PESQUIMAT 20(2): 1–20 (2017) ISSN:1560-912X/ ISSN-E:1609-8439
http://dx.doi.org/10.15381/pes.v20i2.13963 Facultad de Ciencias Matemáticas – UNMSM

Un estudio del algoritmo del elipsoide

Edinson Montoro Alegre, [1] ***Carole Huamán Oriundo,*** [2]
Gladys Melgarejo Estremadoyro [3] ***y Melanio Sampertegui Gonzáles*** [4]

Resumen: En el presente artículo se presenta los principales lemas y teoremas que fundamentan y prueban las bondades del algoritmo del elipsoide de Khachiyan, pero de una menera menos complicada que el trabajo original con la finalidad de poner al alcance de los interesados y de los estudiantes del área de optimización un tema tan importante desde el punto de vista teórico y que ha sido el punto de partida de muchos de otros trabajos de investigación.
Palabras clave: programación lineal; conjuntos convexos; elipsoides; capsula convexa; álgebra lineal.

A Study of the Ellipsoid Algorithm

Abstract: In the present work are presented the principal lemmas and theorems that are based and prove the benefits of the Khachiyan ellipsoid algorithm, but in a less complicated way than the original work in order to make available to the interested parties and the students of the area of optimization a subject so important from the theoretical point of view and that has been the starting point of many other research work.
Keywords: linear programming; convex sets; ellipsoids;convex capsule; linear algebra.

Recibido: 01/10/2016. *Aceptado*: 20/12/2017. *Publicado online*: 31/12/2017

[1]UNMSM, Facultad de Ciencias Matemáticas, e-mail: emontoroa@unmsm.edu.pe
[2]UNMSM, Facultad de Ciencias Matemáticas, e-mail: chuamano@unmsm.edu.pe
[3]UNMSM, Facultad de Ciencias Matemáticas, e-mail: gmelgarejoe@unmsm.edu.pe
[4]UNMSM, Facultad de Ciencias Matemáticas, e-mail: msamperteguig@unmsm.edu.pe

1. Introducción

En el año 1979, el matemático soviético L.G. Khachiyan [2] publicó la demostración para un algoritmo que resuelve problemas de programación lineal, que lo hace en tiempo polinomial, resolviendo así, al menos teóricamente una cuestión abierta desde mucho tiempo atras. El resultado de Khachiyan se basó en los trabajos de otros matemáticos soviéticos sobre programación no lineal como Shor, Yudin y Nemirovskii [4] ; y dicho algoritmo es conocido como el **Algoritmo del Elipsoide**.

El algoritmo del elipsoide toma como entrada un conjunto convexo y retorna un punto del conjunto, probando de esta manera que el conjunto es no vacío, caso contrario el algoritmo retorna el mensaje que el conjunto es vacío. Es claro que este algoritmo es útil para probar la feasibilidad de los Problemas de Programación Lineal . Asi mismo el algoritmo también puede ser usado para resolver Problemas de Programación Lineal. Formalmente, el algoritmo del elipsoide averigua si un conjunto convexo $K \subseteq \mathbb{R}^n$ es vacío o nó.

El Algoritmo necesita como entrada:

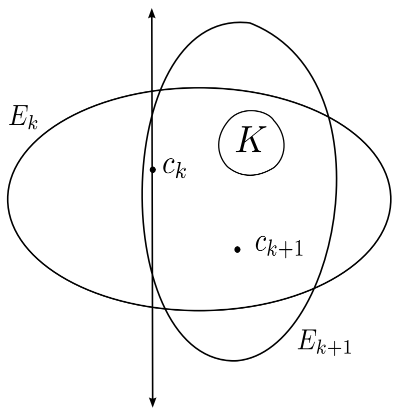
i) El conjunto convexo $K \subseteq \mathbb{R}^n$

ii) Un número $R \in \mathbb{Q}$, $R > 0$ tal que $K \subseteq B(0, R) = E_0$

Dicho algoritmo se aplica de la siguiente manera: Dado un conjunto K determinado por desigualdades lineales $Ax < b$, y se construye en cada iteración una elipsoide que contenga siempre al conjunto K. El elipsoide construido en cada iteración es siempre "mas pequeño"que el anterior, de manera que, despues de un número determinado de iteraciones se encuentra un punto de K o se concluye que K es vacío, es decir que tal punto no existe.

Graficamente podemos esbozar el método de la siguiente manera. Supongase que se tiene un elipsoide $E_k = E(c_k, Q_k)$ y también tenemos un hiperplano separador $H = \left\{x/a_k^t x = a_k^t c_i\right\}$ donde a_k^t es la fila de A^k que c_k no satisface.

Nuestro objetivo será calcular (o determinar) el elipsoide de volumen mínimo E_{k+1} que contenga al semi-elipsoide E_k y $K \subseteq E_{k+1}$ es decir $a_k^t x \geq a_k^t c_k$, y este proceso se repite.



2. Preliminares

2.1. Algoritmo del elipsoide

Consideremos el siguiente sistema de desigualdades lineales estrictas con coeficientes enteros

$$a_i^t x < b_i \quad i = 1, 2, ..., n \tag{1}$$

donde $a_i \in \mathbb{Z}^n$, $x \in \mathbb{R}^n$, $b_i \in \mathbb{Z}$. El conjunto de todos los puntos x que satisfacen (1) es llamado K.

Debemos notar que si tuvieramos coeficientes a_i y b_i en $\mathbb{Q} - \mathbb{Z}$ racionales estos podrían ser llevados al formato entero, simplemente multiplicando por el mínimo común múltiplo de (a_i y b_i) a todas las desigualdades y si fueran irracionales, estos serían truncados cuando se "lleve" el problema al computador, por lo que pueden ser tratados como racionales.

Por la definición de un elipsoide, existe una transformación alfin invertible L^{-1} que toma la elipse E_k y lo transforma en una bola $B(0,1)$ de centro 0 y radio 1, entonces $E_k^{'} = B(0,1)$. Al vector a_k que es una fila de A_k y que el punto c_k no satisface lo lleva a $a_k^{'} = (-1, 0, 0, .., 0)$. Con estos elementos y las formulas (3) y (4) construimos $E_{k+1}^{'}$, luego lo "regresamos" al espacio original y obtenemos el elipsoide que buscamos $E_{k+1} = L(E_{k+1}^{'})$.

Sea, el problema de hallar un x que satisfaga

$$Ax < b \tag{2}$$

donde $A \in \mathbb{R}^{m \times n}$, $x \in \mathbb{R}^n$, $b \in \mathbb{R}^m$.

Definición 2.1 Se define el tamaño del problema (2) como:

$$L = \left\{ \sum_{\substack{i,j \\ a_{i,j} \neq 0}} (\log |a_{ij}| + 1) \right\} + \left\{ \sum_{\substack{i \\ b_i \neq 0}} (\log |b_i| + 1) \right\} + \{\log(mn) + 1\}.$$

Definimos una suceción $\{x_k\} \in \mathbb{R}^n$ de vectores y una sucesión de matrices simétricas definidas positivas de orden n: $\{A_k\} \subset \mathbb{R}^{nxn}$ en forma recursiva:

$$x_{k+1} = x_k - \frac{1}{n+1} \frac{A_k a_{i_k}}{\sqrt{a_{i_k}^t A_k a_{i_k}}} \tag{3}$$

$$A_{k+1} = \frac{n^2}{n^2 - 1} \left(A_k - \frac{2}{n+1} \frac{(A_k a_{i_k})(A_k a_{i_k})^t}{a_{i_k}^t A_k a_{i_k}} \right) \tag{4}$$

con $x_0 = 0$, $A_0 = 2^{2L} I$, $a_{i_k} \in \mathbb{R}^n$, $b_{i_k} \in \mathbb{R}$, $R = 2^L$.

Veremos que si x_k es solución de (1) el proceso dado por el algoritmo se detiene, caso contrario, una de las desigualdades de (1) no se cumple, es decir

$$a_{i_k}^t x \geq b_{i_k}$$

y con este vector a_{i_k} se genera un nuevo punto x_{k+1}.

A continuación presentamos el algoritmo del elipsoide.

Algoritmo Elipsoide (A, b)

Inicio: $x_0 = 0$, $A_0 = 2^L I$, $A = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$ a_i filas de A, $b \in \mathbb{R}^n$

Paso $1:$ Si x_k es solución de
$Ax < b$ (o $a_i^t x < b_i \ \forall i = 1, 2, ..., m$)
Entonces, paramos
sino $\exists\, a_{i_k}^t$ tal que $a_{i_k}^t x_k \geq b_{i_k}$

Paso $2:$ Generamos

$$\begin{aligned} x_{k+1} &:= x_k - \frac{1}{n+1}\frac{A_k a_{i_k}}{\sqrt{a_{i_k}^t A_k a_{i_k}}} \\ A_{k+1} &:= \frac{n^2}{n^2-1}\left(A_k - \frac{2}{n+1}\frac{(A_k a_{i_k})(A_k a_{i_k})^t}{a_{i_k}^t A_k a_{i_k}}\right) \\ k &:= k+1 \end{aligned}$$

Paso $3:$ Si $k > 4(n+1)^2 L$ entonces PARAMOS (el conjunto es vacío no tiene solución)
Si no volver al paso 1

Debemos notar que una elipsoide puede ser definida como la imagen de una bola unitaria vía una transformación afín L, es decir

$$\begin{aligned} L\left(B(0,1)\right) &= \{Lx \in \mathbb{R}^n /\ x \in B(0,1)\} \\ &= \left\{y = Lx \in \mathbb{R}^n /\ x = L^{-1} \in B(0,1)\right\} \\ &= \left\{y \in \mathbb{R}^n /\ \|0 - L^{-1}y\| \leq 1\right\} \\ &= \left\{y \in \mathbb{R}^n /\ \|L^{-1}y\|^2 \leq 1^2\right\} \\ &= \left\{y \in \mathbb{R}^n /\ \left(L^{-1}y\right)^t \left(L^{-1}y\right) \leq 1\right\} \\ &= \left\{y \in \mathbb{R}^n /\ y^t \left(L^{-1}\right)^t \left(L^{-1}y\right) \leq 1\right\} \\ &= \left\{y \in \mathbb{R}^n /\ y^t \left(LL^t\right)^{-1} y \leq 1\right\} \\ &= \left\{y \in \mathbb{R}^n /\ y^t Q^{-1} y \leq 1\right\} = E(0,Q),\ \text{donde } Q = LL^t. \end{aligned}$$

Al último conjunto se le llama Elipsoide centrado en cero y asociada a la matriz cuadrada $Q = LL^t$ que es simétrica y definida positiva. En efecto,

i) $Q^t = \left(LL^t\right)^t = \left(L^t\right)^t L^t = LL^t = Q$, (Simétrica)

ii) Para cualquier $x \in \mathbb{R}^n$

$$\begin{aligned} x^t Q x &= x^t \left(LL^t\right) x \ = \ \left(x^t L\right)\left(L^t x\right) \\ &= \left(L^t x\right)^t \left(L^t x\right) \ = \ \|L^t x\|^2 \geq 0. \end{aligned}$$

Definición 2.2 En general podemos definir una elipsoide:
Dado $x_0 \in \mathbb{R}^n$ y una matriz Q simétrica y semidefinida positiva, definimos el elipsoide $E(x_0, Q)$ con centro en x_0 y radio 1 al conjunto

$$E(x_0, Q) = \left\{ y \in \mathbb{R}^n / \ (y - x_0)^t Q^{-1} (y - x_0) \leq 1 \right\}$$

Observación 2.3

1) Si $Q = I$ entonces $E(x_0, Q) = E(x_0, I) = B(x_0, 1)$
Quiere decir que la bola de centro x_0 y radio 1 es el elipsoide con centro x_0 asociada a la matriz identidad.

2) Si $Q = R^2 I$, $R \in \mathbb{R}$, entonces $E(x_0, Q) = B(x_0, R)$. En efecto:
Si $Q = R^2 I = \begin{pmatrix} R^2 & & & \\ & R^2 & & 0 \\ 0 & & \ddots & \\ & & & R^2 \end{pmatrix}$ entonces $Q^{-1} = \begin{pmatrix} \frac{1}{R^2} & & & \\ & \frac{1}{R^2} & & 0 \\ 0 & & \ddots & \\ & & & \frac{1}{R^2} \end{pmatrix}$
Es decir $Q^{-1} = \dfrac{1}{R^2} I$, Luego

$$\begin{aligned} E(x_0, Q) &= \left\{ y \in \mathbb{R}^n / \ (y - x_0)^t Q^{-1} (y - x_0) \leq 1 \right\} \\ &= \left\{ y \in \mathbb{R}^n / \ (y - x_0)^t \frac{1}{R^2} I (y - x_0) \leq 1 \right\} \\ &= \left\{ y \in \mathbb{R}^n / \ (y - x_0)^t (y - x_0) \leq R^2 \right\} \\ &= \left\{ y \in \mathbb{R}^n / \ ||y - x_0||^2 \leq R^2 \right\} = \{ y \in \mathbb{R}^n / \ ||y - x_0|| \leq R \} = B(x_0, R) \end{aligned}$$

3) Se cumple que:

$$\begin{aligned} E(x_0, Q) &= \left\{ y \in \mathbb{R}^n / \ (y - x_0)^t Q^{-1} (y - x_0) \leq 1 \right\} \\ &= \left\{ y \in \mathbb{R}^n / \ (y - x_0)^t \left(Q^{t^{-\frac{1}{2}}} Q^{-\frac{1}{2}} \right) (y - x_0) \leq 1 \right\} \\ &= \left\{ y \in \mathbb{R}^n / \ \left[(y - x_0)^t \left(Q^{-\frac{1}{2}} \right)^t \right] \left[Q^{-\frac{1}{2}} (y - x_0) \right] \leq 1 \right\} \\ &= \left\{ y \in \mathbb{R}^n / \ \left[\left(Q^{-\frac{1}{2}} \right) (y - x_0) \right]^t \left[Q^{-\frac{1}{2}} (y - x_0) \right] \leq 1 \right\} \\ &= \left\{ y \in \mathbb{R}^n / \ ||Q^{-\frac{1}{2}} (y - x_0)||^2 \leq 1 \right\} = \left\{ y \in \mathbb{R}^n / \ ||Q^{-\frac{1}{2}} (y - x_0)|| \leq 1 \right\} \end{aligned}$$

Lema 2.4 *Las matrices $A_0, A_1, ..., A_k$ de orden $n \times n$ definidas por (3) y (4) son simétricas y definidas positivas.*

Demostración. Probemos la simétria: Por la definición de A_{k+1} y considerando A_k simétrica

$$\begin{aligned} (A_{k+1})^t &= \left[\frac{n^2}{n^2 - 1} \left(A_k - \frac{2}{n+1} . \frac{(A_k a_{i_k}) (A_k a_{i_k})^t}{a_{i_k}^t A_k a_{i_k}} \right) \right]^t \\ &= \left(\frac{n^2}{n^2 - 1} \right)^t \left(A_k^t - \left(\frac{2}{n+1} \right)^t \left[\frac{(A_k a_{i_k}) (A_k a_{i_k})^t}{a_{i_k}^t A_k a_{i_k}} \right]^t \right) \\ &= \left(\frac{n^2}{n^2 - 1} \right) \left(A_k - \frac{2}{n+1} . \left[\frac{\left((A_k a_{i_k})^t \right)^t (A_k a_{i_k})^t}{\left(a_{i_k}^t A_k a_{i_k} \right)^t} \right] \right) \end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{n^2}{n^2-1}\right)\left(A_k - \frac{2}{n+1}.\left(\frac{(A_k a_{i_k})(A_k a_{i_k})^t}{a_{i_k}^t A_k^t \left(a_{i_k}^t\right)^t}\right)\right)\\
&= \left(\frac{n^2}{n^2-1}\right)\left(A_k - \frac{2}{n+1}.\frac{(A_k a_{i_k})(A_k a_{i_k})^t}{a_{i_k}^t A_k a_{i_k}}\right) = A_{k+1}.
\end{aligned}
$$

■

Debemos tener presente que nuestro algoritmo se va iniciar con un elipsoide $E_0 = \left(0, R^2 I\right)$ con centro en el origen y matriz simétrica definida positiva $Q = R^2 I$ con $R = 2^L$.

Por la observación (2.3) sabemos que ésta primera elipse es en realidad una bola $B(0,R)$ con centro en el origen y radio R (Se probará más adelante que la $B(0,R)$ contiene a la región factible $K = \{x/\ Ax < b\}$). También debemos considerar que el punto inicial sera $x_0 = 0$ el origen y que este punto $x_0 \notin K$.

Observación 2.5 *El* $A_0 = Q = R^2 I$, *como* $x_0 \notin K \Rightarrow \exists\ a_{i_k}^t$ *fila de* A *tal que* $a_{i_k} x_0 \geq b_i$.

En general supongamos que $E_k = E(x_k, A_k)$ es una elipsoide asociada con A_k simétrica y definida positiva. Entonces, para toda elipsoide E_k existe una transformación afin L^{-1} tal que

$L^{-1}(E_k) = B(0,1)$, y la matriz asociada a L es $A_k^{'}$ que es diagonal y definida positiva,

con $L^{-1}(x_k) = 0 = y_0$ y $L^{-1}(a_{i_k}) = (-1, 0, ..., 0)$.
Luego, en el espacio transformado calculamos el y_1 segun (3) y (4)

$$
\begin{aligned}
y_1 &= y_0 - \frac{1}{n+1}.\frac{A_k^{'}(-1,0,...,0)}{\sqrt{(-1,0,...,0)^t A_k^{'}(-1,0,...,0)}}\\
y_1 &= 0 - \frac{1}{n+1}.\frac{1}{\alpha_k^{'}}(-\alpha_k^{'}, 0, ..., 0)\begin{pmatrix}-1\\0\\\vdots\\0\end{pmatrix} = \left(\frac{1}{n+1}, 0, ..., 0\right)
\end{aligned}
$$

y de aqui calculamos $x_{k+1} = L y_1$.

Ahora calculamos $A_{k+1}^{'}$ el cual también será diagonal definida positiva. En efecto, usando (3) y (4)

$$
\begin{aligned}
A_{k+1}^{'} &= \frac{n^2}{n^2-1}\left[A_k^{'} - \frac{2}{n+1}\frac{\left(A_k^{'} a_{i_k}^{'}\right)\left(A_k^{'} a_{i_k}^{'}\right)^t}{\left(a_{i_k}^{'}\right)^t A_k^{'}\left(a_{i_k}^{'}\right)}\right]\\
A_{k+1}^{'} &= \frac{n^2}{n^2-1}\left[I - \frac{2}{n+1}\left[\frac{\left(I\begin{pmatrix}-1\\0\\\vdots\\0\end{pmatrix}\right)\left(I\begin{pmatrix}-1\\0\\\vdots\\0\end{pmatrix}\right)^t}{(-1,0,...,0)I\begin{pmatrix}-1\\0\\\vdots\\0\end{pmatrix}}\right]\right]
\end{aligned}
$$

$$
\begin{aligned}
A'_{k+1} &= \frac{n^2}{n^2-1}\left[I - \frac{2}{n+1}\begin{pmatrix} 1 & & \\ & 0 & 0 \\ 0 & & \ddots \\ & & 0 \end{pmatrix}\right] = \frac{n^2}{n^2-1}\begin{pmatrix} 1-\frac{2}{n+1} & & \\ & 1 & 0 \\ 0 & & \ddots \\ & & 1 \end{pmatrix} \\
A'_{k+1} &= \frac{n^2}{n^2-1}\begin{pmatrix} \frac{n-1}{n+1} & & \\ & 1 & 0 \\ 0 & & \ddots \\ & & 1 \end{pmatrix} = \frac{n^2}{n^2-1} diag\left(\frac{n-1}{n+1}, 1, ..., 1\right)
\end{aligned}
$$

el cual es definida positiva y diagonal.

A partir de A'_{k+1} calculamos $A_{k+1} = LA'_{k+1}$ que será la matriz asociada a la elipse

$$E_{k+1} = (x_{k+1}, A_{k+1}).$$

Notación: Por simplicidad vamos a denotar a la elipse $E(x_k, A_k)$ por E_k.

Lema 2.6 *Se cumple*

$$2^L \geq \prod_{i=1}^{m}\prod_{j=1}^{n}(|a_{ij}|+1)\cdot\prod_{i=1}^{m}(|b_i|+1)\,(mn+1)$$

donde L es el tamaño del problema 2*.*

Demostración. Primero se probará que:

$$2^{\log n+1} \geq (n+1) \quad \forall n \in \mathbb{N} - \{0\} \tag{5}$$

o equivalentemente $\log_2(n+1) \leq \log_2 n + 1$.
Consideremos el intervalo $I_p = \left[2^p, 2^{p+1}-1\right]$, $p \in \mathbb{N}$ y $n \in I_p \cap (\mathbb{N} - \{0\})$. Por ser $\log_2$ una funcion monótona creciente se tiene

$$
\begin{aligned}
n &\leq 2^{p+1}-1 \\
n+1 &\leq 2^{p+1} \\
\log_2(n+1) &\leq p+1 \qquad (6)
\end{aligned}
$$

y

$$
\begin{aligned}
2^p &\leq n \\
\log_2 2^p &\leq \log_2 n \\
p &\leq \log_2 n \\
p+1 &\leq \log_2 n + 1. \qquad (7)
\end{aligned}
$$

De (6) y (7) se obtiene

$$\log_2(n+1) \leq \log_2(n+1).$$

Finalmente

$$
\begin{aligned}
2^L &= 2^{\sum\sum(\log(|a_{ij}|+1))+\sum(\log(|b_i|+1))+(\log(mn+1))} \\
&= 2^{\log(|a_{ij}|+1)}\ldots 2^{\log(|a_{mn}|)}\cdot 2^{\log(|b_i|+1)}\ldots 2^{\log(|b_m|+1)}\ldots 2^{\log(mn)} \\
&= \prod_{i=1}^{m}\prod_{j=1}^{n} 2^{\log(|a_{ij}|+1)}\cdot\prod_{i=1}^{m} 2^{\log(|b_i|+1)}\cdot 2^{\log(mn+1)} \qquad (8)
\end{aligned}
$$

De (5) y (8) se obtiene

$$2^L \geq \prod_{i=1}^{m}\prod_{j=1}^{n}(|a_{ij}|+1)\cdot\prod_{i=1}^{m}(|b_i|+1)\,(mn+1).$$

■

Lema 2.7 *Si M es el valor de la determinante de una matriz $A=[a_{ij}]_{m\times n}$ cuyos elementos son $a_{ij}\in\mathbb{Z}$ que define el vértice de un poliedro, se cumple*

$$M \leq \prod_{i=1}^{m}\prod_{j=1}^{n}(|a_{ij}|+1).$$

Demostración. Veamos para el caso $n=3$, $\quad A=\begin{bmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix}$

Sea

$$\begin{aligned}
M_1 &= a_{11}\\
M_2 &= \begin{vmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{vmatrix} = a_{11}a_{22}-a_{21}a_{12}\\
M_3 &= a_{11}\begin{vmatrix} a_{22} & a_{23}\\ a_{32} & a_{33}\end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23}\\ a_{31} & a_{33}\end{vmatrix} - a_{13}\begin{vmatrix} a_{21} & a_{22}\\ a_{31} & a_{32}\end{vmatrix}\\
&= a_{11}(a_{22}a_{33}-a_{32}a_{23}) - a_{12}(a_{21}a_{33}-a_{31}a_{23}) + a_{13}(a_{21}a_{32}-a_{22}a_{31})\\
&= a_{11}a_{22}a_{33} - a_{11}a_{32}a_{23} - a_{12}a_{21}a_{33} + a_{12}a_{31}a_{23} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}
\end{aligned}$$

Es facil notar que

$$\begin{aligned}
M_i \leq\ & (|a_{11}|+1)(|a_{12}|+1)(|a_{13}|+1)(|a_{21}|+1)(|a_{22}|+1)(|a_{23}|+1)\cdots\\
& \cdots(|a_{31}|+1)(|a_{32}|+1)(|a_{33}|+1)
\end{aligned}$$

pues el lado derecho es un polinomio de grado 9 y los determinantes son de grado a lo más 3. El mismo análisis se hace para $n=4$ y $n=5$. Concluyéndose por inducción que es válido para n.

■

Lema 2.8 *Sea $v^t=(v^1,v^2,...,v^n)$ un vértice cualquiera del poliedro*

$$\begin{aligned}
\Gamma &= \left\{x\in\mathbb{R}^n/\ \begin{matrix} Ax\leq b\\ x\geq 0\end{matrix}\right\}\\
&= \left\{x\in\mathbb{R}^n/\ \begin{matrix} a_i^t x\leq b_i\\ x\geq 0\end{matrix},\ i=1,2,\cdots,m\right\}\ \text{con } m<n.
\end{aligned}$$

Se cumple

a) Las coordenadas de v son números racionales de denominador menor que $\dfrac{2^L}{n}$.

b) $||v||<2^L$.

Demostración.

a) Por ser v un vértice, entonces satisface $Av = b$ luego v es solución del sistema $m \times n$. Por la Regla de Cramer los $v^i = \dfrac{M^i}{M}$ donde M^i y M son determinantes de submatrices que a lo más serán de orden $m \times m$. Asi mismos esas determinantes son el producto de los coeficientes o entradas de A y b (a_{ij} y b_i) por lo tanto como a_{ij}, b_i son enteros, entonces M y M^i también seran enteros. Luego por el lema anterior

$$M \leq \prod_{i=1}^{m}\prod_{j=1}^{m}(|a_{ij}|+1)\prod_{i=1}^{m}(|b_i|+1)$$

Por otro lado

$$\begin{aligned}\prod_{i=1}^{m}\prod_{j=1}^{m}(|a_{ij}|+1)\prod_{i=1}^{m}(|b_i|+1) &< \prod_{i=1}^{m}\prod_{j=1}^{n}(|a_{ij}|+1)\prod_{i=1}^{m}(|b_i|+1)n \\ &< \prod_{i=1}^{m}\prod_{j=1}^{n}(|a_{ij}|+1)\prod_{i=1}^{m}(|b_i|+1)(mn+1) \leq 2^L\end{aligned}$$

De aqui

$$\begin{aligned}\prod_{i=1}^{m}\prod_{j=1}^{n}(|a_{ij}|+1)\prod_{i=1}^{m}(|b_i|+1)n &< 2^L \\ \prod_{i=1}^{m}\prod_{j=1}^{n}(|a_{ij}|+1)\prod_{i=1}^{m}(|b_i|+1) &< \frac{2^L}{n}\end{aligned}$$

b) Por ser M entero no nulo $\Rightarrow |M| \geq 1$. Por las mismas razones de (a) $M^i \leq \dfrac{2^L}{n}$
Luego

$$v^i = \frac{M^i}{|M|} \leq M^i \cdot 1 \leq \frac{2^L}{n} \quad \forall\, i = 1, 2, \cdots n.$$

Entonces

$$\begin{aligned}||v|| &= \sqrt{\sum_{i=1}^{n}(v^i)^2} \leq \sqrt{\sum_{i=1}^{n}\left(\frac{2^L}{n}\right)^2} \\ &= \sqrt{\left(\frac{2^L}{n}\right)^2\sum_{i=1}^{n}1} = \sqrt{\frac{(2^L)^2}{n^2}n} = \frac{2^L}{\sqrt{n}} < 2^L.\end{aligned}$$

Esto prueba que el poliedro Γ esta acotado.

■

Definición 2.9 Definimos el volumen de la Envoltura convexa en $\mathbb{R}^n$ como:

$$Vol_n = abs\left|\sum_{k=0}^{n}(-1)^k\int_0^{y_k} Vol_{n-1,k}\cdot\frac{y^{n-1}}{y_k^{n-1}}dy\right|$$

donde y_k es la última componente de $(u_k^t, y_k) = (u_{0k}, u_{1k}, \cdots, u_{(n-1)k}, y_k)$, además

$$Vol_{n-1,k} = \frac{1}{(n-1)!} det \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ u_{10} & u_{11} & \cdots & u_{1(k-1)} & u_{1(k+1)} & \cdots & u_{1n} \\ u_{20} & u_{21} & \cdots & u_{2(k-1)} & u_{2(k+1)} & \cdots & u_{2n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ u_{(n-1)0} & u_{(n-1)1} & \cdots & u_{(n-1)(k-1)} & u_{(n-1)(k+1)} & \cdots & u_{(n-1)n} \end{pmatrix}_{n\times n}$$

de esta manera

$$Vol_n = \frac{1}{n!} \left| det \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ u_{10} & u_{11} & \cdots & u_{1(k-1)} & u_{1k} & u_{1(k+1)} & \cdots & u_{1n} \\ u_{20} & u_{21} & \cdots & u_{2(k-1)} & u_{2k} & u_{2(k+1)} & \cdots & u_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ u_{(n-1)0} & u_{(n-1)1} & \cdots & u_{(n-1)(k-1)} & u_{(n-1)k} & u_{(n-1)(k+1)} & \cdots & u_{(n-1)n} \\ y_0 & y_1 & \cdots & y_{k-1} & y_k & y_{k+1} & \cdots & y_n \end{pmatrix}_{(n+1)\times(n+1)} \right|$$

Lema 2.10 *Sea* $Q = \left\{ x \in \mathbb{R}^n / \substack{a_i x < b_i \\ ||x|| < 2^L},\ a_i \in \mathbb{R}^n\ \forall i = 1, 2, .., n \right\}$ *es un poliedro acotado Se cumple*

a) $Q \subset E_0 = B(0, R^2 I)$, *con* $R = 2^L$

b) Si $Q \neq \emptyset$ *entonces* $Vol(Q) > 2^{-(n+1)L}$

Demostración.

a) Iniciamos $E_0 = E(0, R^2 I) = B(0, R)$ con $A_0 = RI$ y $R = 2^L$. Esta parte está probada por (b) del Lema 2.8.

b) Por el Algoritmo: El x_k que se elige es el que no pertenece a Γ, por lo tanto debe existir un $a_{i_k}^t$ tal que no satisface

$$a_{i_k}^t x_k > b_{i_k}. \tag{9}$$

Entonces existe un Hiperplano $H_{a_{i_k}, x_k} = \left\{ x \in \mathbb{R}^n / \ a_{i_k}^t x = a_{i_k}^t x_k \right\}$ que separa Γ y el punto x_k.
Por otro lado sea $x \in Q \Rightarrow a_{i_k}^t x < b_{i_k} < a_{i_k}^t x_k$ (por (9)), luego $x \in \Gamma$.

$$\therefore Q \subset \Gamma \subseteq \mathbb{R}^n \quad (dim(\Gamma) < dim(\mathbb{R}^n))$$

c) Si $Q \neq \emptyset$ entonces como Q es un conjunto abierto ha de contener un punto interior. Se verifica que dicho poliedro tiene $n + 1$ vértices linealmente independiente.
En efecto, si todos los conjuntos de $n + 1$ vértices son linealmente dependiente, entonces el poliedro estaría contenido en un hiperplano de dimensión menor que n. En efecto, como a lo más $Q \subset \Gamma$ tendría n vertices linealmente independiente eso implica que $dim(Q) \leq n - 1$ y como el hiperplano a lo más posee $dim\, H = n - 1$, entonces el poliedro está contenido dentro del hiperplano.
Por otro lado, sea x un punto interior y sea $\epsilon > 0$ la mínima distancia de x a las caras del poliedro.
Evidentemente, $\epsilon > 0$ y la esfera de centro x y radio ϵ está totalmente contenido en el poliedro $\subset$ Hiperplano pero la esfera $\in \mathbb{R}^n$ y H es un hiperplano $\in \mathbb{R}^n$, jamas una esfera está dentro

de un hiperplano si ambos subconjuntos son de $\mathbb{R}^n$ (contradicción).
Sean $v_0, v_1, \cdots, v_n, n+1$ vértices linealmente independiente. Denotemos por C_0 la *capsula convexa* definida por dichos vértices.
Si $x \in C_0$, por una parte verifica $a_i x < b_i$, para todo i
Por otro lado, como $v_i \in C_0 \Rightarrow ||v_i|| < 2^L, \ \forall\, i$
Como $x \in C_0$ es combinación convexa entonces $x = \sum_{i=0}^{n} \alpha_i v_i$ y $\sum_{i=0}^{n} \alpha_i = 1, \ \alpha_i \geq 0.$
Luego

$$\begin{aligned} ||x|| &= \left|\left|\sum_{i=0}^{n} \alpha_i v_i\right|\right| \leq \sum_{i=0}^{n} ||\alpha_i v_i|| = \sum_{i=0}^{n} \alpha_i ||v_i|| \\ &< \sum_{i=0}^{n} \alpha_i 2^L = 2^L \left(\sum_{i=0}^{n} \alpha_i\right) = 2^L \end{aligned}$$

Esto prueba que

$$int(C_0) \subset Q \Rightarrow Vol(Q) > Vol(C_0) \tag{10}$$

Por otro lado

$$Vol(C_0) = \frac{1}{n!}\left| det \begin{pmatrix} v_0 & v_1 & v_2 & \cdots & v_n \\ & & & & \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix}_{(n+1)\times(n+1)} \right|$$

y por ser $v_j^i = \dfrac{M_j^i}{M_j}$, se tiene

$$Vol(C_0) = \left(\frac{1}{n!}\right)\left(\frac{1}{|M_0||M_1|\cdots|M_n|}\right)\left[det \begin{pmatrix} M_0^{'} & M_1^{'} & \cdots & M_n^{'} \\ \vdots & \vdots & & \vdots \\ M_0^n & M_1^n & \cdots & M_n^n \\ M_0 & M_1 & \cdots & M_n \end{pmatrix} \right]$$

Notemos que el valor absoluto de la determinante es entero y diferente de cero (pues los v_i son linealmente independiente) entonces es mayor o igual a 1 y como los $|M_i| < \dfrac{2^L}{n}$ $\forall\, i = 1, \cdots n$; luego $\dfrac{1}{|M_j|} > \dfrac{n}{2^L}$. Entonces

$$\begin{aligned} Vol(C_0) &= \frac{1}{n!}\cdot\frac{1}{|M_0||M_1|\cdots|M_n|}\left| det \begin{pmatrix} M_0^{'} & M_1^{'} & \cdots & M_n^{'} \\ \vdots & \vdots & & \vdots \\ M_0^n & M_1^n & \cdots & M_n^n \\ M_0 & M_1 & \cdots & M_n \end{pmatrix} \right| \geq \frac{1}{n!}\cdot\frac{1}{|M_0||M_1|\cdots|M_n|} \\ &> \frac{1}{n!}\cdot\frac{n\cdot n\cdots n}{2^L\cdot 2^L\cdots 2^L} = \frac{1}{n!}\cdot\frac{n^{n+1}}{(2^L)^{n+1}} > \frac{1}{2^{L(n+1)}} = 2^{-L(n+1)} \end{aligned} \tag{11}$$

De (10) y (11) se tiene

$$Vol(Q) > 2^{-L(n+1)}.$$

■

Observación 2.11 *En caso de que el poliedro*

$$K = \left\{x \in \mathbb{R}^n / \ a_i^t x < b_i, \ i = 1, 2, \cdots, m; \ a_i \in \mathbb{Z}^n, \ \ b_i \in \mathbb{Z}\right\}$$

no fuera acotado, bastará añadir las restricciones

$$|x_i| < \frac{2^L}{n}, \qquad i = 1, 2, \cdots, n.$$

Lema 2.12 *Para todo k*

$$E_k \cap \left\{x \in \mathbb{R}^n / \ -a_{i_k}^t (x - x_k) > 0, \ a_{i_k}, \, x_k \in \mathbb{R}^n\right\} \subset E_{k+1}.$$

Demostración. Siguiendo los mismos pasos de la página 3 y 4, podemos decir que existe una transformación Afin, tal que E_k puede ser transformado en la esfera de radio 1 centrado en el origen (que deja dicha esfera invariante), el vector $-a_{i_k}$ se puede transformar en $(+1, 0, \cdots, 0)^t$. Por la propiedades de dichas transformaciones en $\mathbb{R}^n$, podemos realizar la demostración con dichos elementos siguiendo los pasos dados en la páginas 3 y 4.

$$\begin{aligned} x_{k+1} &= \left(\frac{1}{n+1}, 0, \cdots, 0\right) \\ A_{k+1} &= \frac{n^2}{n^2 - 1} diag\left(\frac{n-1}{n+1}, 1, \cdots, 1\right). \end{aligned}$$

Sea $x \in E_k \cap \left\{x \in \mathbb{R}^n / \ -a_{i_k}^t (x - x_k) > 0, \ a_{i_k}, \, x_k \in \mathbb{R}^n\right\}$, entonces $x \in E_k$, luego $||x||^2 \leq 1$. Como $x_k = 0$, podemos operar

$$0 < -a_{i_k}(x - x_{1k}) = 1(x_1 - 0) = 1x_1 = x_1.$$

Ahora probamos que $x \in E_{k+1}$, para esto hacemos $x = (x_1, \bar{x})$

$$\begin{aligned} (x - x_{k+1})^t A_{k+1}^{-1} (x - x_{k+1}) &= \frac{n^2 - 1}{n^2} \left(x_i - \frac{1}{n+1}, \bar{x}\right)^t \begin{pmatrix} \frac{n+1}{n-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \left(x_1 - \frac{1}{n+1}, \bar{x}\right) \\ &= \frac{n^2 - 1}{n^2} \left[\left(x_1 - \frac{1}{n+1}, \bar{x}\right)^t \begin{pmatrix} \frac{n+1}{n-1} \cdot \left(x_1 - \frac{1}{n+1}\right) \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} \right] \\ &= \frac{n^2 - 1}{n^2} \left[\frac{n+1}{n-1} \left(x_1 - \frac{1}{n+1}\right)^2 + \bar{x} \cdot \bar{x} \right] \\ &= \frac{(n-1)}{n^2} (n+1) \cdot \frac{(n+1)}{(n-1)} \cdot \left(x_1 - \frac{1}{n+1}\right)^2 + \frac{n^2 - 1}{n^2} ||\bar{x}||^2 \\ &= \frac{(n+1)^2}{n^2} \cdot \frac{1}{(n+1)^2} \left[(n+1)x_1 - 1\right]^2 + \frac{(n^2 - 1)}{n^2} ||\bar{x}||^2 \end{aligned} \tag{12}$$

Sabemos que $||x|| \leq 1$, entonces

$$||\bar{x}|| \ \ \leq \ \ 1 - x_1^2.$$

En (12), obtenemos

$$
\begin{aligned}
(x-x_{k+1})^t A_{k+1}^{-1}(x-x_{k+1}) &\leq \frac{1}{n^2}((n+1)x_1-1)^2+\frac{(n^2-1)}{n^2}\cdot(1-x_1^2)\\
&= \frac{1}{n^2}\left[(n+1)^2x_1^2-2(n+1)x_1+1\right]+\frac{n^2-1}{n^2}-\frac{(n^2-1)}{n^2}\cdot x_1^2\\
&= \frac{(n+1)^2}{n^2}x_1^2-\frac{2(n+1)}{n^2}x_1+\frac{1}{n^2}+1-\frac{1}{n^2}-\frac{(n-1)(n+1)}{n^2}\cdot x_1^2\\
&= \left(\frac{n+1}{n^2}\right)x_1^2(n+1-(n-1))-\frac{2(n+1)}{n^2}x_1+1\\
&= \frac{2(n+1)}{n^2}(x_1^2-x_1)+1\leq 1.
\end{aligned}
$$

Por otro lado, si consideramos

$$
\begin{aligned}
0\leq x_1\leq 1 \quad &\Rightarrow \quad 0\leq x_1^2\leq x_1\leq 1\\
&\Rightarrow \quad x_1^2-x_1\leq 0 \quad \text{y} \quad 2\left(\frac{n+1}{n\cdot n}\right)=2\left(\frac{1}{n}+\frac{1}{n^2}\right).
\end{aligned}
$$

Como

$$
\begin{aligned}
n>1 \quad &\Rightarrow \quad \frac{1}{n}<1 \quad \text{y} \quad \frac{1}{n^2}<\frac{1}{n}<1\\
&\Rightarrow \quad \frac{1}{n}+\frac{1}{n^2}<\frac{1}{n}+\frac{1}{n}
\end{aligned}
$$

Luego

$$
\begin{aligned}
0 \;&<\; \frac{2(n+1)}{n^2} \;<\; \frac{4}{n} \;<\; 1 \quad \forall\, n\geq 4\\
1 \;&>\; 0 \;>\; \frac{2(n+1)}{n^2}(x_1^2-x_1) \;>\; (x_1^2-x_1).
\end{aligned}
$$

Esto prueba que $x\in E_{k+1}=E(x_{k+1},A_{k+1})$. ■

Definición 2.13 Sea $T:\mathbb{R}^n\to\mathbb{R}^n$ una transformación afín definida como $Tx=Ax+b$, $A\in M_{n\times n}$ y $b\in\mathbb{R}^n$ y la imagen de un conjunto γ

$$T(\gamma)=\{y\in\mathbb{R}^n/\ y=Tx=Ax+b,\ si\ x\in\gamma\}.$$

Definición 2.14 El volumen de un conjunto $\gamma\subseteq\mathbb{R}^n$, lo denotamos por $Vol(\gamma)$ y se define como:

$$Vol(\gamma)=\int_{x\in\gamma}dx$$

de modo que

$$Vol(T(\gamma))=\int_{y\in T(\gamma)}dy=\int_{x\in\gamma}|det(J(x))|dx$$

$J(x)$ es el Jacobiano de $T(x)$

$$
\begin{aligned}
Vol(T(\gamma)) &= \int_{x\in\gamma}|det(A)|dx=|det(A)|\int_{x\in\gamma}dx\\
&= |det(A)|Vol(\gamma)\\
Vol(T(\gamma)) &= |det(A)|Vol(\gamma).
\end{aligned}
$$

Observación 2.15 De aqui, podemos deducir que el volumen de una elipsoide $E(c, Q)$ que es la imagen de una esfera unitaria $B(0, 1)$ a travez de una transformación afín $T = Lx$ entonces

$$E(c, Q) = L(B(0, 1)) + c' \text{ entonces}$$

$$\begin{aligned} Vol(c, Q) &= |del(L)|Vol(B(0, 1)) \quad \text{ó} \\ Vol(c, Q) &= \sqrt{det(Q)} \cdot Vol(B(0, 1)) \end{aligned}$$

donde $Q = LL^t$.

Observación 2.16 Si R es una matriz de rotación definida como

$$R = \frac{2(u - ||u||e_1)(u + ||u||e_1)^t}{u + ||u||e_1} - I, \; e_1 = (1, 0, \cdots, 0), \; u \in \mathbb{R}^n.$$

Entonces $R^t R = I$.

Por otro lado, si D es simétrica y definida positiva entonces posee inversa D^{-1} y puede definir una elipsoide. Además se puede descomponer en:

$$D^{-1} = D^{-\frac{1}{2}} \cdot D^{-\frac{1}{2}} \text{ y } D = D^{\frac{1}{2}} \cdot D^{\frac{1}{2}}.$$

Entonces, dadas las elipsoides

$$E_0 = E(0, R^t R) = E(0, I) \text{ y } E_1 = E(x_0, D).$$

definimos $S(x)$ una transformación afín como: $S(x) = D^{-\frac{1}{2}}(x - x_0)$.
Además, $W(x) = RS(x)$ es otra transformación afín y $W(x) = RD^{-\frac{1}{2}}(x - x_0)$.
Si $x \in E$, entonces

$$\begin{aligned} ||S(x)|| &= S^t(x) \cdot S(x) \\ &= \left[D^{-\frac{1}{2}}(x - x_0)\right]^t \left[D^{-\frac{1}{2}}(x - x_0)\right] \\ &= (x - x_0)^t D^{-\frac{1}{2}} \cdot D^{-\frac{1}{2}}(x - x_0) \\ &= (x - x_0)^t D^{-1}(x - x_0) \\ &\leq 1 \end{aligned}$$

Luego,

$$S(x) \in B(0, 1) \text{ para todo } x \in E.$$

Sea $y = S(x) \in B(0, 1)$

$$\begin{aligned} R(B(0, 1)) &= \{Ry \in \mathbb{R} \,/\, y \in B(0, 1)\} \;=\; \{z = Ry \,/\, y \in B(0, 1)\} \\ &= \left\{z \,/\, R^{-1}z \in B(0, 1)\right\} \;=\; \left\{z \,/\, ||R^{-1}z||^2 \leq 1^2\right\} \\ &= \left\{z \,/\, (R^{-1}z)^t(R^{-1}z) \leq 1\right\} \;=\; \left\{z \,/\, (z)^t(R^{-t}R^{-1})(z) \leq 1\right\} \\ &= \left\{z \,/\, (z)^t(RR^t)^{-1}z \leq 1\right\} \;=\; E_0 = E(0, RR^t). \end{aligned}$$

Esto prueba que

$$W(E_1) = E_0.$$

Por otro lado, definimos la transformación afín lineal $F : \mathbb{R}^n \to \mathbb{R}^n$ como $F(x) = D^{-\frac{1}{2}}(x - x_0)$. Si $x \in F$, entonces

$$\begin{aligned}
||F(x)|| &= F^t(x) \cdot F(x) \\
&= \left[D^{-\frac{1}{2}}(x - x_0)\right]^t \left(D^{-\frac{1}{2}}(x - x_0)\right) \\
&= \left[\left(D^{-\frac{1}{2}}\right)^t ((x - x_0)^t)^t\right]^t \left(D^{-\frac{1}{2}}(x - x_0)\right) \\
&= \left((x - x_0)^t D^{-\frac{1}{2}}\right) \left(D^{-\frac{1}{2}}(x - x_0)\right) \\
&= (x - x_0)^t D^{-\frac{1}{2}} D^{-\frac{1}{2}}(x - x_0) \\
&= (x - x_0)^t D^{-1}(x - x_0) \\
&\leq 1.
\end{aligned}$$

Luego,

$$F(x) \in B(0, 1) \text{ para todo } x \in F.$$

Esto prueba que

$$F(E_1) = E_0.$$

Finalmente $E_1 = F^{-1}(E_0)$, entonces.

$$\begin{aligned}
Vol(E_1) &= Vol(F^{-1}(E_0)) \;=\; |det\left(D^{\frac{1}{2}}\right)|Vol(E_0) \\
Vol(E_1) &= \sqrt{det(D)}Vol(E_0).
\end{aligned}$$

Lema 2.17 *Se cumple*

a) $Vol(E_0) < 2^{(L+1)n}$

b) $\forall k,\ Vol(E_{k+1}) = c_n Vol(E_k)$, *siendo* $c_n < 2^{-\frac{1}{2(n+1)}}$

Demostración.

a) Consideremos

$$\begin{aligned}
E_0 &= E(0, 2^{2L}I) \;=\; \left\{x \,/\, x^t \left(2^{2L}I\right)^{-1} x \,\leq\, 1\right\} \\
2^{2L}I &= \left(2^L I\right)\left(2^L I\right) \;=\; \left\{x \,/\, x^t \left(2^{-2L}I\right) x \,\leq\, 1\right\} \\
&= \left\{x \,/\, 2^{-2L}(x^t I x) \,\leq\, 1\right\} \;=\; \left\{x \,/\, x^t x \,\leq\, 2^{2L}\right\} \\
&= \left\{x \,/\, ||x||^2 \leq 2^{2L}\right\} \;=\; \left\{x \,/\, ||x|| \,\leq\, 2^L\right\} \;=\; B(0, 2^L).
\end{aligned}$$

Esta bola está incluido en un cubo de lado $2 \cdot 2^L$ es decir de lado $\ell = 2^{L+1}$ y cuyo volumen es ℓ^n

$$\begin{aligned}
Vol(cubo) &= 2^{n(L+1)} \\
Vol(E_0) &< Vol(cubo) \;=\; 2^{n(L+1)}.
\end{aligned}$$

b) Razonemos como en el lema anterior
E_k es la esfera centrada en el origen y de radio 1 y $a_{i_k} = (-1, 0, \cdots, 0)$. Tendremos

$$\begin{aligned}
Vol(E_{k+1}) &= \sqrt{det(A_{k+1})} \cdot Vol(E_0) \\
Vol(E_k) &= \sqrt{det(A_k)} \cdot Vol(E_0).
\end{aligned}$$

Entonces

$$Vol(E_{k+1}) = \left[\frac{det(A_{k+1})}{det(A_k)}\right]^{\frac{1}{2}} Vol(E_k)$$

y

$$Vol(E_{k+1}) \leq [det(A_{k+1})]^{\frac{1}{2}} \cdot Vol(E_k) = c_n Vol(E_k)$$

$$\text{Como } A_{k+1} = \frac{n^2}{n^2-1} diag\left(\frac{n-1}{n+1}, 1, \cdots, 1\right) = \begin{pmatrix} \frac{n^2}{n^2-1}\cdot\frac{n-1}{n+1} & & & \\ & \frac{n^2}{n^2-1} & & 0 \\ & 0 & \ddots & \\ & & & \frac{n^2}{n^2-1} \end{pmatrix}.$$

Entonces

$$\begin{aligned} c_n &= [det(A_{k+1})]^2 = \left[\left(\frac{n^2}{n^2-1}\right)^n \cdot \left(\frac{n-1}{n+1}\right)\right] \\ &= \left[\left(\frac{n^2}{n^2-1}\right)^{n-1} \cdot \left(\frac{n^2}{n^2-1}\right) \cdot \left(\frac{n-1}{n+1}\right)\right]^{\frac{1}{2}} \\ &= \left[\left(\frac{n^2}{n^2-1}\right)^{n-1} \cdot \left(\frac{n^2}{(n-1)(n+1)}\right) \cdot \left(\frac{n-1}{n+1}\right)\right]^{\frac{1}{2}} = \left[\left(\frac{n^2}{n^2-1}\right)^{n-1} \cdot \left(\frac{n}{n+1}\right)^2\right]^{\frac{1}{2}} \\ &= \left(\frac{n}{n+1}\right) \cdot \left(\frac{n^2}{n^2-1}\right)^{\frac{n-1}{2}}. \end{aligned}$$

Usando propiedad $1 + z \leq \exp(z)$ se obtiene

$$\begin{aligned} \frac{n}{n+1} &= 1 - \frac{1}{n+1} < \exp\left(-\frac{1}{n+1}\right) \\ \frac{n^2}{n^2-1} &= 1 + \frac{1}{n^2-1} < \exp\left(\frac{1}{n^2-1}\right). \end{aligned}$$

Luego

$$\begin{aligned} c_n &< \exp\left(-\frac{1}{n+1}\right) \cdot \exp\left(\frac{1}{n^2-1}\right)^{\frac{n-1}{2}} = \exp\left(\frac{n-1}{2(n^2-1)} - \frac{1}{n+1}\right) \\ c_n &< \exp\left(-\frac{1}{2(n+1)}\right) < 2^{-\frac{1}{2(n+1)}}. \end{aligned}$$

■

Teorema 2.18
Si el algoritmo se detiene, x_k es una solución de (1) ($F \neq \emptyset$)
Si el algoritmo no se detiene en $4(n+1)^2 L$ pasos, entonces (1) no tiene solución (es decir $F = \emptyset$).

$$Q = \left\{ x \in \mathbb{R}^n \;/\; \begin{matrix} Ax < b \\ ||x|| < 2^L \end{matrix}, A \in \mathbb{Z}_{n\times n}, b \in \mathbb{Z}^n, x \in \mathbb{R}^n \right\}.$$

Demostración. Supongamos que $F \neq \emptyset \Rightarrow Q \neq \emptyset$ es decir existe $x \in F$ y el algoritmo no ha proporcionado en k pasos con $k \geq 4(n+1)^2 L$.
Por el Lema 2.17

$$\begin{aligned} Vol(E_k) &= c_n Vol(E_{k-1}) = \cdots = c_n^k Vol(E_0) \\ &< 2^{-\frac{k}{2(n+1)}} \cdot 2^{n(L+1)} \leq 2^{-\frac{4(n+1)^2 L}{2(n+1)}} \cdot 2^{n(L+1)} \\ &= 2^{-(n+1)L} \cdot 2^{-(n+1)L} \cdot 2^{n(L+1)} \\ &= 2^{-(n+1)L} \cdot 2^{n-L} < 2^{-(n+1)L} \quad \textit{pues } n < L. \end{aligned}$$

Por otro lado los lemas implican

$$Q \subset E_k \Rightarrow Vol(Q) < 2^{-(n+1)L}.$$

Sin embargo, si $Q \neq \emptyset$ por el Lema 2.10 se tiene

$$Vol(Q) > 2^{-(n+1)L}$$

lo cual es una contradicción. ■

2.2. Solución de un problema de programación lineal (P.P.L)

Sea el $(P.P.L)$

$$\left.\begin{array}{r} \text{mín} \quad c^t x \\ s.a \quad\quad \\ Ax \geq b \\ x \geq 0 \end{array}\right\} (P)$$

donde $A \in M_{m\times n}$; c, $x \in \mathbb{R}^n$; $b \in \mathbb{R}^m$ y por el otro lado su dual

$$\left.\begin{array}{r} \text{máx} \quad b^t y \\ s.a \quad\quad \\ A^t y \geq c \\ y \geq 0 \end{array}\right\} (D)$$

donde $y \in \mathbb{R}^m$.
Por teoría de dualidad sabemos que si $\bar{x}, \bar{y}$ son factibles en (P) y (D) y si $c^t\bar{x} = b^t\bar{y}$ entonces $\bar{x}$ y $\bar{y}$ son soluciones en (P) y (D).
Consideremos el siguiente sistema

$$\left.\begin{array}{c} c^t x = b^t y \\ Ax \geq b \\ A^t y \leq c \\ x \geq 0,\, y \geq 0 \end{array}\right\} (C)$$

Si la solución de (P) existe y es finita, entonces para hallarla basta calcular una solución de (C).
Por último, observemos que el algoritmo del elipsoide se aplica a un sistema con desigualdades estrictas. En el caso de que esto no suceda, como por ejemplo en el problema (C), el sistema se puede transformar en otro con desigualdades estrictas añadiendo perturbaciones. La validez de este procedimiento queda asegurada por el siguiente lema.

Lema 2.19
El sistema

$$a_i^t x \leq b_i \quad (i = 1, 2, \cdots m,\, x \in \mathbb{R}^n,\, a_i \in \mathbb{Z}^n,\, b_i \in \mathbb{Z}) \tag{13}$$

tiene solución si y solo si el sistema

$$a_i^t x < b_i + \epsilon \quad (i = 1, 2, \cdots, m,\, a_i \in \mathbb{Z}^n,\, b_i \in \mathbb{Z}) \tag{14}$$

tiene una solución. (Donde $\epsilon = 2^{-2L}$)

Demostración.

($\Rightarrow$) Si x satisface $a_i x \leq b_i$, entonces también satisface (14).

($\Leftarrow$) Sea x_0 solución del sistema (14). Consideremos el conjunto de vectores

$$I = \left\{ a_i \in \mathbb{Z}^n \,/\, b_i \leq a_i^t x_0 < b_i + \epsilon,\, x_0 \in \mathbb{R}^n,\, b_i \in \mathbb{Z} \right\}.$$

Podemos suponer sin perdida de generalidad que

$$a_j = \sum_{a_i \in I} \beta_{ji} a_i,\ \forall j,\ \beta_{ji} \text{ constantes.}$$

En efecto, si a_j es linealmente independiente de los vectores $a_i \in I$, entonces el sistema

$$\left\{ \begin{array}{c} a_i^t z = 0,\ i \in I,\ z \in \mathbb{R}^n \\ a_j^t z = 1 \end{array} \right. \quad \Leftrightarrow \left(\begin{array}{c} A^t \\ a_j^t \end{array} \right) z = \left(\begin{array}{c} 0 \\ \vdots \\ 0 \\ 1 \end{array} \right)$$

tiene una solución z_0
Tomamos $x_1 = x_0 + \lambda z_0$ para λ suficientemente pequeño
entonces

$$a_i^t x_1 = a_i^t (x_0 + \lambda z_0) = a_i^t x_0 + \lambda a_i^t z_0$$

como $b_i \leq a_i^t x_0 < b_i + \epsilon$.
Luego existe $\lambda \in \mathbb{R}$ tal que

$$b_i < b_i + \lambda a_i^t z_0 \leq a_i^t x_0 + \lambda a_i^t z_0 \leq a_i^t x_0 + \lambda < b_i + \epsilon$$

y donde

$$\begin{array}{ll} a_i^t z_0 = 0, & \text{si} \quad i \in I \\ a_i^t z_0 = 1, & \text{si} \quad i = j \end{array}$$

un λ tal que $\lambda < \epsilon$, entonces

$$\begin{array}{rcccl} b_i & \leq & a_i^t x_0 + \lambda & < & b_i + \epsilon \\ b_i & \leq & a_i x_i & < & b_i + \epsilon \end{array}$$

Con esto probamos que $x_1 \in I$ y $a_j \in I$.
Este procedimiento lo podemos repetir hasta m veces. Asi pues

$$a_j = \sum_{a_i \in I'} \beta_{ji} a_i,\ \forall j \text{ para algún } I' \subset I$$

de vectoreslinealmente independiente de I.
Por la regla de Cramer, los coeficientes β_{ji} son cocientes de determinantes de valores absolutos menores que 2^L (Lema 2.8)
Escribamos $\beta_{ji} = \dfrac{M_{ij}}{|M|}$ y consideremos $\bar{x}$ una solución $\bar{x}$ del sistema

$$a_i^t x = b_i, \; a_i \in I^{'}$$

Para cada j tendremos:

$$\begin{aligned}
|M|\left(a_j^t \bar{x} - b_j\right) &= |M| \left(\sum_{a_i \in I'} \frac{M_{ij}}{|M|} a_i^t \bar{x} - b_j \right) \\
&= \sum_{a_i \in I'} M_{ij} a_i^t \bar{x} - |M| b_j \\
&= \sum_{a_i \in I'} M_{ij} b_i - |M| b_j \\
&= -\sum M_{ij}\left(a_i^t x_0 - b_i\right) \; + \; |M|\left(a_j^t x_0 - b_j\right) \\
&< \epsilon\left(-\sum M_{ij} + |M|\right) \; \leq \; \epsilon\left(\sum |M_{ij}| + |M|\right) \\
&< 2^{-2L}(m+1)\cdot 2^L \; < \; 2^{-2L}\cdot 2^L \cdot 2^L \; = \; 1.
\end{aligned}$$

Pero como $2^L > m+1$ entonces

$$|M|(a_j^t \bar{x} - b_j) < 1.$$

Por otro lado, por la definición de x los denominadores de sus componentes dividen exactamente, es decir debe ser entero, entonces

$$|M|(a_j^t \bar{x} - b_j)$$

debe ser entero y menor que 1. Por lo tanto

$$(a_j^t \bar{x} - b_j) \leq 0.$$

Luego la ecuación (1) tiene solución. ■
Observe que la construcción de x es a partir de x_0 en un número polinomial de pasos.

3. Resultados

El algoritmo del elipsoide resuelve el problema de feasibilidad de un conjunto poliédrico racional en tiempo polinomial. El algoritmo establece la existencia o no de un punto en el poliedro de un modo satisfactoriamente teórico.

4. Discusión

Se debe notar que en cada iteración el algoritmo del elipsoide necesita identificar la restricción o desigualdad que es “violada”. Esta identificación es equivalente a resolver un problema de separación es decir hallar el hiperplano que separa al poliedro. Aqui hemos asumido que el número de restricciones que describen al poliedro $\mathcal{K}$ no es exponencial y que pueden ser “chequeadas” cada una de ellas. ¿Que pasaría si el número de restricciones que describen al poliedro sea de orden exponencial en n; el algoritmo seguiría siendo polinomial?. Podriamos hacer otra pregunta, ¿si para un poliedro racional, el problema de feasibilidad puede ser resuelto en tiempo polinomial, entonces el problema de separación para el poliedro puede ser resuelto también en tiempo polinomial?

5. Conclusión

Ha sido posible presentar el algoritmo del elipsoide que resuelve el problema de feasibilidad para un poliedro racional
Como una aplicación del algoritmo del elipsoide se tiene la solución de un problema de programación lineal cuyo conjunto factible es un poliedro racional.

Referencias bibliográficas

[1] Karmarkar, N. (1984). A New Polinomial time-algorithm for linear programing *Combinatórica*, 4(4), 373-395.

[2] Khachiyan, L. (1980). Algorithm Linear Programing. *Computational Mathematics y Mathematical Physics*, 20(1), 53-72.

[3] Mora, H. (1992). El Método de Karmarka. 8vo Coloquio Distrital de Matemática y Estadística. Coloquio llevado a cabo en la Universidad Nacional de Colombia. Colombia.

[4] Shor, Y., y Nemirovskii, A. (1988). A new polynomial algorithm for linear programming, *Soviet mathematics - doklady*, 37, 264-269.

[5] Flores, J. (2010). *Estudio del Algoritmo Proyectivo de Karmarkar y sus Aplicaciones en la Ingeniería*. Tesis de maestría en ciencias, mención Matemáticas Aplicadas. Universidad Nacional de Ingeniería, Perú.

[6] Lang, S. (1980). *Algebra Lineal*. México: Mc Graw Hill. 1980.