CUADRADOS MÁGICOS E IDEALES TÓRICOS

MARÍA ANGÉLICA CUETO

1. Definiciones y conceptos básicos

En el presente texto trataremos de caracterizar los cuadrados mágicos y su relación con los ideales tóricos, como bien presagia el título. Antes de empezar con la explicación de este vínculo, al principio no claro, necesitamos fijar definiciones y un poco de notación.

Definición 1. *Un* cuadrado mágico *de tamaño n y suma s es una matriz m de $n \times n$ con coeficientes enteros positivos, cuyas filas y columnas suman s cada una (o sea, cada fila y columna tiene norma uno igual a s).*

Existen otras condiciones que podríamos pedir. Una es que las diagonales de la matriz también sumen s, o por ejemplo que cada entero entre 1 y n^2 aparezca una y sólo una vez como coeficientes de M, pero no consideraremos estas restricciones, para simplificar un poco el problema. Antes de continuar, veamos un ejemplo de 3×3 y otro de 4×4, de larga data (*Melancholia* de Albrecht Dürer).

$$\begin{pmatrix} 4 & 3 & 8 \\ 9 & 5 & 1 \\ 2 & 7 & 6 \end{pmatrix} \quad ; \quad \begin{pmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 8 \\ 4 & 15 & 14 & 1 \end{pmatrix} .$$

En el primer caso, las filas, columnas y diagonales suman 15; además, cada uno de los números entre 1 y 9 aparece en la matriz. En el segundo, la suma es 24.

Definición 2. *Sea $\mathcal{C}M_n$ el conjunto de cuadrados mágicos, y $\mathcal{C}M_n(s)$ los cuadrados mágicos que suman s. Definimos $M_n(s) := \#(\mathcal{C}M_n(s))$ (o sea, el número de cuadrados mágicos de tamaño n y suma s).*

Nuestro objetivo consistirá en calcular $M_n(s)$, fijados n y s.

Lema 1. *Los cuadrados mágicos de tamaño n forman un monoide asociativo respecto de la suma (esto es, $\mathcal{C}M_n$ es cerrado por sumas y esta operación es asociativa).*

Demostración: Basta ver que la suma de dos cuadrados mágicos es mágico, y esto es claro porque la suma de matrices es lugar a lugar. Como la suma de matrices es asociativa, estamos hechos. ■

Para facilitar la construcción del espacio $\mathcal{C}M_n$, necesitamos encontrar un buen sistema de generadores.

Observación 1. *Miremos como ejemplo una matriz de permutación de tamaño n, esto es, una matriz $P := P_\sigma$, donde $\sigma \in \mathbb{S}_n$ y*

$$P_{i,j} = \begin{cases} 1 & \text{si } j = \sigma(i) \\ 0 & \text{si no} \end{cases} .$$

Claramente las filas y columnas suman 1. Luego, tenemos que toda mariz de permutación es un cuadrado mágico, de suma 1. Más aún, estas matrices son todos los cuadrados mágicos de suma 1, ya que por la condición sobre la suma, cada fila y columna tiene exactamente un coeficiente 1 y el resto ceros. Es muy sencillo ver

que,siendo M mágico de suma 1, $\sigma(i) = j$ si $M_{i,j} = 1$, da una buena definición de $\sigma \in \mathbb{S}_n$, y que hace $M = P_\sigma$.

Hay otra propiedad que cumplen las matrices de permutación:

Proposición 1. *Las matrices de permutación son un sistema de generadores del semigrupo $\mathcal{C}M_n$. Más aún, todo cuadrado mágico de suma s está generado por exactamente s permutaciones (no necesariamente distintas).*

Demostración: Procederemos por inducción en k = número de coeficientes no nulos de un cuadrado mágico.

- Caso $k = 1$: es claro.
- Paso inductivo: Sea $k > 1$ y M un cuadrado mágico, y supongamos que vale para todo $r < k$. Buscamos entre los k coeficientes no nulos alguna elección de fila y columnas, de manera de formar una matriz de permutación: es decir buscamos n entradas no nulas de M, una por cada fila y columna. El Teorema de Hall nos dará lo que necesitamos (ver Lema 2).
  Supongamos que tal elección de n elementos existe, y sean $d > 0$ el menor elementos entre estos n coeficientes elegidos, y P la matriz de permutación que tiene unos en cada uno de los lugares correspondientes. Entonces $M - d * P$ es mágico y tiene al menos una entrada nula más, y es un cuadrado mágico de suma $s - d$. Por lo tanto, por hipótesis inductiva, tenemos el resultado deseado. ■

Teorema 1. *(Hall) Sean I_1, I_2 dos conjuntos de cardinal n, y $S \subseteq I_1 \times I_2$. Para cada $i \in I_1$ consideremos $S_i = \{j \in I_2 \text{ tal que } (i,j) \in S\}$. Entonces, existen n elementos distintos $s_i \in S_i$ $i = 1, \dots, n$ si y sólo si $\forall J \subseteq I_2$ se tiene*

$$\#(\bigcup_{i \in J} S_i) \geq \#J \ .$$

Lema 2. *Los cuadrados mágicos complen las condiciones de Hall.*

Demostración: Tomemos $M = (m_{ij})_{i,j} \in \mathcal{C}M_n(s)$, $I_1 = I_2 = \{1, \dots, n\}$ y sea $S := \{(i,j) \ tq \ m_{ij} \neq 0\}$. Para ver las condiciones de Hall basta probar que vale para $J = \{1, \dots, r\}$ con $r \leq n$, ya que los cuadrados mágicos son invariantes por permutación de filas y/o columnas. Sea entonces

$$A := \begin{pmatrix} m_{11} & \dots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \dots & m_{rn} \end{pmatrix}$$

dicha submatriz asociada a J. Sabemos que la suma de cada fila de A es s y que cada columna suma a lo sumo s. Si sumamos todos los coeficientes de la matriz A obtenemos $r * s$, porque estamos sumando r filas que suman s. Los coeficientes positivos de A deben pertenecer a columnas indexadas por $\bigcup_{i=1}^{r} S_i$. Ahora bien, si sumamos los coeficientes positivos a_{ij} con $j \in \bigcup S_i$ obtenemos $r * s$ y al mismo tiempo sabemos que no puede exceder $s * \#\big(\bigcup_{i=1}^{r} S_i\big)$, ya que las columnas de M suman a lo sumo s cada una. Luego $r * s \leq s * \#(\bigcup_{i=1}^{r} S_i)$, o lo que es lo mismo $\#(\bigcup_{i=1}^{r} S_i) \geq r$, como queríamos probar. ■

Observación 2. *Es importante señalar, y será nuestra herramienta principal, que las matrices de permutación no son linealmente independientes sobre $\mathbb{Q}$. Esto es claro si $n \geq 4$, porque las matrices de tamaño $n \times n$ tienen dimensión n^2 sobre $\mathbb{Q}$ y $n! > n^2$ si $n \geq 4$. Pero más aún, son l.d. sobre $\mathbb{Z}$ para cualquier $n \geq 3$, y esta condición es la que vamos a explotar.*

Para una demostración, ver ecuación (7) y posterior desarrollo en Sección 2.

Ejemplo 1. *Calculemos $M_n(s)$ para algunos valores pequeños de s o n. Por ejemplo, por Observación 1 sabemos que $M_n(1) = \#(\text{matrices de permutación}) = \#\mathbb{S}_n = n!$.*
Por otra parte, es claro que $M_1(s) = 1$, mientras que $M_2(s) = s + 1$, ya que los elementos de $\mathcal{C}M_2(s)$ son

$$\begin{pmatrix} a & s-a \\ s-a & a \end{pmatrix} \quad \text{donde } a = 0, \ldots, s.$$

Para calcular $M_n(s)$ con $n \geq 3$ veremos que las cosas no son tan sencillas. En efecto, necesitaremos bastantes herramientas algebraicas, entre ellas, la función de Hilbert y los ideales tóricos. Además, para calcular efectivamente $M_n(s)$ haremos uso de las bases de Gröbner de algunos ideales tóricos. El método que usaremos para contar cuadrados mágicos será asociar cada conjunto $\mathcal{C}M_n(s)$ con una región poliedral en R^n.

Notemos que los coeficientes de un cuadrado mágico están relacionados por ecuaciones lineales. En efecto, $M = (m_{ij})_{i,j} \in \mathcal{C}M_n$ sii

$$\begin{cases} m_{11} + \ldots + m_{1n} &= s & \text{(suma de la primer fila)} \\ & \vdots & \\ m_{n1} + \ldots + m_{nn} &= s & \text{(suma de la n-esima fila)} \\ m_{11} + \ldots + m_{n1} &= s & \text{(suma de la primer columna)} \\ & \vdots & \\ m_{1n} + \ldots + m_{nn} &= s & \text{(suma de la n-esima columna)} \end{cases}$$

Miremos las matrices como vectores de n^2 coordenadas en $\mathbb{Z}_{\geq 0}^{n^2}$, poniendo una fila a continuación de otra. Entonces, M es un cuadrado mágico de tamaño n sii M es solución positiva del sistema homogéneo de $n(n-1)$ ecuaciones

$$\begin{cases} \sum_{i=1}^n m_{1i} - \sum_{i=1}^n m_{ji} & \text{para todo } j \neq 1 \\ \sum_{i=1}^n m_{1i} - \sum_{i=1}^n m_{ij} & \text{para todo } j = 1, \ldots, n\ . \end{cases}$$

que proviene de pedir que la primer fila sume igual que cualquiera de las demás filas (primer grupo de ecuaciones) y que la primer fila también sume igual que cada una de las columnas (segundo grupo). La matriz A_n del sistema tendrá coeficientes 0, 1 ó -1 y será de tamaño $n(n-1) \times n^2$. La suma de la matriz M será la suma de cualquiera de sus filas, o columnas.

Ejemplo 2. *Para ilustrar un poco veamos cómo es la matriz de nuestro sistema lineal en el caso $n = 3$. En efecto,*

$$\vec{m} := (m_{11}, m_{12}, m_{13}, m_{21}, m_{22}, m_{23}, m_{31}, m_{32}, m_{33})$$

es cuadrado mágico sii tiene coeficientes positivos y es solución del sistema $A_3\vec{m} = 0$, donde

$$A_3 := \begin{pmatrix} 1 & 1 & 1 & -1 & -1 & -1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & -1 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & 0 \\ 1 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & -1 \end{pmatrix} \in \mathbb{Z}^{5\times 9}. \tag{1}$$

Definición 3. *Sea $\mathcal{K}_n := \ker(A_n) \cap \mathbb{Z}_{\geq 0}^{n\times n}$ el conjunto positivo de ceros de la matriz A_n.*

Tenemos entonces:

Proposición 2. *Con la notación anterior, $\mathcal{C}M_n = \mathcal{K}_n$.*

De ahora en más, trabajaremos con el conjunto $\mathcal{K}_n$, olvidando su "origen mágico". Veamos primero algunas propiedades sencillas que verifica.

Proposición 3. *Para cada $n \in \mathbb{N}$*

1. *$\mathcal{K}_n$ es cerrado bajo sumas de vectores en $Z^{n\times n}$, y contiene al vector $\vec{0}$.*[1]
2. *El conjunto $\mathcal{C}_n$ de soluciones de $A_n\vec{m} = \vec{0}$ con $\vec{m} \in \mathbb{R}^{n\times n}_{\geq 0}$ es un cono poliedral convexo en $\mathbb{R}^{n\times n}$ con vértice en el origen.*

Demostración: La afirmación (1) es clara por ser solución de un sistema homogéneo. Para probar (2), basta notar que el conjunto está formado por las soluciones de un sistema homogéneo que verifican las desigualdades $m_{ij} \geq 0$. Por otra parte, es un cono porque cualquier múltiplo positivo de una solución positiva es también una solución positiva. Finalmente, es convexo porque si $\vec{m}, \vec{m}' \in \mathcal{C}_n$, y $0 \leq t \leq 1$ entonces $t * \vec{m} + (1-t) * \vec{m}' \in \mathcal{C}_n$, ya que satisface el sistema $A_n x = 0$ y tiene coeficientes positivos porque cada coordenada es combinación convexa de coeficientes positivos. Es claro que el origen es vértice del cono $\mathcal{C}_n$. ■

A continuación trataremos de entender en profundidad la estructura de semigrupo de $\mathcal{K}_n$: buscaremos un sistema de generadores minimal para este conjunto. En este contexto surge naturalmente la siguiente definión.

Definición 4. *Sea $\mathcal{K}$ un sub-semigrupo de $\mathbb{Z}^N_{\geq 0}$. Un subconjunto finito $\mathcal{H} \subseteq \mathcal{K}$ es una* base de Hilbert *para $\mathcal{K}$ si satisface:*

1. *Para todo $k \in \mathcal{K}$ existen $h_i \in \mathcal{H}$ $(i = 1, \ldots, q_{(k)})$ y enteros no negativos c_i tales que $k = \sum_{i=1}^{q} c_i * h_i$,*
2. *$\mathcal{H}$ es minimal con respecto a la inclusión.*

Es un resultado conocido que las bases de Hilbert existen y son únicas para cualquier sub-semigrupo de $\mathcal{Z}^N_{\geq 0}$. En este caso, en vez de probar esta propiedad, daremos un algoritmo que, a partir de un sub-semigrupo $\mathcal{K} = \ker(A) \cap \mathbb{Z}^N_{\geq 0} \subseteq \mathbb{Z}^N_{\geq 0}$, donde A es una matriz entera con N columnas, dará un base de Hilbert. Usaremos las bases de Gröbner en todo este desarrollo.

Dado que nuestra matriz A admite coeficientes negativos, vamos a trabajar con polinomios de Laurent. A partir de $A = (a_{ij}) \in \mathbb{Z}^{m\times N}$ con coeficientes enteros, introducimos una variable z_i por cada fila, $i = 1, \ldots, m$ y consideramos el anillo de polinomios de Laurent:

$$k[z_1^{\pm}, \ldots, z_m^{\pm}] \simeq k[z_1, \ldots, z_m, t]/(tz_1 \cdots z_m - 1) \; .$$

A partir de esto, definimos una función

$$\psi : k[v_1, \ldots, v_N, w_1, \ldots, w_N] \longrightarrow k[z_1^{\pm}, \ldots, z_m^{\pm}][w_1, \ldots, w_N] \tag{2}$$

como sigue. Primero asignamos su valor en cada variable, y luego extendemos polinomialmente, de modo que resulte un morfismo de anillos. Definimos entonces:

$$\psi(v_j) = w_j \cdot \prod_{i=1}^{m} z_i^{a_{ij}} \quad ; \quad \psi(w_j) = w_j \qquad j = 1, \ldots, N \; .$$

Nuestro objetivo es detectar vectores enteros en $\ker(A)$.

Proposición 4. *Un vector entero positivo $\alpha^t \in \ker(A)$ si y sólo si $\psi(v^\alpha - w^\alpha) = 0$, esto es, si y sólo si $v^\alpha - w^\alpha$ pertenece al núcleo del morfismo ψ.*

[1] Esto dice que $\mathcal{K}_n$ es un sub-semigrupo de $\mathbb{Z}^{n\times n}_{\geq 0}$.

Demostración: Tomemos $v^\alpha - w^\alpha$ y calculemos su imagen vía ψ.
Por definición:

$$\psi(v^\alpha - w^\alpha) = \psi(v)^\alpha - \psi(w)^\alpha = \prod_{j=1}^{N} \psi(v_j)^{\alpha_j} - \prod_{j=1}^{N} w_j^{\alpha_j} = \prod_{j=1}^{N} (w_j \cdot \prod_{i=1}^{m} z_i^{a_{ij}})^{\alpha_j} -$$

$$- \prod_{j=1}^{N} w_j^{\alpha_j} = \prod_{j=1}^{N} w_j^{\alpha_j} \cdot \prod_{j=1}^{N} (\prod_{i=1}^{m} z_i^{a_{ij}})^{\alpha_j} - \prod_{j=1}^{N} w_j^{\alpha_j} = \big(\prod_{j=1}^{N} w_j^{\alpha_j}\big)\big(1 - \prod_{i=1}^{m}\prod_{j=1}^{N} z_i^{a_{ij}\alpha_j}\big) =$$

$$\big(\prod_{j=1}^{n} w_j^{\alpha_j}\big)\big(1 - \prod_{j=1}^{N} z_i^{\sum_{i=1}^{m} a_{ij}\cdot\alpha_j}\big) = \big(\prod_{j=1}^{N} w_j^{\alpha_j}\big)\big(1 - (z^{(A\alpha^t)^t})\big) .$$

Por lo tanto, $v^\alpha - w^\alpha \in \ker(\psi)$ si y sólo si $A\alpha^t = 0$, como queríamos probar. ■

Llamemos entonces $J = \ker(\psi)$ que es un ideal de $k[v_1, \ldots, v_N, w_1, \ldots, w_N]$. Tenemos una caracterización más precisa de J.

Proposición 5. *Con la notación anterior,*

$$J = \ker(\psi) = I \cap k[v_1, \ldots, v_N, w_1, \ldots, w_N]$$

donde

$$I = \underbrace{(w_j \cdot \prod_{i=1}^{m} z_i^{a_{ij}} - v_j \ : \ j = 1, \ldots, N)}_{h_j} \subseteq k[z_1^{\pm}, \ldots, z_m^{\pm}][v_1, \ldots, v_N, w_1, \ldots, w_N] .$$

Demostración: Lo haremos por doble inclusión.

(⊆) Como sabemos $\ker(\psi) \subset k[v_1, \ldots, v_N, w_1, \ldots, w_N]$, entonces basta ver que $\ker(\psi) \subset I$. Sea $f \in \ker(\psi)$,

$$\psi(f(v_1, \ldots, w_N) = f(\psi(v_1), \ldots, \psi(w_N) = f(\psi(v_1), \ldots, \psi(v_N), w_1, \ldots, w_N) . \tag{3}$$

Miremos las cosas en en $k[z_1^{\pm}, \ldots, z_m^{\pm}][v_1, \ldots, v_N, w_1, \ldots, w_N]/I$. Sabemos que $v_j - \psi(v_j) = h_j \in I$, luego $\bar{v_j} = \psi(v_j)$. Entonces, en el anillo cociente

$$0 = \bar{0} = \overline{\psi(f)} = \overline{f(\psi(v_1), \ldots, \psi(v_N), w_1, \ldots, w_N)} = \overline{f(v_1, \ldots, w_N)} \tag{4}$$

Luego $f \in I$, como queríamos probar.

(⊇) Sea $f \in I \cap k[v_1, \ldots, v_N, w_1, \ldots, w_N]$, y veamos que $\psi(f) = 0$.

Extendamos la función ψ al anillo $k[v, w][z^{\pm}]$, ya que las variables son todas algebraicamente independientes, vía $\tilde{\psi}(z_i) = z_i$. Entonces, por definición de los generadores de I, $\tilde{\psi}(I) = 0$. Por lo tanto, si $f \in I \cap k[v, w]$, tendremos también $\psi(f) = \tilde{\psi}(f) = 0$, como queríamos.

■

Corolario 1. *$J = \ker(\psi)$ contienen a un ideal tórico $\mathcal{I}$ de $k[v, w]$: el ideal asociado a la asociado a la matriz $\tilde{A}$, donde*

$$\tilde{A} = \left(\begin{array}{c|c} A & 0 \\ \hline I & I \end{array}\right) \in \mathbb{Z}^{(m+N)\times 2N} .$$

Demostración: Basta ver que

$$\mathcal{I} = (v^\alpha - w^\alpha \ : \ \alpha \in \ker(A)) = ((v, w)^{\tilde{\alpha}_+} - (v, w)^{\tilde{\alpha}_-} \ : \ \tilde{\alpha} \in \ker(\tilde{A}) \cap \mathbb{Z}^N_{\geq 0}) ,$$

ya que este ideal está incluido en J por Proposición 5. ■

Lema 3. *Con la notación de Proposición 5, J es un ideal homogéneo.*

Demostración: Sea $f \in J$, y veamos que cada una de sus componentes homogéneas está en J. Ahora bien, I es un ideal homogéneo de $k[z^{\pm}][v,w]$, por estar generado por polinomios homogéneos. Y entonces, cada una de las componentes homogéneas de f está en I. Pero además, están en $k[v,w]$ porque f lo está. Entonces, por la Proposición 5, queda probado el resultado. En efecto, J es la intersección de I un ideal homogéneo de $k[z^{\pm}][u,v]$ con un subanillo $k[u,v]$ de $k[z^{\pm}][u,v]$, luego es homogéneo. ■

El siguiente algoritmo de Sturmfels (Algorithm 1.4.5 de [2]) nos da una manera de encontrar la base de Hilbert de $\mathcal{K}$.

Teorema 2. *Sea $\mathcal{G}$ una base de Gröbner de I respecto de cualquier orden de eliminación $\succ$ tal que todas las variables $z_i, t \succ v_j$ y todas las $v_j \succ w_j$. Sea $\mathcal{S}$ el subconjunto de $\mathcal{G}$ formado por los elementos $v^\alpha - w^\alpha$ para algún $\alpha \in \mathbb{Z}^N_{\geq 0}$(en particular, estos binomios están en el ideal $\mathcal{I} \subset J$). Entonces*

$$\mathcal{H} = \{\alpha : v^\alpha - w^\alpha \in \mathcal{S}\}$$

es la base de Hilbert de $\mathcal{K}$.

Demostración: (Seguimos el Algoritmo 1.4.5 de [2]) En primer lugar, notemos que el ideal $J = J_A$ es un ideal primo y homogéneo, y que no hay monomios contenidos en J. En efecto, es ideal primo por ser el núcleo de un morfismo cuya imagen está incluida en un dominio. Es ideal homogéneo por el Lema 3. La imagen de monomios es no nula (es un monomio de Laurent), por lo tanto, ningún monomio puede estar en J.

Análogamente, $\beta \in \mathbb{Z}^N_{\geq 0}$ cae en $\mathcal{K}$ si y sólo si el binomio $v^\beta - w^\beta \in J$.

Queremos probar que el conjunto $\mathcal{H}$ genera el semigrupo $\mathcal{K}$. Lo haremos por el absurdo. Supongamos que no genera. En tal caso, existe un monomio minimal (respecto de la división[2]) v^β tal que $\beta \in \mathcal{K}$ pero β no es combinación de elementos de $\mathcal{H}$. El binomio $v^\beta - w^\beta$ pertenece a J (por Proposición 4), por lo tanto, se reduce a cero módulo $\mathcal{G}$. Por la especial elección del orden monomial, la primer parte de la división por $\mathcal{G}$ reduce v^β a un monomio $v^\gamma w^\delta$ donde $\delta = \beta - \gamma$ es no nulo (ambos monomios son homogéneos[3] del mismo grado β), ya que la división se hará con los elementos de $\mathcal{S}$ y sobre $k[v,w]$. En consecuencia:

$$v^\gamma w^\delta - w^\beta = w^\delta(v^\gamma - w^\gamma) \in J\ .$$

Pero J es un ideal primo y no contiene monomios, entonces $v^\gamma - w^\gamma \in J$, lo cual implica que $\gamma \in \mathcal{K}$. Por tanto, $\delta = \beta - \gamma \in \mathcal{K}$ (tanto β como γ pertenecen a $\mathcal{K}$, que es el núcleo positivo de A). Por ser β minimal, tenemos que tanto δ como γ son generados por elementos de $\mathcal{H}$. Luego, $\beta = \delta + \gamma$ también lo es. Esto contradice nuestra suposición, y el resultado queda probado. ■

Observación 3. *El Teorema anterior tiene vital importancia en el contexto de la Programación Entera. Ver Capítulo 6 Sección §1 en* [1]*, para más detalles.*

Ejemplo 3. *(Extraido de* [1]*) Veamos un ejemplo para ilustrar el Teorema 2. Consideremos el sub-semigrupo de $\mathbb{Z}^4_{\geq 0}$, dado por $\mathcal{K} = \ker(A) \cap \mathbb{Z}^4_{\geq 0}$, donde*

$$A = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 1 & 1 & -1 & -2 \end{pmatrix}\ .$$

Para encontrar la base de Hilbert de $\mathcal{H}$, consideramos el ideal I generado por

$$w_1 z_1 z_2 - v_1\ ;\ w_2 z_1^2 z_2 - v_2\ ;\ w_3 t - v_3\ ;\ w_4 z_1^2 t^2 - v_4\ ;\ z_1 z_2 t - 1\ .$$

en k[v,z,w,t]. Calculando una base de Gröbner $\mathcal{G}$ respecto de un orden de eliminación como el del Teorema, tenemos $\mathcal{S} = \{v_1 v_3 - w_1 w_3\}$. Por lo tanto, $\mathcal{H} = \{(1,0,1,0)\}$.

[2]El orden de división es: dados $a, b \in \mathbb{Z}^N_{\geq 0}$, $a \prec b$ sii $v^a | v^b$.

[3]Ver nota al pie [1].

Observación 4. *En el ejemplo anterior, además, dada la forma de la matriz A, se tiene* $rk(A) = 2$. *Sin embargo, al mirar directamente los coeficientes de la martiz se puede ver que todo punto entero positivo de* $\ker(A)$ *es un múltiplo entero positivo de* $(1, 0, 1, 0)$. *Sin embargo,* $\dim_{\mathbb{Q}} \ker(A) = \dim_{\mathbb{R}} \ker(A) = 2$. *En general, no hay relación alguna entre el cardinal de* (H) *y* $\dim_{\mathbb{R}} \ker(A)$. *Cada una de estas magnitudes depende exclusivamente de la matriz A.*

Antes de continuar, veamos un poco cómo es la estructura de una base de Gröbner cuando $I = I_A$ es un ideal tórico.

Proposición 6. *Cualquier base de Gröbner reducida de un ideal tórico* I_A *está formada por binomios.*

Demostración: Dada una matriz $A \in \mathbb{Z}^{m\times N}$, sabemos que

$$I_A = (X^\alpha - X^\beta \ : \ \alpha, \beta \in \mathbb{N}_0^N \setminus \{0\} \ , \ A(\alpha - \beta) = 0) \ .$$

Por Noetherianidad del anillo de polinomios, sabemos que I_A tiene un sistema finito de generadores, que resultarán binomios. De acuerdo con el algoritmo de Buchberger para la construcción de una base de Gröbner $\mathcal{G}$, cada paso consiste en la construcción de un S–polinomio y de tomar el resto del mismo. Veamos entonces que en cada paso, seguimos obteniendo binomios.
Dados $g_1 = X^{\alpha_1} - X^{\beta_1}$ y $g_2 = X^{\alpha_2} - X^{\beta_2}$, suponiendo $LT_\succ(g_i) = X^{\alpha_i}$, tenemos

$$S(g_1, g_2) = \frac{mcm(X^{\alpha_1}, X^{\alpha_2})}{X^{\alpha_1}} * g_1 - \frac{mcm(X^{\alpha_1}, X^{\alpha_2})}{X^{\alpha_2}} * g_2 =$$
$$-\big(\frac{mcm(X^{\alpha_1}, X^{\alpha_2})}{X^{\alpha_1}} * X^{\beta_1} - \frac{mcm(X^{\alpha_1}, X^{\alpha_2})}{X^{\alpha_2}} * X^{\beta_2}\big)$$

y resulta entonces un binomio. Además, al hacer la división entre 1 binomio y un conjunto de binomios, en cada etapa de la división, seguimos teniendo binomios, y cuando un monomio no es divisible por ningún monomio de cabeza, entonces el otro monomio no está en el ideal de los binomios. En efecto, si partimos de un monomio, y dividimos por los binomios, siempre obtendremos monomios, ya que en cada etapa obtendremos $X^\alpha - X^\beta(X^u - X^v)$ con $\alpha = \beta + u$, y esto da un monomio: $-X^{\beta+v}$.[4] Por lo tanto, si el primer monomio no es divisible por ningún monomio de cabeza, entonces pasa a formar parte del resto. Al dividir el otro monomio que queda, finalmente obtendremos un monomio, que se sumará a monomio que tenemos ya en el resto. En consecuencia, el resto será, siempre, 0 (si siempre podemos hacer la división entre los monomios de cabeza) o un binomio. ■

Proposición 7. *Todos los elementos* $x^\alpha - x^\beta$ *de una base de Gröbner de un ideal tórico* I_A *verifican* $\alpha - \beta \in \ker(A)$.

Demostración: Basta ver que en cada etapa del algoritmo de Buchberger obtenemos elementos con esta propiedad. Sea

$$\Gamma = \{x^\alpha - x^\beta \in I : \alpha - \beta \in \ker(A)\} \ .$$

Sabemos que I admite un conjunto de generadores que verifican la propiedad de Γ. El algoritmo de Buchberger se construye a partir de estos generadores. Sean g_1, g_2 binomios en $\mathcal{S}$, construido a partir de generadores de I vía el algoritmo que calcula $\mathcal{G}$, y veamos que si tienen la propiedad del enunciado (o sea $g_1, g_2 \in \Gamma$), entonces $S(g1, g2)$ y su resto en la división por $\mathcal{S}$ también tienen esta propiedad.

Por lo visto en la demostración de Proposición 6, tenemos que

$$S(g_1, g_2) = -\big(\frac{X^\delta}{X^{\alpha_1}} * X^{\beta_1} - \frac{X^\delta}{X^{\alpha_2}} * X^{\beta_2}\big) \ .$$

[4]Notar que si tenemos I ideal homogéneo, entonces $|\beta + v| = |\beta + u| = |\alpha|$, lo que muestra por qué el ideal del Teorema 2 es homogéneo.

Pero $A * \alpha_i^t = A * \beta_i^t$ para $i = 1, 2$, entonces $A * (\delta - \alpha_1 + \beta_1)^t = A * (\delta - \alpha_2 + \beta_2)^t$. Por lo tanto

$$g_1, g_2 \in \Gamma \quad \Longrightarrow \quad S(s_1, s_2) \in \Gamma \, .$$

Calculemos ahora el resto de la división de $S(g_1, g_2)$ por $\mathcal{S}$. Para ver que tiene la propiedad que queremos, veamos que el binomio obtenido en cada etapa de la división tiene la propiedad deseada. Sin pérdida de generalidad, supongamos que $LT_{\prec}(S(g_1, g_2)) = \frac{X^{\delta}}{X^{\alpha_1}} * X^{\beta_1}$. Entonces, sean $u, v \in \mathbb{Z}^N_{\geq 0}$ tales que $X^u - X^v \in \mathcal{S}$ y $LT_{\prec}(X^u - X^v) = X^u$ divide a $\frac{X^{\delta}}{X^{\alpha_1}} * X^{\beta_1}$. En consecuencia,

$$-S(g_1, g_2) = X^{((\delta - \alpha_1 + \beta_1) - u)} * (X^u - X^v) + X^{((\delta - \alpha_1 + \beta_1) - u) + v} - X^{(\delta - \alpha_2 + \beta_2)} \, .$$

Luego, hay que ver que $X^{((\delta - \alpha_1 + \beta_1) - u) + v} - X^{(\delta - \alpha_2 + \beta_2)} \in \Gamma$. Pero como $A * u^t = A * v^t$ y $A * (\delta - \alpha_1 + \beta_1)^t = A * (\delta - \alpha_2 + \beta_2)^t$ entonces

$$A * ((\delta - \alpha_1 + \beta_1) + (-u + v))^t = A * (\delta - \alpha_2 + \beta_2)^t$$

como queríamos probar. Luego, al finalizar la división tenemos que el resto tiene también la propiedad. En consecuencia

$$g_1, g_2 \in \Gamma \quad \Longrightarrow \quad R_{\mathcal{S}}(S(s_1, s_2)) \in \Gamma \, .$$

Por lo tanto, el algoritmo de Buchberger es invariante respecto de la propiedad que define a Γ y la Proposición queda demostrada. ■

Observación 5. *Dado que una base de Gróbner de un ideal tórico está formada por binomios, el cálculo de dicha base suele ser bastante rápido, aún teniendo muchos generadores. Esta es una gran ventaja, que permite hacer efectivos los cálculos que necesitamos para resolver nuestro problema.*

Continuaremos con nuestro problema de contar los cuadrados mágicos vía el Teorema 2. En nuestro caso, recordemos que nuestro conjunto $\mathcal{C}M_n$ está asociado al núcleo positivo y entero de una matriz A_n, que llamamos $\mathcal{K}_n$. Esto permite, vía el Teorema 2, construir una base de Hilbert para dicho núcleo, donde $\mathcal{S}$ es un subconjunto de una base de Gröbner $\mathcal{G}$ del ideal tórico I_{A_n}, asociado a la matriz A_n (de acuerdo con el Corolario 1). Trabajaremos con un orden monomial conveniente, para acelerar los cálculos de $\mathcal{G}$ y así obtener rápidamente una base de Hilbert para $\mathcal{K}_n$.

2. Caso $n = 3$

Veamos a modo de ejemplo introductorio el caso $n = 3$.

Ejemplo 4. *La expresión (1) nos da la matriz A_3, de acuerdo con esto, el ideal I_{A_3} está generado por los binomios:*

$$\begin{array}{rcl}
v_1 - w_1 z_1 z_2 z_4 z_5 & ; & v_2 - w_2 z_1^2 z_2^2 z_3^2 z_5 t \, ; \\
v_3 - w_3 z_1^2 z_2^2 z_3^2 z_4 t & ; & v_4 - w_4 z_2 z_4^2 z_5^2 t \, ; \\
v_5 - w_5 z_2 z_3 z_5 t & ; & v_6 - w_6 z_2 z_3 z_4 t \, ; \\
v_7 - w_7 z_1 z_4^2 z_5^2 t & ; & v_8 - w_8 z_1 z_3 z_5 t \, ; \\
v_9 - w_9 z_1 z_3 z_4 t & ; & t z_1 z_2 z_3 z_4 z_5 - 1
\end{array}$$

en el anillo $k[z_1, \ldots, z_5, t, v_1, \ldots, v_9, w_1, \ldots, w_9]$.
Usando un orden de eliminación como el indicado en el Teorema 2 (por ejemplo lexicográfico puro con orden $z_1 \succ \ldots \succ z_5 \succ t \succ v_1 \succ \ldots \succ v_9 \succ w_1 \succ \ldots \succ w_9$). En general, para cualquier orden de eliminación, la base de Gröbner correspondiente

al ideal I_{A_3} es muy grande, pero el conjunto $\mathcal{S}$ en este caso está formado por sólo 6 polinomios, a saber:

$$\begin{aligned} & v_3v_5v_7 - w_3w_5w_7 \quad ; \quad v_3v_4v_8 - w_3w_4w_8 \ ; \\ & v_2v_6v_7 - w_2w_6w_7 \quad ; \quad v_2v_4v_9 - w_2w_4w_9 \ ; \\ & v_1v_6v_8 - w_1w_6w_8 \quad ; \quad v_1v_5v_9 - w_1w_5w_9 \ . \end{aligned} \tag{5}$$

Identificando cada uno de los elementos anteriores con la matriz mágica correspondiente, ocurre un fenómeno interesante y que es coherente con el primer resultado enunciado (Proposición 1). En efecto, las matrices que aparecen son las 6 matrices de permutación de tamaño 3×3. Por ejemplo, el elemento $(0,0,1,0,1,0,1,0,0) \in \mathcal{H}$ correspondiente al primer polinomio en (5) es la matriz

$$T_{13} = P_{(1,3)} := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \ ,$$

asociada con la permutación que fija x_2. Análogamente, las otras matrices correspondientes son, en orden de aparición coincidente con la lista (5):

$$S = P_{(1,2,3)} := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad ; \quad S^2 = P_{(1,2,3)^2} := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \ ;$$

$$T_{12} = P_{(1,2)} := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad ; \quad T_{23} = P_{(2,3)} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \ ;$$

$$I = P_{id} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \ .$$

Con esto, para $n = 3$ tenemos, gracias al Teorema 2, que toda matriz M de $\mathcal{K}_3$ se escribe en la forma

$$M = a * I + b * S + c * S^2 + d * T_{12} + e * T_{13} + f * T_{23} \ , \tag{6}$$

donde a, b, c, d, e, f son enteros no negativos. Con esto, la suma de M es

$$s = a + b + c + d + e + f \ ,$$

como nos decía ya la Proposición 1.

En principio, podría parecer que hemos resuelto nuestro problema para $n = 3$, esto es, alcanza con contar la forma de escribir a s como suma de 6 enteros no negativos. Sin embargo, hay una pequeña dificultad: las matrices de permutación de 3×3 no son linealmente independientes, como hemos señalado oportunamente en la Observación 2. De hecho, hay una relación trivial

$$P_{id} + P_{(1,2,3)} + P_{(1,2,3)^2} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = P_{(1,2)} + P_{(1,3)} + P_{(2,3)} \ . \tag{7}$$

Como podemos incluir a $\mathbb{S}_3$ en $\mathbb{S}_n$ para todo $n \geq 3$ y los coeficientes que dan la combinación l.d. en ambos lados suman lo mismo (en este caso, 3) entonces, estos mismos coeficientes dan una relación l.d. entre P_σ con $\sigma \in \mathbb{S}_3 \subset \mathbb{S}_n$. Esto demuestra completamente la Observación 2 de la Sección anterior.

Como consecuencia de esta dependencia lineal, vemos que hay muchas combinaciones distintas de coeficientes que dan el mismo s. Por ende, necesitamos encontrar todas las relaciones entre las matrices de permutación, para tener una forma de eliminar estas combinaciones repetidas.

Lema 4. *Toda igualdad*

$$aI + bS + cS^2 + dT_{12} + eT_{13} + fT_{23} = a'I + b'S + c'S^2 + d'T_{12} + e'T_{13} + f'T_{23} \ ,$$

con $a, \ldots, f, a', \ldots, f'$ son enteros no negativos, es consecuencia de la relación (7), esto es

$$(a - a', \ldots, f - f') = \lambda(1, 1, 1, -1, -1, -1) \quad \lambda \in \mathbb{Z} \ ,$$

Demostración: Esto es consecuencia del siguiente hecho: las matrices de permutación de 3×3 forman un subespacio lineal de dimensión 5 en $M_n(\mathbb{R}, 3)$. En efecto, tenemos un núcleo de dimensión 1, y un generador con coeficientes enteros, que es el $(1, 1, 1, -1, -1, -1)$. ■

Con esto, ya estamos en condiciones de resolver nuestro problema, para $n = 3$. Vamos a identificar cada 6–upla $(a, b, c, d, e, f) \in \mathbb{Z}^6_{\geq 0}$ con un monomio en 6 nuevas variables $x_1, \ldots, x_6$:

$$\alpha = (a, b, c, d, e, f) \longleftrightarrow x^\alpha = x_1^a x_2^b x_3^c x_4^d x_5^e x_6^f \ .$$

De acuerdo con la ecuación (7) queremos identificar $x_1x_2x_3$ con $x_4x_5x_6$. Traduciendo a cocientes, necesitamos trabajar en el anillo

$$k[x_1, x_2, x_3, x_4, x_5, x_6]/(x_1x_2x_3 - x_4x_5x_6)$$

con los representantes de los monomios x^α.

Ahora, introduciremos la última herramienta necesaria: la función de Hilbert de este anillo cociente. En efecto, $M_n(s)$ se podrá reinterpretar como dicha función de Hilbert, en grado s. Para esto, introducimos algunas definiciones

Definición 5. *Dado un ideal homogéneo $I \subset k[x_1, \ldots, x_N]$ y el anillo cociente $R = k[x_1, \ldots, x_N]/I$ definimos la* función de Hilbert $H_R(s)$ *como*

$$H_R(s) = dim_k k[x_1, \ldots, x_N]_s / I_s = dim_k k[x_1, \ldots, x_N]_s - dim_k I_s \ , \tag{8}$$

donde $k[x_1, \ldots, x_N]_s$ es el k–espacio vectorial de los polinomios homogéneos de grado s, y I_s es el k–esp. vect. de los polinomios en I que son homog. y de grado s. A veces, también se nota a esta función con $HF_I(s)$, si queremos destacar al ideal en cuestión.

Un resultado conocido afirma que la función de Hilbert para I y $LT_\succ(I)$ es la misma, para cualquier orden monomial $\succ$. Luego, para calcular el valor de $HR(s)$ alcanza con calcular una base de Gröbner de I y mirar el número de monomios debajo del ideal inicial $LT_\succ(I)$ (monomios standard) para cada grado s, esto es, el conjunto de monomios de grado s que están fuera de $LT_\succ(I)$.

Proposición 8. *La función $M_3(s)$ coincide con la función de Hilbert $HR(s) = HF_I(s)$ del ideal homogéneo $I = (x_1x_2x_3 - x_4x_5x_6)$.*

Demostración: Para probar el resultado, basta encontrar una biyección entre los cuadrados mágicos $\mathcal{C}M_3(s)$ (o sea, con elementos de $\mathcal{K}_3$ de suma s) y los monomios standard de grado s.

Notemos primero que el elemento que forma el conjunto $\mathcal{G} = \{x_1x_2x_3 - x_4x_5x_6\}$ ya es una base de Gröbner para el ideal que genera, respecto de cualquier orden monomial[5]. Fijemos un orden monomial de modo que el monomio de cabeza de este polinomio sea $x_1x_2x_3$, para simplificar la notación. Con esto, los monomios standard de grado total s en $k[x_1, \ldots, x_6]$ son los monomios de grado total s no divisibles por $x_1x_2x_3$.
Dado un monomio $x^\alpha = x_1^a x_2^b x_3^c x_4^d x_5^e x_6^f$, buscamos su forma standard respecto de $\mathcal{G}$. Sea $D = \text{mín}\{a, b, c\}$, construyamos:

$$\alpha' = (a - D, b - D, c - D, d + D, e + D, f + D) \ ,$$

[5]Esta propiedad es la que simplifica el caso $n = 3$ frente a valores mayores de n.

de forma que $x^{\alpha'}$ no es divisible por $x_1x_2x_3$ y tiene igual grado que x^α. En consecuencia, es un monomio standard.
Afirmación: $x^{\alpha'}$ es el resto de x^α en la división por $\mathcal{G}$.
En efecto,

$$x^\alpha = q(x_1,\dots,x_6) * (x_1x_2x_3 - x_4x_5x_6) + x^{\alpha'}$$

donde

$$q = \big((x_1x_2x_3)^{D-1} + (x_1x_2x_3)^{D-2}(x_4x_5x_6) + \ldots + (x_4x_5x_6)^{D-1}\big) * \\ * x_1^{a-D}x_2^{b-D}x_3^{c-D}x_4^d x_5^e x_6^f \ .$$

Esto determina completamente α', y da su unicidad, por ser $x^{\alpha'}$ el resto de la división por $\mathcal{G}$. Luego, $HF_I(s) = \#\{\alpha'\} = \#\{x^{\alpha'}\}$.
Veamos ahora que $\mathcal{C}M_3(s)$ esta en correspondencia 1–1 con los $x^{\alpha'}$. Definamos la función

$$\varphi \ : \ \mathcal{C}M_3(s) \longrightarrow \{x^{\alpha'}\}$$

donde

$$\varphi(M_\alpha) = \varphi(aI + bS + cS^2 + dT_{12} + eT_{13} + fT_{23}) := x^{\alpha'} \ ,$$

si $\alpha = (a,b,c,d,e,f)$. La buena definición está garantizada por el Lema 4. Más aún, la suma de M coincide con el grado de $x^{\alpha'}$, por construcción.
Veamos que φ es la biyección buscada:

- Claramente φ es sobreyectiva, ya que tomando $\alpha = \alpha'$ obtenemos $\varphi(M_\alpha) = \alpha'$.
- φ es inyectiva. En efecto, sean α, β, tales que $\alpha' = \beta'$, y veamos que entonces $M_\alpha = M_\beta$. Sabemos que $M_\alpha = M_{\alpha'}$ y $M_\beta = M_{\beta'}$; por lo tanto, basta ver que $M_{\alpha'} = M_{\beta'}$, que es consecuencia inmediata de $\alpha' = \beta'$. ■

Corolario 2. *La cantidad de cuadrados mágicos en $\mathcal{C}M_3(s)$ es*

$$M_3(s) = \binom{s+5}{5} - \binom{(s-3)+5}{5} = \binom{s+5}{5} - \binom{s+2}{5} \ .$$

(Por convención $\binom{a}{b} = 0$ si $a < b$.)

Demostración: Los monomios no standard son los divisibles por $x_1x_2x_3$, por lo tanto, su número coincide con la cantidad de monomios en las variables $x_1,\dots,x_6$ de grado $s-3$. Como el total de monomios de grado 6 es $\binom{s+5}{5}$ y el de grado $s-3$ es $\binom{s+2}{5}$, el resultado sigue naturalmente. ■

Ejemplo 5. $M_3(1) = 6$, $M_3(2) = 21$, $M_3(3) = 56 - 1 = 55$.

Observación 6. *Hay otra manera, vinculada con las variedades tóricas, de entender la relación entre el semigrupo $\mathcal{K}_3$ y el anillo $R = k[x_1,\dots,x_6]/(x_1x_2x_3 - x_4x_5x_6)$, con su correspondiente variedad $\boldsymbol{V}(x_1x_2x_3 - x_4x_5x_6)$. En efecto, si $\mathcal{A} = (\vec{m}_1,\dots,\vec{m}_6) \subset \mathbb{Z}^9$ es el conjunto de vectores que representa todas las matrices de permutación de 3×3 (que es la base de Hilbert de $\mathcal{K}_3$) y definimos*

$$\phi_{\mathcal{A}} \ : \ (\mathbb{C}^*)^9 \longrightarrow \mathbb{P}^5 \qquad \phi_{\mathcal{A}}(t) = (t^{\vec{m}_1},\dots,t^{\vec{m}_6}) \ ,$$

entonces la variedad tórica Spec(R), que es la clausura (Zariski) de la imagen de $\phi_{\mathcal{A}}$, es la variedad proyectiva $\boldsymbol{V}(x_1x_2x_3 - x_4x_5x_6)$. El ideal $I_{\mathcal{A}} = (x_1x_2x_3 - x_4x_5x_6)$ es el idea tórico asociado a $\mathcal{A}$ como ya hemos comentado.

3. ¿Cómo generalizar a un n cualquiera?

El caso $n = 3$, pese a su sencillez, nos da todas las herramientas necesarias para trabajar en más dimensiones. Construiremos un método general, paso a paso a partir del caso $\mathcal{C}M_3$.
De acuerdo con lo visto en Proposición 1 sabemos que las permutaciones generan $\mathcal{C}M_n$, o lo que es lo mismo $\mathcal{K}_n$. En el caso $n = 3$ buscamos las relaciones de dependencia entera entre las matrices de permutaciones. En este caso, procederemos igual. Para ello, pensando a las matrices de permutaciones como vectores en n^2 entradas, construimos:

$$B_n := \left(\begin{array}{c|c|c|c|c} P_{\sigma_1} & P_{\sigma_2} & \cdots\cdots & P_{\sigma_{N-1}} & P_{\sigma_N} \end{array} \right) \in \{0,1\}^{m\times N} \subset \mathbb{Z}_{\geq 0}^{m\times N} ,$$

siendo $m = n^2$ y $N = n!$, y donde $\mathbb{S}_n = \{\sigma_1, \ldots, \sigma_N\}$.

Ahora, las relaciones enteras entre las matrices de permutación coinciden con los vectores enteros (no nulos) en el núcleo de B_n. Sea entonces

$$\tilde{\mathcal{K}} := \ker(B_n) \cap \mathbb{Z}_{\geq 0}^N$$

el conjunto de dichas relaciones enteras.

Lema 5. *$\tilde{\mathcal{K}}$ es un cono racional poliedral, con vértice en 0.*

Demostración: A tiene coeficientes enteros, entonces podemos elegir una base del núcleo en $\mathbb{Q}^N$; 0 es vértice porque tenemos las desigualdades $k_{ij} \geq 0$ para todo $k \in \tilde{\mathcal{K}}$. ■

Observación 7. *Una pregunta interesante a formular es cúal es la dimensión de $\tilde{\mathcal{K}}$ sobre $\mathbb{Q}$ (o $\mathbb{Z}$) y cuál es el cardinal de una base de Hilbert de este sub-semigrupo de $\mathbb{Z}_{\geq 0}^N$.*
En el caso $n = 4$, vía un cálculo con Maple, se ve que el rango de B_4 es 10, con lo cual, $\dim_{\mathbb{Q}}(\ker B_n) = 4! - 10 = 14$.

A continuación, siguiendo la construcción para $n = 3$, tenemos que mirar el ideal tórico en $k[x_1, \ldots, x_N]$, (en el caso $n = 3$ era $N = 6 = 3!$) asociado a la matriz B_n, esto es:

$$I = I_{B_n} := (x^{\alpha_+} - x^{\alpha_-} \ : \ \alpha \in \mathbb{Z}^N \ , \ B_n\alpha^t = 0) .$$

Siguiendo el caso anterior, debemos trabajar entonces en el anillo cociente $R = k[x_1, \ldots, x_n]/I$. Hay que ver si el ideal que tenemos es homogéneo. Esto equivale a ver que el vector $v = (1, 1, \ldots, 1) \in \mathbb{Z}_{\geq 0}^N$ está en el espacio generado sobre $\mathbb{Q}$ por las filas de B_n. Para el caso $n = 4$ esto es cierto. Veamos que esta hipótesis se cumple.

Lema 6. *I es un ideal homogéneo.*

Demostración: Veamos que $v = (1, 1, \ldots, 1) \in \mathbb{Z}_{\geq 0}^N$ está en el espacio generado por las filas, con coeficientes en $\mathbb{Q}$. Como las columnas de B_n son matrices de permutación, entonces cada columna de B_n tiene exactamente n unos. En consecuencia:

$$v * B_n = n(1, \ldots, 1) = n * v .$$

Como $n \neq 0$, esto dice que v está en el espacio de las filas. Y por lo señalado anteriormente, esto dice que todo vector del núcleo tiene suma de coordenadas nula. O sea $|\alpha_+| = |\alpha_-|$, y el ideal I es homogéneo por estar generado por polinomios homogéneos. ■

El siguiente paso, es tomar un orden monomial arbitrario $\succ$, y considerar $\mathcal{G}$ la base de Gröbner reducida de I respecto de este orden $\succ$. Como I es un ideal

binomial, entonces $\mathcal{G}$ será un conjunto finito de binomios. Además sus elementos serán homogéneos, de acuerdo con lo dicho en la Proposición 7.

Ahora, por Definición 5, siendo I ideal homogéneo, podemos considerar $HF_I(s)$ y veremos que efectivamente:

Proposición 9. *Con las notaciones anteriores*

$$M_n(s) = HF_I(s) \ .$$

Demostración: Sabemos que $HF_I(s) = HF_{LT_\succ(I)}(s)$. Por lo tanto, basta ver que hay una biyección entre los cuadrados mágicos de suma s y los monomios de grado s que no pertenecen a $LT_\succ(I)$.

Dado $\alpha \in \mathbb{Z}^N_{\geq 0}$, definimos $M_\alpha = \sum_{i=1}^N \alpha_i * P_{\sigma_i}$. Sabemos además que si $s = |\alpha|$, entonces $M_\alpha \in \mathcal{C}M_n(s)$. Miremos entonces para cada α de norma s, el monomio x^α y su resto en la división por $\mathcal{G}$, que llamaremos α'. Al igual que en la Proposición 8 para el caso $n = 3$, sabemos que

$$HF_I(s) = \#(\{x^{\alpha'}\}) = \#(\{\alpha'\}) \ .$$

Construimos la función

$$\varphi \ : \ \mathcal{C}M_n(s) \longrightarrow \{x^{\alpha'}\} \qquad \varphi(M_\alpha) = \alpha' \ .$$

Esta función está bien definida, por el Lema 7 que sigue. Veamos que φ es una biyección:

- φ es sobreyectiva: $M_{\alpha'} \mapsto \alpha'$, por Lema 7;
- φ es inyectiva. Es análoga al caso $n = 3$. Sólo hay que usar $M_\alpha = M_{\alpha'}$, que es parte del Lema 7.

■

Lema 7. *φ definida en la demostración de la Proposición 9 está bien definida. Además $M_\alpha = M_{\alpha'}$.*

Demostración: Supongamos $M_\alpha = M_\beta$, y veamos que entonces $\alpha' = \beta'$. Sabemos que $M_\alpha = \sum_{i=1}^N \alpha_i * P_{\sigma_i} = \sum_{i=1}^N \beta_i * P_{\sigma_i} = M_\beta$ si y sólo si $\sum_{i=1}^N (\alpha - \beta)_i * P_{\sigma_i} = 0$, o sea $\alpha - \beta \in \ker(B_n)$. En consecuencia, si $u := \alpha - \beta$, resulta $x^{u_+} - x^{u_-} \in I$. Necesitamos probar

$$\alpha - \beta \ \in \ker(B_n) \quad \iff \quad x^\alpha \equiv x^\beta \mod I \ .$$

Lo haremos por inducción en $LT_\succ(\underbrace{x^\alpha - x^\beta}_{:=f})$, si $f \neq 0$.

El caso base es $LT_\succ(f) = 1$. S.p.g. supongamos $LT(f) = x^\beta$. Esto dice $\beta = 0$. Luego, $u = \alpha - \beta \in \ker(\varphi)$ sii $\alpha \in \ker(\varphi)$. Esto dice $x^{u_+} - x^{u_-} \in I$, o equivalentemente, $x^{\alpha_+} \equiv x^{\alpha_-} \mod I$. Pero $\alpha = \alpha_+$ porque todos los coeficientes son positivos, entonces $x^\alpha = x^{\alpha_+} \equiv x^0 = x^\beta \mod I$, como queríamos.
Supongamos $LT(f) = x^\beta$ y que vale para todo $\gamma \prec \beta$. Vimos que $u \in \ker(B_n)$ sii $x^{u_+} - x^{u_-} \in I$. Dividamos entonces a nuestro binomio $f = x^\alpha - x^\beta$ por el conjunto $\mathcal{G}$. En un primer paso,

$$f = x^{\beta - v_+}(x^{v_+} - x^{v_-}) + x^{(\beta - v_+ + v_-)} - x^\alpha \ ,$$

donde $x^{v_+} - x^{v_-} \in \mathcal{G}$ y suponemos $x^{v_+} \succ x^{v_-}$. Pero entonces $x^{v_+}x^\beta = x^{v_+ + \beta} \succ x^{v_- + \beta} = x^{v_-}x^\beta$, o lo que es lo mismo $x^{(\beta - v_+ + v_-)} \prec x^\beta$, porque $\gamma = \beta - v_+ + v_- \in \mathbb{Z}^N_{\geq 0}$. Como:

- $\alpha, \gamma \prec \beta$;
- γ verifica $\alpha - \gamma \in \ker(B_n)$ sii $\alpha - \beta \in \ker(B_n)$ porque $\mathcal{G}$ es base de Gröbner de I (y uso Proposición 7);
- $f \equiv x^\gamma - x^\alpha \mod I$;

- Para todo $h \in k[x_1, \ldots, x_N] : h \in I \Leftrightarrow -h \in I$;

entonces, por hipótesis inductiva estamos hechos.

Finalmente $M_\alpha = M_{\alpha'}$ porque $x^\alpha \equiv x^{\alpha'} \bmod I$, y entonces $\alpha - \alpha' \in \ker B_n$. ■

En resumen, obtenemos:

Algoritmo 1. *Algoritmo para calcular $M_n(s)$.*

1. *Construir $B_n \in \mathbb{Z}_{\geq 0}^{m \times N}$ para obtener las relaciones enteras (racionales) entre las matrices de permutaciones (que son un sistema de generadores de $\mathcal{C}M_n$) (en este caso, $m = n^2$ y $N = n!$);*
2. *Construir $I = I_{B_n} \in k[x_1, \ldots, x_N]$ ideal tórico asociado a la matriz entera B_n;*
3. *Fijar un orden monomial arbitrario $\prec$ y calcular una base de Gröbner de I respecto de este orden;*
4. *Para cada $s \in \mathbb{N}$:*

   $$M_n(s) = \#\{\text{monomios de grado } s \text{ que están fuera de } LT_\prec(I)\} .$$

   Este es el cardinal del conjunto de restos en la división por $\mathcal{G}$ de los monomios en $k[x_1, \ldots, x_N]$ de grado s, que se puede calcular ya que el número de monomios de grado s es finito.

4. Generalización a otros cuadrados mágicos

En el caso de

$$D\mathcal{C}M_n(s) = \{M \in \mathcal{C}M_n(s) \ : \ \sum_{i=1}^{n} m_{ii} = s\}$$

o sea, los cuadrados mágicos en $\mathcal{C}M_n(s)$ que cumplen la restricción que la suma de cada diagonal es s, el método expuesto en la Sección 3 ya no puede aplicarse, debido a que las matrices de permutación ya no son un sistema de generadores sobre $\mathbb{Z}$. Para este caso, vamos a tener que utilizar el Teorema 2, para obtener un sistema de generadores, y luego conseguir las relaciones enteras entre los coeficientes. Esto se hace vía el cálculo del núcleo de un matriz C_n, cuyas columnas están formadas por los N elementos $\alpha \in \mathcal{H}$ del Teorema 2 (en este caso no tiene por qué ser $N = n!$; más aún será $N \leq n! - 2$ porque tenemos 2 condiciones extra). En el caso que el vector $v = (1, \ldots, 1) \in \mathbb{Z}_{\geq 0}^N$ estuviera en el espacio generado sobre $\mathbb{Q}$ por las filas de C_n, entonces el ideal tórico $I = I_{C_n}$ será homogéneo y podemos seguir el Algoritmo 1 para calcular la cantidad de cuadrados mágicos en $\mathcal{C}M_n(s)$ con suma de las diagonales igual a s. La dificultad adicional creada por la falta de una base de Hilbert canónica es la que muestra por qué eliminamos esta condición extra para las diagonales en la Definición 1.

Ejemplo 6. *Si miramos el caso $n = 3$, cada $M \in \mathcal{C}M_3(s)$ está asociado a $(a, b, c, d, e, f) \in \mathbb{Z}_{\geq 0}^6$ tales que si escribimos M como en la ecuación 6, entonces*

$$M \in D\mathcal{C}M_3(s) \iff 3a + f + d + e = s = a + b + c + d + e + f = 3e + a + b + c$$
$$\iff 2a = b + c \ \wedge \ 2e = f + d \, .$$

Por lo tanto:

$$D\mathcal{C}M_3(s) \longleftrightarrow (a, b, c, d, e, f) = (a, b, 2a - b, d, e, 2e - d) \in \mathbb{Z}_{\geq 0}^6$$

Los generadores son entonces: $\{I + 2 * S^2 \ ; \ S - S^2 \ ; \ T_{13} - T_{23} \ ; T_{13} + 2 * T_{23}\}$. Este conjunto tiene cardinal $4 = 3! - 2$.

Como la relación de dependencia entera que había en el caso $n = 3$ para $\mathcal{C}M_3$ se sigue manteniendo ($2 * a = 2 = 1 + 1 = b + c$; $2 * e = 2 = 1 + 1 = d + f$),

entonces $v = (1, 1, 1, 1)$ está en el espacio de las filas de la matriz C_n formada con los nuevos generadores. Luego, el ideal tórico asociado será homogéneo y podemos proceder como en el Algoritmo 1, cambiando B_n por C_n en el primer paso.

Referencias

[1] D. Cox, J. Little, D. O'Shea, "*Using Algebraic Geometry*". Graduate Texts in Mathematics, vol. 185. Springer-Verlag, New York, 1998, Capítulo 6.

[2] B. Sturmfels, "*Algorithms in Invariant Theory*". Texts and Monographs in Symbolic Computation. Springer-Verlag, New York, 1993.

[3] J.-P. Brasselet, "*Introduction to Toric Varieties*". 23° Colóquio Brasileiro de Matemática. IMPA, 2001.

[4] S. Hoşten, R. Thomas, "*Gröbner basis and integer programming*". "Groebner Bases and Applications, (Proc. of 33 Years of Groebner Bases Conference)", [B. Buchberger and F. Winkler eds.], London Math. Soc. Lecture Notes Series 251, Cambridge University Press, 1998, pp. 144-158.