la fórmula de Taylor discreta se convierte en la identidad polinomial:

$$P(x) = \sum_{i=0}^{n} \frac{\Delta^i P(x_0)}{i!} (x - x_0)^{(i)}.$$

De dicha fórmula se deduce una caracterización de los polinomios $P \in \mathbb{C}[X]$ tales que $P(\mathbb{Z}) \subseteq \mathbb{Z}$. Son precisamente las combinaciones $\mathbb{Z}-$lineales de los polinomios $\binom{x}{k}$, dado que éstos claramente verifican las condiciones, y cualquier polinomio $P \in \mathbb{C}[X]$ con $P(\mathbb{Z}) \subseteq \mathbb{Z}$ tendrá $\Delta^k P(0) \in \mathbb{Z}\ \forall\, k \geq 0$ entonces

$$P(x) = \sum_{k=0}^{n} \frac{\Delta^k P(0)}{k!} x^{(k)} = \sum_{k=0}^{n} \Delta^k P(0) \binom{x}{k}.$$

Recursividad lineal:

Definición A.0.25 *Decimos que una sucesión $\{a_n\} \subseteq A$, indexada en $\mathbb{N}_0$ o en $\mathbb{Z}$, es* recursiva lineal *si satisface cierta* relación de recurrencia *de la forma:*

$$a_{n+k} = \sum_{i=0}^{k-1} r_i a_{n+i}$$

para cierto $r = (r_0, \ldots, r_{k-1}) \in A^k$ *fijo. Decimos que es de* orden k *si* $r_0 \neq 0$*, y que* verifica r *si queremos especificar la relación de recurrencia.*

El polinomio característico *de la recursión* r *es* $Char_r(T) = T^k - \sum_{i=0}^{k-1} r_i T^i$.

Notamos $\mathcal{S}(r) \subseteq A^{\mathbb{N}_0}$ *al* $A-$*módulo de sucesiones que verifican* r.

Observación A.0.26 *Si* $r \in A^k$*, cualquier* $a \in \mathcal{S}(r)$ *queda unívocamente determinada por sus primeros* k *términos.*

Cálculo Eficiente

A continuación veremos una manera de calcular a_m dado $m \in \mathbb{N}$, $r \in A^k$ y $a_0, a_1, \ldots, a_{k-1}$, y más adelante cómo implementarla de manera eficiente, entendiendo por "eficiente" que el número de pasos sea polinomial en el tamaño de la entrada, sin preocuparnos por la complejidad de cada operación en A.

Consideramos la matriz $S \in A^{k\times k}$ y la sucesión de vectores $\{\widehat{a}_n\}_{n\geq k-1} \subseteq A^k$ definidos por

$$S = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ r_0 & r_1 & \cdots & r_{k-2} & r_{k-1} \end{pmatrix} \qquad \widehat{a}_{k-1} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-2} \\ a_{k-1} \end{pmatrix} \qquad \widehat{a}_{n+1} = S\widehat{a}_n \quad \forall\, n \geq k-1.$$

Observación A.0.27 $S \in A^{k\times k}$ *es la matriz del operador shift restringido a* $\mathcal{S}(r)$ *en la base canónica* $\{e^0, e^1, \ldots, e^{k-1}\} \subseteq \mathcal{S}(r)$ *donde las sucesiones* $\{e^0, e^1, \ldots, e^{k-1}\}$ *se definen por* $(e^i)_j = \delta^i_j \ \forall i, j = 0, \ldots, k-1$*, extendiéndolas de modo que se satisfaga la recursión* r.

Como suponemos que $a \in \mathcal{S}(r)$ se puede ver por inducción que

$$\widehat{a}_n = S^{n+1-k}\widehat{a}_{k-1} = \begin{pmatrix} a_{n+1-k} \\ \vdots \\ a_n \end{pmatrix}.$$

Entonces, calculando S^{n+1-k} podemos conseguir $\widehat{a}_n$ y, en particular, $a_n = (\widehat{a}_n)_k$.

Veamos cómo calcular S^n haciendo $O(log(n))$ multiplicaciones de matrices.

Comenzamos escribiendo a $n = \sum_{i=0}^{N} d_i 2^i = (d_N, \ldots, d_1, d_0)_2$ con $d_i \in \{0, 1\}$ (su desarrollo en base dos).

Luego calculamos recursivamente S^{n_j} donde $n_j = \sum_{i=N-j}^{N} d_i 2^{i-N+j} = (d_N, \ldots, d_{N-j})_2$ y $j = 0, \ldots, N$, de la siguiente manera:

- $S^{n_0} = S^0 = I$ la matriz identidad en $A^{k\times k}$
- $S^{n_{j+1}} = S^{2n_j + d_{N-j-1}} = (S^{n_j})^2 S^{d_{N-j-1}}$ realiza a lo sumo dos multiplicaciones, una al elevar al cuadrado S^{n_j} y otra, quizás, al multiplicar por $S^{d_{N-j-1}}$ que es igual a S ó I dependiendo del valor de $d_{N-j-1} = 1$ ó 0.

Luego, conseguimos $S^n = S^{n_N}$ en $N+1$ pasos, donde $N+1$ es la cantidad de dígitos de n en su desarrollo binario, que tiene orden $log(n)$.

Observación A.0.28 *Este método se puede mejorar teniendo en cuenta que el polinomio característico χ_S de S coincide con $Char_r$, el de la recursión, y ya lo conocemos. Calcular S^n es lo mismo que calcular $R(S)$ si $R \in A[X]$ es el resto de x^n en la división por χ_S (recordemos que como χ_S es mónico, esta división tiene sentido para cualquier A).*

De esta manera, en lugar de guardar las matrices S^{n_j} sólo debemos almacenar $R_j(x) \in A[X]$ el resto de x^{n_j} módulo χ_S, y en lugar de multiplicar las matrices, calculamos el resto módulo χ_S del producto de los restos.

Y al final, para calcular $\widehat{a}_n = S^{n+1-k}\widehat{a}_{k-1}$ teniendo calculado el resto $R = \sum_{i=0}^{k-1} p_i x^i \in A[X]$ de x^{n+1-k} en la división por χ_S, observar que

$$\widehat{a}_n = S^{n+1-k}\widehat{a}_{k-1} = R(S)\widehat{a}_{k-1} = (\sum_{i=0}^{k-1} p_i S^i)\widehat{a}_{k-1} = \sum_{i=0}^{k-1} p_i S^i \widehat{a}_{k-1} = \sum_{i=0}^{k-1} p_i \widehat{a}_{i+k-1}$$

y los vectores $\{\widehat{a}_{i+k-1}\}_{i=0}^{k-1}$ tienen por coordenadas los términos $a_0, \ldots, a_{2k-2}$, que pueden calcularse previamente iterando la recursión $a_{n+k} = \sum_{i=0}^{k-1} r_i a_{n+i}$.

Caracterización de las Sucesiones Recursivas

Supongamos ahora que $A = K$ un cuerpo algebraicamente cerrado y que la factorización de $Char_r$ en $K[X]$ es

$$Char_r(x) = \prod_{i=1}^{m}(x - \lambda_i)^{\nu_i},$$

donde $\{\lambda_i\}$ son las raíces y $\{\nu_i\}$ sus multiplicidades.

De la definición, tenemos que $\mathcal{S}(r) = \ker(Char_r(S))$ donde $Char_r(S) : K^{\mathbb{N}_0} \longrightarrow K^{\mathbb{N}_0}$ se define por $Char_r(S) = S^k - \sum_{i=0}^{k-1} r_i S^i = \prod_{i=1}^{m}(S - \lambda_i I)^{\nu_i}$.

Fijemos $\lambda = \lambda_i$ y $\nu = \nu_i$ para cierto $i \in \{1, \ldots, m\}$. Veamos que para todo $0 \leq j < \nu$, la sucesión $\{n^{(j)}\lambda^n\}_n$ verifica r, es decir, pertenece a $\mathcal{S}(r)$. Basta observar que pertenece al núcleo de $(S - \lambda I)^\nu$. Como

$$\begin{aligned}(S - \lambda I)(n^{(j)}\lambda^n) &= (n+1)^{(j)}\lambda^{n+1} - n^{(j)}\lambda^{n+1} = ((n+1)^{(j)} - n^{(j)})\lambda^{n+1} = \\ &= \lambda(\Delta n^{(j)}\lambda^n) = \lambda j n^{(j-1)}\lambda^n,\end{aligned}$$

de donde

$$(S - \lambda I)(\{n^{(j)}\lambda^n\}_n) = \{\lambda(\Delta n^{(j)})\lambda^n\}_n.$$

Si $j < \nu$ tendremos

$$\begin{aligned}(S - \lambda I)^\nu(\{n^{(j)}\lambda^n\}_n) &= (S - \lambda I)^{\nu-1}(\{\lambda(\Delta n^{(j)})\lambda^n\}_n) \\ &= (S - \lambda I)^{\nu-2}(\{\lambda^2(\Delta^2 n^{(j)})\lambda^n\}_n) \\ &\ldots \\ &= \{\lambda^\nu(\Delta^\nu n^{(j)})\lambda^n\}_n = 0.\end{aligned}$$

Entonces, cualquier sucesión de la forma $\{\lambda^n P(n)\}_n$ con $P \in K[X]$ de grado menor a ν, verifica r. Más generalmente, tenemos la siguiente:

Proposición A.0.29 *$a \in \mathcal{S}(r)$ si y sólo si a es de la forma $\{\sum_{i=1}^{m} \lambda_i^n P_i(n)\}_n$ con cada $P_i \in K[X]$ de grado menor a ν_i.*

Demostración. Si a es combinación lineal de sucesiones que verifican r, a también verifica r. Esto prueba la suficiencia en virtud de la observación anterior.

Veamos la necesidad. Como $\widehat{a}_n = S^{n+1-k}\widehat{a}_{k-1}$ y el polinomio característico de S es precisamente $Char_r$, esta matriz admite una forma de Jordan, donde el tamaño del bloque correspondiente a λ_i será a lo sumo [1] ν_i, por lo que las entradas de S^{n+1-k} serán combinaciones lineales de sucesiones exponenciales en los λ_i multiplicadas por polinomios de grado menor que ν_i (dado que esto pasa para los bloques de Jordan y se mantiene por cambios de base). Entonces $a_n = (\widehat{a}_n)_k$ será de la forma $\{\sum_{i=1}^{m} \lambda_i^n P_i(n)\}_n$ con cada $P_i \in K[X]$ de grado menor a ν_i. Q.E.D.

Observación A.0.30 *En caso de que K no sea algebraicamente cerrado, ésta caracterización sigue valiendo si $Char_r$ se factoriza linealmente.*

Funciones Racionales

Las sucesiones recursivas lineales guardan una estrecha relación con las funciones racionales, que también nos brindan otro punto de vista para abordar la Caracterización de la Proposición A.0.29. En lo que sigue K será simplemente un cuerpo.

Supongamos $f = \frac{P}{Q} \in K(X)$ con $P, Q \in K[X]$, $gr(P) < gr(Q)$ y $Q(0) \neq 0$. Sean $P(x) = \sum_{i=0}^{m} p_i x^i$ y $Q(x) = \sum_{i=0}^{k} q_i x^i$. Supongamos adicionalmente que $q_k = 1$ Llamemos $r \in K^k$ al vector $r = (r_1, \ldots, r_k) = (-q_{k-1}, \ldots, -q_0)$.

Sea $\chi = x^k Q(\frac{1}{x}) = \sum_{i=0}^{k} q_{k-i} x^i$ el polinomio mónico que se obtiene al invertir el orden de los coeficientes de Q.

Está claro que cualquier sucesión que verifique r tendrá como polinomio característico a χ y viceversa.

En $K[[X]]$, f admite un desarrollo en serie de potencias de la forma

$$f(x) = \frac{P(x)}{Q(x)} = \frac{\sum_{i=0}^{m} p_i x^i}{\sum_{i=0}^{k} q_i x^i} = \sum_{i=0}^{\infty} a_i x^i.$$

[1] de hecho será igual

Sea $a = \{a_i\}_i$ la sucesión de los coeficientes. Veamos que es recursiva lineal, más aún, tenemos la siguiente:

Proposición A.0.31 *a verifica r.*

Demostración. Multiplicando por $Q(x)$ obtenemos

$$\sum_{i=0}^{m} p_i x^i = (\sum_{i=0}^{k} q_i x^i) \sum_{j=0}^{\infty} a_j x^j = \sum_{i=0}^{\infty} (\sum_{j=0}^{k} q_j a_{i-j}) x^i$$

considerando $a_i = 0$ para los subíndices negativos.

Como el miembro izquierdo sólo tiene términos de grado menor o igual a m, lo mismo debería pasar con el miembro derecho, en particular, $\forall i \geq k$:

$$\sum_{j=0}^{k} q_j a_{i-j} = 0,$$

es decir, a verifica r. Q.E.D.

Recíprocamente tenemos la siguiente

Proposición A.0.32 *Sean Q y r como antes, y $a \in \mathcal{S}(r)$ entonces $\sum_{i=0}^{\infty} a_i x^i$ representa una función racional con denominador Q y numerador de grado menor a $gr(Q)$.*

Demostración. Basta observar que

$$Q(x) \sum_{i=0}^{\infty} a_i x^i = (\sum_{i=0}^{k} q_i x^i) \sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} (\sum_{j=0}^{k} q_j a_{i-j}) x^i$$

es un polinomio que sólo tiene términos de grado menor que k, llamando P a este polinomio obtenemos $\frac{P}{Q} = \sum_{i=0}^{\infty} a_i x^i$ Q.E.D.

Por lo visto en los parágrafos anteriores, dada $f = \frac{P}{Q} \in K(X)$ podemos calcular de manera recursiva los términos a_n del desarrollo como serie de potencias de $f = \sum_{i=0}^{\infty} a_i x^i$. Una vez calculados los primeros $k = gr(Q)$ términos, podemos obtener a_n en $O(log(n))$ muliplicaciones de matrices cuadradas de lado k.

Otra forma de llegar a la caracterización de las sucesiones recursivas lineales a que verifican r es considerar $\sum_{i=0}^{\infty} a_i x^i$ y escribirla, según las proposiciones anteriores, como

$$f = \frac{P}{Q} = \sum_{i=0}^{\infty} a_i x^i.$$

Descomponiendo a $\frac{P}{Q}$ como suma de fracciones simples y recordando que

$$\frac{1}{(x-\alpha)^\nu} = \frac{(-1)^\nu}{\alpha^\nu (1-\frac{x}{\alpha})^\nu} = (\frac{-1}{\alpha})^\nu \sum_{i=0}^{\infty} \binom{i+\nu-1}{i} \alpha^{-i} x^i.$$

Sólo resta observar que si α es raíz de Q de multiplicidad ν, entonces $\lambda = \alpha^{-1}$ será raíz de $Char(T)$ de la misma multiplicidad, y que al ser f combinación lineal de fracciones simples, a queda combinación lineal de sucesiones de la forma

$$\binom{i+\nu-1}{i} \lambda^i = \frac{1}{(\nu-1)!} (i+\nu-1)^{(\nu-1)} \lambda^i$$

que son exponenciales, multiplicadas por polinomios de grado menor que ν.

Observación A.0.33 *Las sucesiones $\{a_i\}_{i\in\mathbb{N}_0} \subseteq \mathbb{C}$ de período n son recursivas lineales y verifican el vector $(1,0,\ldots,0) \in \mathbb{C}^n$, cuyo polinomio característico es $Char(T) = T^n - 1$. Entonces son combinaciones lineales de exponenciales de raíces $n-$ésimas de la unidad.*

Proposición A.0.34 *Los cuasipolinomios son combinaciones lineales de polinomios multiplicados por exponenciales de raíces de la unidad. Más precisamente, si $f(k)$ es un cuasipolinomio de grado d y período n, satisface una recursividad lineal de polinomio característico $(T^n-1)^{d+1}$.*

Demostración. Sea $f(k) = \sum_{j=0}^{d} p_j(k) k^j$ con las sucesiones $p_j(k)$ de período n. Por la observación anterior las $p_j(k)$ son combinaciones lineales de sucesiones ξ^k con $\xi \in \mathbb{G}_n$. Entonces $p_j(k)k^j$ es un polinomio de grado $\leq d$ multiplicado por una sucesión exponencial de base $\xi \in \mathbb{G}_n$, por lo que satisface una recursividad lineal de polinomio característico $(T^n-1)^{d+1}$. La demostración concluye recordando que las sucesiones que verifican un mismo vector forman un espacio vectorial. Q.E.D.

Recursividad Multilineal

La notación y los resultados de esa sección son de utilidad en la demostración del Teorema 3.1.2.

Hemos caracterizado las sucesiones recursivas lineales como sumas de sucesiones polinomiales, multiplicadas por exponenciales, y vimos alguna manera de calcular sus términos. Veremos ahora cómo se llevan estas ideas al caso de varios parámetros.

Definición A.0.35 *Una* multisucesión de m parámetros *o una* m-sucesión $a \in K^{\mathbb{N}_0^m}$ *es una función de* $\mathbb{N}_0^m$ *en* K.

Notaremos $a_n = a_{n_1,\dots,n_m} = a(n_1,\dots,n_m)$ *si* $n = (n_1,\dots,n_m) \in \mathbb{N}_0^m$.

Definición A.0.36 *Dado* $k = (k_1,\dots,k_m) \in \mathbb{N}_0^m$ *y* m *vectores* $r_1,\dots,r_m$ *donde* $r_i \in K^{k_i}$, *decimos que* a verifica [2] $r = (r^1,\dots,r^m) \in \oplus_{i=1}^m K^{k_i}$ *si* a *es una* $m-$*sucesión tal que para cada* $t = 1,\dots,m$ *y cada elección de subíndices* $\{n_i\}_{1\le i\le m, i\neq t}$, *la sucesión* $b \in K^{\mathbb{N}}$ *dada por* $b_n = a(n_1,\dots,n_{t-1},n,n_{t+1},\dots,n_m)$ *verifica* r^t. *Diremos que tiene* multiorden k *o simplemente* orden k *si* $r_0^t \neq 0 \;\forall\, t = 1,\dots,m$.

Llamamos $\mathcal{S}(r) = \mathcal{S}(r^1,\dots,r^m)$ *al espacio vectorial formado por las multisucesiones que verifican* r.

Observación A.0.37 *Consideremos* m *sucesiones* $a^1 = \{a_i^1\}_{i\in\mathbb{N}_0},\dots,a^m = \{a_i^m\}_{i\in\mathbb{N}_0}$ *que verifican* $r^1,\dots,r^m$ *respectivamente, es decir,* $a^i \in \mathcal{S}(r^i)$. *Tomando a como la* $m-$*sucesión* producto *definida por* $a_n = a_{n_1,\dots,n_m} = a_{n_1}^1 a_{n_2}^2 \dots a_{n_m}^m$ *obtenemos una que verifica* r. *La siguiente proposición muestra que éstas son esencialmente todas las que hay.*

Proposición A.0.38 *Con la notación anterior,* $\dim_K(\mathcal{S}(r)) = k_1k_2\dots k_m$ *y* $\mathcal{S}(r)$ *está generado por productos de sucesiones* $a^i \in \mathcal{S}(r^i)$

Demostración. Está claro que una $m-$sucesión $a \in \mathcal{S}(r)$ está determinada por sus términos $a_{n_1,\dots,n_m}$ con $n_i < k_i$.

[2] en este parágrafo, r representa un vector de m entradas, siendo cada una de ellas vectores de tamaños k_i

Para cada multiíndice $(n_1, \ldots, n_m) < (k_1, \ldots, k_m)$ consideramos la $m-$sucesión $e^{n_1,\ldots,n_m}$ en $\mathcal{S}(r)$ definida por $(e^{n_1,\ldots,n_m})_{j_1,\ldots,j_m} = \delta^{n_1,\ldots,n_m}_{j_1,\ldots,j_m}$ para los subíndices $(j_1, \ldots, j_m) < (k_1, \ldots, k_m)$.

Evidentemente $\{e^{n_1,\ldots,n_m}\}_{(n_1,\ldots,n_m)<k}$ forma una base para $\mathcal{S}(r)$, por lo que $\dim_K(\mathcal{S}(r)) = k_1 k_2 \ldots k_m$. Teniendo en cuenta que cada elemento $e^{n_1,\ldots,n_m}$ de esta base es el producto de las sucesiones $e(i)^{n_i}$ de las bases canónicas $\{e(i)^0, \ldots, e(i)^{k_i-1}\}$ de los $\mathcal{S}(r^i)$ llegamos a que $\mathcal{S}(r)$ está generado por productos de sucesiones en los $\mathcal{S}(r^i)$. Q.E.D.

Observación A.0.39 *Dada la relación de recurrencia r y los términos $a_{j_1,\ldots,j_m}$ que corresponden a $(j_1, \ldots, j_m) < (k_1, \ldots, k_m)$, podemos calcular inductivamente el término $a_{n_1,\ldots,n_m}$ si sabemos hacerlo para sucesiones de un parámetro (elevando matrices, por ejemplo), calculando los términos $a_{n_1,\ldots,n_{m-1},1}, a_{n_1,\ldots,n_{m-1},2}, \ldots, a_{n_1,\ldots,n_{m-1},k_m}$, y luego $a_{n_1,\ldots,n_{m-1},n_m}$, teniendo en cuenta que la sucesión $\{a_{n_1,\ldots,n_{m-1},i}\}_{i\in\mathbb{N}_0} \in \mathcal{S}(r^m)$ y para cada i, las multisucesiones $\{a_{n_1,\ldots,n_{m-1},i}\}_{n_1,\ldots,n_{m-1}\in\mathbb{N}_0^{m-1}} \in \mathcal{S}(r^1, r^2, \ldots, r^{m-1})$.*

Observación A.0.40 *Si para cada $i = 1, \ldots, m$ tenemos que las sucesiones de $\mathcal{S}(r^i)$ pueden escribirse como combinaciones lineales de polinomios multiplicados por exponenciales, entonces las multisucesiones de $\mathcal{S}(r)$ podrán escribirse como combinaciones lineales de polinomios en varias variables, multiplicados por exponenciales.*

Observación A.0.41 *Como en el caso de un parámetro, si una multisucesión es combinación lineal de polinomios multiplicados por exponenciales, también satisface cierto r. Alcanza verlo para monomios multiplicados por exponenciales, pero este caso es justamente producto de sucesiones recursivas lineales, en virtud de la Prop. A.0.29.*

Apéndice B

Complejidad Algorítmica

Sean f y g funciones a valores en $\mathbb{R}$. Decimos que una función f tiene *orden* g, y notamos $f = O(g)$, si existe una constante $k \in \mathbb{R}$ tal que $|f| \leq k|g|$.

Si f está definida en algún subconjunto de $\mathbb{R}^d$ (por ejemplo, los puntos con coordenadas enteras, o naturales, o con las primeras $d-1$ iguales a cero) diremos que tiene orden *polinomial* si es de orden g, para cierto $g \in \mathbb{R}[x_1, \ldots, x_d]$, y que tiene orden *exponencial* si puede tomarse g como suma de exponenciales de bases mayores a 1.

La *complejidad* $f(N)$ de un algortimo es el número de pasos que realiza para una cierta entrada de tamaño N, y si f es de orden g se dice que el algoritmo tiene *orden* $g(N)$.

A menudo, al hablar de algoritmos y sus órdenes uno se topa con la frase "éste es un problema NP-completo", que suele venir acompañada de algún algoritmo de orden malo [1], o de alguna restricción al problema original, que lo simplifica considerablemente.

Saber que un problema es NP-completo no lo resuleve, pero ayuda a buscar alternativas, subproblemas menos ambiciosos.

Los siguientes son ejemplos clásicos de problemas de esta clase:

El *problema del viajante de comercio*: Dada una lista de ciudades, caminos entre ellas y costo de los mismos, se pretende pasar por todas minimizando el costo.

[1] exponencial o peor.

SATISFIABILITY o simpemente SAT: Dado un conjunto U de variables booleanas, y una lista C de disyunciones sobre las variables de U, se pregunta si se puede o no asignar valores de verdad (V o F) a las variables, de manera de satisfacer todas las disyunciones.

Subproblemas de SAT son los llamados N-SAT (por ejemplo, 2-SAT o 3-SAT), donde cada disyunción de C involucra un número de variables acotado por N.

El SAT es un *problema de decisión* pues la respuesta esperada es o bien un "si" o un "no". El problema del viajante de comercio puede tranformarse en uno de decisión, agregando a los datos una cota K y preguntando si existe un recorrido de costo total menor o igual a K.

En el marco teórico que trata estos temas, no se habla de problemas sino de *lenguajes* y *esquemas de codificación*, y no se habla de computadoras sino de *máquinas de Turing*.

Un *lenguaje* es un conjunto de *palabras* en un alfabeto Σ, es decir, sucesiones finitas de elementos de Σ. Por *esquema de codificación* se entiende la manera en que se interpretan las palabras como instancias de un cierto problema Π, y el lenguaje asociado a dicho problema está formado por aquellas palabras que corresponden a instancias de Π que dan "sí" como respuesta.

Existen modelos más complejos de máquinas determinísticas, pero con este ejemplo alcanzará para ilustrar la idea.

Una *máquina de Turin determinística*, o MTD, es un modelo formal de lo que entendemos por computadora, compuesto por una una "cinta", un cabezal lector/escritor, y un controlador de finitos estados. Un programa para dicha máquina consiste en:

- un conjunto finito Γ de símbolos, que contiene al alfabeto Σ.
- un conjunto finito Q de estados posibles, con tres estados distinguidos q_0, q_Y y q_N correspondientes al estado de inicio, y a los de finalización con respuesta afirmativa y negativa, respectivamente.
- una función de transición $\delta : (Q \setminus \{q_Y, q_N\}) \times \Gamma \longrightarrow Q \times \Gamma \times \{1, -1\}$.

En cada paso, la función δ lee el estado q y el dato g de la cinta, y la respuesta $\delta(q, g) =$

(q', g', ϵ) cambia el estado a q', escribe en la cinta g' (borrando a g) y mueve la cinta un lugar a la derecha o a la izquierda, según $\epsilon = 1$ o $\epsilon = -1$.

En caso de llegar al estado q_Y o q_N el programa termina y devuelve la respuesta afirmativa o negativa, respectivamente.

El *número de pasos* o *tiempo* de un programa, corresponde a la cantidad de veces que se utiliza la función δ.

La *máquina de Turing no determinística*, o MTND, es básicamente lo mismo, sólo que antes de comenzar, escribe una solución tentativa en la cinta, y al ejecutarse procesa la entrada junto con la presunta solución. En otras palabras, trata de adivinar una solución y luego verificarla.

Nosotros hablaremos simplemente de problemas. Resolver un problema Π es dar una MTD que contesta correctamente cierta codificación de Π, y verificarlo será dar una MTND que para cierta solución tentativa, lo resuelve.

La clase de problemas P, es la formada por problemas de decisión que pueden resolverse algorítmicamente en un número de pasos que es polinomial en el tamaño de la entrada.

La clase NP se define como aquellos problemas de decisión cuya respuesta afirmativa puede verificarse (es decir, con una MTND) en un número de pasos de orden polinomial.

Por ejemplo, el problema del viajante de comercio es NP, ya que una respuesta afirmativa puede verificarse en tiempo polinomial (dado un recorrido, sólo resta chequear que el costo sea menor que lo pedido, y que efectivamente es un recorrido). El SAT también es NP, puesto que con dar una asignación a cada variable, sólo resta chequear si se satisfacen todas las disyunciones. Es sabido que el 2-SAT está en P.

El problema de Programación Linear Entera (PLE), que consiste en decidir si un polítopo racional $Q = \{Ax \leq b\} \subseteq \mathbb{R}^d$ contiene o no puntos de $\mathbb{Z}^d$, es un problema NP. Alcanza con dar un punto de coordenadas enteras y chequear todas las desigualdades que definen a Q.

Claramente $P \subseteq NP$, pero no se sabe si la inclusión es estricta, aunque se conjetura que sí. Éste es uno de los problemas abiertos más importantes de la actualidad (ver

http://www.claymath.org/millennium/).

Dados dos problemas Π_1 y Π_2 decimos que Π_1 es una *reducción polinomial* de Π_2, y lo notamos $\Pi_1 \leq_p \Pi_2$ si podemos transformar toda instancia de Π_1 en alguna de Π_2, con un número de pasos polinomial en el tamaño, de manera que se mantenga el valor de la respuesta. En otras palabras, podemos resolver Π_1 si podemos resolver Π_2.

Podemos ver que 3-SAT $\leq_p$ SAT (puesto que es un subproblema) y que SAT $\leq_p$ 3-SAT (agregando variables para partir cada disyunción en otras que involucren 3 o menos).

La clase NP-hard consiste en los problemas Π tales que todo problema $\Pi' \in NP$ se reduce a Π. Es decir, el problema $\Pi \in NP$-hard es "más difícil" que todos los problemas de NP. Por último, un problema se dice que es NP-completo, si es NP y NP-hard.

Si un sólo problema NP-completo resultase estar también en P, cualquier problema de la clase NP podría reducirse a él, y por lo tanto resolverse en tiempo polinomial, lo que nos daría $P = NP$.

En la búsqueda de un algoritmo para resolver cierto problema Π, descubrir que es NP-completo no lo resuelve, pero nos hace pensar si el problema está mal planteado, y deberíamos buscar algún resultado menos ambicioso.

En el año 1971, S.A. Cook demuestra (ver [17]) que SAT (equivalentemente 3-SAT) es NP-completo, dando origen a toda esta teoría.

Proposición B.0.42 *El problema de Programación Linear Entera es NP-completo.*

Demostración. Veamos que SAT $\leq_p$ PLE.

Tomemos una instancia de SAT, dada por un conjunto $U = \{u_1, \ldots, u_d\}$ de variables booleanas y una colección de disyunciones $C = \{c_1, \ldots, c_n\}$.

A cada variable u_i le asociamos una coordenada x_i.

Para cada disyunción $c_j = u'_{j1} \vee \ldots \vee u'_{jk_j}$ consideramos la función $\widehat{c}_j(x)$ que se calcula sumando x_i o $1 - x_i$ según u_i o $\neg u_i$ sea uno de los u'_{jl}, . Por ejmplo, si $c = u_1 \vee \neg u_2 \vee u_4$, tenemos $\widehat{c}(x) = x_1 + 1 - x_2 + x_4$.

Consideramos en $\mathbb{R}^d$ el polítopo definido por

$$Q = \{x \in \mathbb{R}^d / \ 0 \leq x_i \leq 1,\ \widehat{c}_j(x) \geq 1,\ i = 1, \ldots, d,\ j = 1, \ldots, n\}.$$

Cualquier punto con coordenadas enteras de Q deberá estar en $\{0,1\}^d$ por las primeras desigualdades, y asignando V a aquellas u_i que correspondan a $x_i = 1$ y F a las otras, obtendremos una asignación booleana que satisface las disyunciones de C.

Como esta construcción se puede hacer en un número polinomial de pasos, tendremos resuelto el SAT, que es NP-completo. Q.E.D.

Es de esperar entonces, que los algoritmos para resolver problemas de PLE tengan órdenes de complejidad malos.

Tiene sentido plantearse algún subproblema algo más tratable. Por ejemplo, fijar la dimensión $d \in \mathbb{N}$ y mirar el mismo problema de PLE.

Para estos casos, Barvinok y Woods demostraron (ver [4]) que cuando la dimensión se considera fija, el problema restringido de PLE se puede resolver en tiempo polinomial.

Apéndice C

Algoritmo LLL

En el algoritmo de Barvinok (Capítulo 4) necesitamos hallar un vector no nulo relativamente "corto" dentro de un lattice Λ dado. El siguiente algoritmo ofrece una manera eficiente de hacerlo. Se conoce como la reducción Lenstra-Lenstra-Lovász, o siplemente la reducción LLL (ver [33]).

Definición C.0.43 *Sea $\Lambda \subseteq \mathbb{R}^d$ un lattice y $u_1, \ldots, u_d$ una base de Λ. Sean los subespacios $L_k = \langle u_1, \ldots, u_k \rangle_{\mathbb{R}}$ con $k = 1, \ldots, d$ y $L_0 = \{0\}$. Sea $L_k^{\perp}$ el complemento ortogonal de L_k y w_k la proyección ortogonal* [1] *de u_k sobre $L_{k-1}^{\perp}$. Observemos que $\|w_k\| = d(u_k, L_{k-1})\ \forall\ k = 1, \ldots, d$. Escribiendo $u_k = w_k + \sum_{i=1}^{k-1} \alpha_{ki} w_i$ diremos que la base $u_1, \ldots, u_d$ es* reducida *si se cumplen:*

- $|\alpha_{ki}| \leq \frac{1}{2}\ \forall\ 1 \leq i < k \leq d$
- $d(u_k, L_{k-1})^2 \leq \tau d(u_{k+1}, L_{k-1})^2\ \forall\ 1 \leq k \leq d-1$

donde τ lo tomaremos igual a $\frac{4}{3}$ pero para la mayoría de las aplicaciones alcanza con pedir $1 < \tau < 4$.

[1] $\{w_k\}_{k=1,\ldots,d}$ es la ortogonalización de Gram-Schmidt de $\{u_k\}_{k=1,\ldots,d}$, sin normalizar

Teorema C.0.44 *Sea $\lambda \subseteq \mathbb{R}^d$ un lattice y $u_1, \ldots, u_d$ una base reducida. Entonces*[2]

$$\|u_1\| \leq 2^{\frac{d-1}{2}} \|v\| \; \forall \, v \in \lambda \setminus \{0\}.$$

Demostración. Observemos que $d(u_{k+1}, L_{k-1}) = \|w_{k+1} + \alpha_{k+1,k} w_k\|^2$.

De las desigualdades de la base reducida tenemos que:

$$\|w_k\|^2 = d(u_k, L_{k-1})^2 \leq \tau d(u_{k+1}, L_{k-1})^2 = \tau(\|w_{k+1}\|^2 + \alpha_{k+1,k}^2 \|w_k\|^2) \leq \tau \|w_{k+1}\|^2 + \frac{\tau}{4}\|w_k\|^2,$$

entonces

$$\|w_{k+1}\|^2 \geq \frac{1}{\tau}(1 - \frac{\tau}{4})\|w_k\|^2 = \frac{1}{2}\|w_k\|^2,$$

de donde

$$\|w_k\|^2 \geq \frac{1}{2}\|w_{k-1}\|^2 \geq (\frac{1}{2})^2 \|w_{k-2}\|^2 \geq (\frac{1}{2})^3 \|w_{k-3}\|^2 \geq \ldots \geq (\frac{1}{2})^{k-1} \|w_1\|^2,$$

que implica

$$d(u_k, L_{k-1}) = \|w_k\| \geq 2^{\frac{1-d}{2}} \|w_1\| = 2^{\frac{1-d}{2}} \|u_1\|.$$

Ahora, si $v \in \Lambda \setminus \{0\}$, podemos escribirlo como $v = \sum_{i=1}^{k} n_i u_i$ donde $n_i \in \mathbb{Z}$ y n_k no nulo. Entonces

$$\|v\| = \|\sum_{i=1}^{k} n_i u_i\| = |n_k| \|u_k + \sum_{i=1}^{k-1} \frac{n_i}{n_k} u_i\| \geq \|u_k + \sum_{i=1}^{k-1} \frac{n_i}{n_k} u_i\| \geq d(u_k, L_{k-1}) \geq 2^{\frac{1-d}{2}} \|u_1\|,$$

es decir $\|u_1\| \leq 2^{\frac{d-1}{2}} \|v\|$. Q.E.D.

Veamos cómo construir una base reducida:

Suponemos Λ dado por una base $u_1, \ldots, u_d$. El algoritmo consiste en iterar dos subrutinas. En ambas, la entrada y la salida son bases de Λ que por comodidad llamaremos $u_1, \ldots, u_d$ y $v_1, \ldots, v_d$ respectivamente.

1er subrutina Dada $u_1, \ldots, u_d$ calculamos $w_1, \ldots, w_d$ su ortogonalización de Gram-Schmidt y escribimos cada u_k como $\sum_{i=1}^{k} \alpha_{ki} w_i$. Si todos los coeficientes $|\alpha_{ki}| \leq \frac{1}{2}$, pasamos a la segunda subrutina. Si no, consideramos $|\alpha_{ki}| > \frac{1}{2}$ con i máximo. Devolvemos la base

[2] a esto nos referimos con decir que u_1 es relativamente "corto"

$v_1, \ldots, v_d$ definida por $v_j = u_j \ \forall\ j \neq k$ y $v_k = u_k - [\alpha_{ki}]u_i$, donde $[x] = \lfloor x + \frac{1}{2} \rfloor$ es[3] el entero más cercano a x (redondeando para arriba). Los subespacios $L_j = \langle u_1, \ldots, u_j \rangle$ no se modifican, ni la base $w_1, \ldots, w_d$. Escribiendo $v_1, \ldots, v_d$ en la base ortogonal tendremos las mismas coordenadas α salvo para el vector v_k cuya i-ésima coordenada es ahora menor o igual a $\frac{1}{2}$, las primeras $i-1$ coordenadas pueden haber cambiado y las últimas $k-i$ coordenadas siguen siendo α_{kj} con $i < j \leq k$.

Repitiendo este proceso a lo sumo $\frac{d(d-1)}{2}$ veces obtenemos una base de Λ que cumple con la primera de las condiciones de base reducida.

2da subrutina Es fácil chequear si se cumple la segunda condición, teniendo la escritura de $u_1, \ldots, u_d$ en la base ortogonal $w_1, \ldots, w_d$. En caso de satisfacerse todas las desigualdades, ya tenemos una base reducida y el algoritmo termina. Si tuviésemos $d(u_k, L_{k-1})^2 > \tau d(u_{k+1}, L_{k-1})^2$ para cierto k, intercambiamos u_k y u_{k+1} devolviendo $v_i = u_i \ \forall i \neq k, k+1$, $v_k = u_{k+1}$ y $v_{k+1} = u_k$. Y regresamos a la primer subrutina.

Veremos a continuación que el algoritmo termina en un tiempo polinomial.

Observación C.0.45 *Sea $u_1, \ldots, u_d$ una base de $\Lambda \subseteq \mathbb{R}^d$, y $w_1, \ldots, w_d$ su ortogonalización. Viendo a $\Lambda_k = \Lambda \cap L_k$ como sublattice de L_k tenemos que $det\Lambda_k = \prod_{i=1}^{k} \|w_i\|$, pues ambos miembros representan al volumen del paralelepípedo determinado por $u_1, \ldots, u_k$, relativo a L_k (puede tomarse esto como definición de $det\Lambda_k$, ver [5]).*

Por otro lado, si $\lambda = \min_{v \in \Lambda \setminus \{0\}} \|v\|$, el cubo abierto centrado en el origen de lado $\frac{2\lambda}{\sqrt{d}}$ es convexo, simétrico y no contiene elementos no nulos de Λ por lo que, en virtud del teorema de Minkowski ([5], pg. 294), su volumen debe ser menor o igual a 2^d veces el del paralelepípedo fundamental de Λ, es decir

$$2^d det\Lambda \geq \left(\frac{2\lambda}{\sqrt{d}}\right)^d \Rightarrow det\Lambda \geq \left(\frac{\lambda}{\sqrt{d}}\right)^d.$$

Similarmente $det\Lambda_k \geq \left(\frac{\lambda}{\sqrt{k}}\right)^k \ \forall\ k = 1, \ldots, d.$

[3] $\lfloor x \rfloor = \max\{n \in \mathbb{Z} / n \leq x\}$ es la parte entera de x

Teorema C.0.46 *Sea* $D(u_1, \ldots, u_d) = \prod_{k=1}^{d-1} det\Lambda_k$. *Si* $m \in \mathbb{N}$ *es tal que*

$$\tau^{-\frac{m}{2}} D(u_1, \ldots, u_d) < \lambda^{\frac{d(d-1)}{2}} \prod_{k=1}^{d-1} k^{-\frac{k}{2}},$$

el algoritmo LLL realiza a lo sumo $m+1$ *veces la segunda subrutina.*

Corolario C.0.47 *Todo lattice tiene una base reducida.*

Demostración. (del teorema) Al cambiar la base de Λ no se modifica el miembro derecho de la desigualdad, pero el izquierdo puede verse modificado, ya que los subespacios L_k (y por lo tanto Λ_k y $det\Lambda_k$ también) están generados por los primeros vectores.

La primer subrutina no modifica los subespacios L_k.

En la segunda subrutina, si intercambiamos u_k con u_{k+1} se modifica sólo L_k. Veamos cómo acotar el nuevo $det\Lambda_k = \prod_{i=1}^{k} \|w_i\|$.

Como $\|w_k\| = d(u_k, L_{k-1}) > \tau^{\frac{1}{2}} d(u_{k+1}, L_{k-1})$, la norma del nuevo w_k será menor o igual a $\tau^{-\frac{1}{2}}$ por la anterior. Entonces

$$D(v_1, \ldots, v_d) \leq D(u_1, \ldots, u_d)\tau^{-\frac{1}{2}}.$$

Por la observación anterior tenemos que

$$D(u_1, \ldots, u_d) = \prod_{k=1}^{d-1} det\Lambda_k \geq \prod_{k=1}^{d-1} \left(\frac{\lambda}{\sqrt{k}}\right)^k \geq \lambda^{\frac{d(d-1)}{2}} \prod_{k=1}^{d-1} k^{-\frac{k}{2}}$$

cualquiera sea la base $u_1, \ldots, u_d$. Entonces el algoritmo LLL no puede usar más de $m+1$ veces la segunda subrutina, por la elección de m. Q.E.D.

Bibliografía

[1] M. Agfalvi, I. Kadar and E. Papp: *Generalization of Pick's Theorem for Surface of Polyhedra*, APL99 On Track To The 21st Century Volume 29 Number 2.

[2] Baldoni-Silva y Vergne: *Residues formulae for volumes and Ehrhart polynomials of convex polytopes.* (math.ArXiv, CO/010397).

[3] Baldoni-Silva, De Loera y Vergne: *Counting Integer Flows in Networks* (arXiv:math.CO/0303228 v1 19 Mar 2003).

[4] Barvinok, A.: *A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed* Math. Oper. Res. 19 (1994),769-779.

[5] Barvinok, A.: *A Course in Convexity, Graduate Studies in Mathematics*, AMS (2002).

[6] Barvinok, A.: *Computing the Volume, Counting Integral Points, and Exponential Sums*, Discrete & Computational Geometry, 10 (1993), N 2 123-141.

[7] Barvinok, A. - Pommersheim, J.: *An algorithmic theory of lattice points in polyhedra*, in: New perspective in algebraic combinatorics, Math. Sci. Res. Inst. Publ., vol.38, Cambridge University Press, Cambridge, 1999, 91-147.

[8] Barvinok,A. - Woods, K.: *Short rational generating functions for lattice point problems*, J. Amer. Math. Soc. 16 (2003), N. 4, 957-979.

[9] Beck, M. : *The Partial Fraction Method for Counting Solutions to Integral Linear System*, (arxiv:math.co/0309332 v2 25 May 2004).

[10] Beck, De Loera, Develin, Pfeinfle y Stanley, *Coefficients and Roots of Ehrhart Poynomials* (arxiv:math.co/0402148 v1 9 Feb 2004).

[11] Beck, M. y Robins, S.: *Computing the Continuous Discretely*, Springer (por aparecer http://math.sfsu.edu/beck/ccd.html).

[12] Beck, M. y Sottile, F. : *Irrational proofs for three Theorems of Stanley* (arXiv:math.CO/0501359 v3 21 Mar 2005).

[13] Braun, Benjamin : *Norm Bounds for Ehrhart Polynomial Roots*, (arXiv:math.CO/0602464 v1 21 Feb 2006).

[14] Brion,M.: *Points entiers dans les polyèdres convexes*, Ann. Sci. Ècole Norm. Sup. (4), 21(4):653-663,1988.

[15] Brion,M. - Vergne,M.: *Residue formulae, vector partition functions and lattice points in rational polytopes*, J. Amer. Math. Soc. 10 (1997) N.4, 797-833.

[16] Brion,M. - Vergne,M.: *Lattice points in simple polytopes*, J. Amer. Math. Soc. 10 N.2 (1997), 371-392.

[17] Cook, Stephen (1971): *The Complexity of Theorem Proving Procedures*, Proceedings of the third annual ACM symposium on Theory of computing, 151158.

[18] J. de Loera, D. Haws, R. Hemmecke, P. Huggins, B. Sturmfels, R. Yoshida: *Short rational functions for toric algebra and applications*, J. Symb. Comput. 38 (2004), N.2, 959-974.

[19] J. De Loera., D. Haws, R. Hemmecke, P. Huggins, J. Tauzer, R. Yoshida: *A User's Guide for LattE v1.1*, 2003 (http://www.math.ucdavis.edu/latte/).

[20] J. De Loera., R. Hemmecke, J. Tauzer y R. Yoshida: *Effective Lattice Point Counting in Rational Convex Polytopes*, March 10, 2003 (http://www.math.ucdavis.edu/ ramon/articles/LattE.ps).

[21] Diaz, R. y Robins, S: *The Ehrhart polynomial of a lattice poltytope*, Annals of Mathematics, 145 1997, 503-518.

[22] Dyer, M y Kannan, R. : *On Barvinok's algorithm for counting lattice points in fixed dimension*, Math of Op. Res. 22 (1997) 545-549.

[23] E. Ehrhart: *Sur les polyèdres rationnels homotetiques à n dimensions*, C.R. Acad. Sci. Paris, 254 (1962), 616-618.

[24] Ewald, G.: *Combinatorial Convexity and Algebraic Geometry*, Graduate Texts in Mathematics, Springer.

[25] Forsberg, M.- Passare, M. - August Tsikh : *Laurent Determinants and Arrangements of Hyperplane Amoebas*, Advances in Mathematics 151, 45 70 2000.

[26] M. R. Garey, D. S. Johnson: *Computers and Intractability : A Guide to the Theory of NP-Completeness* (Series of Books in the Mathematical Sciences).

[27] Gelfand, I. - Kapranov, M. - Zelevinsky, A.: *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser, Boston, 1994.

[28] Grünbaum, Blanko: *Convex polytopes*,vol. 221 of Graduate Text in Mathematics. Springer-Verlag, New York, second edition, 2003.

[29] R. Kannan: *Solutions of the Frobenius Problem and its Generalization*, Nov 27, 1989 (http://www.cs.cmu.edu/afs/cs.cmu.edu/user/kannan/public/www/Papers/frobenius.ps.Z).

[30] Karshon, Stemberg y Weistman: *Exact Euler Maclaurin Formulas for Simple Lattice Polytopes*, (arxiv:math.co/0507572 v1 27 Jul 2005).

[31] Knopp, K.: *Theory and application of infinite series*, Blackie and Son Limited, London and Glasgow (1928).

[32] J. Lasserre : *Generating functions and duality for integer programs*, Rapp. LAAS N02402, 2003.

[33] Lenstra, Lenstra y Lovász: *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), 515-534.

[34] Miller, E. - Sturmfels, B: *Combinatorial Commutative Algebra*, por aparecer, Springer Verlag, 2004. Disponible en: http://www.math.umn.edu/∼ezra.

[35] Reeve, J. E.: *On the volume of a Lattice Polyhedra*, Proc. London Math. Soc. (3) 7 1957.

[36] Reeve, J. E.: *A further note on the volume of Lattice Polyhedra*, Journal of London Math. Soc. 34 (1959), 57-62.

[37] Schrijver A.: *Theory of Linear and Integer Programming*, Wiley series in Discrete Mathematics and Optimization, 1982.

[38] Stanley, Richard P.: *Combinatorics and Commutative Algebra*, Progress in Mathematics, Birkhäuser, Boston, 1996.

[39] Sturmfels, B.: *On vector parttion functions*, J. Combin. Theory Ser. A 72 (1995), no. 2, 302-309.

[40] Ziegler, Günter M.: *Lectures on polytopes*, Graduate Texts in Mathematics, 152, Springer-Verlag, New York, 1995.