PUNTO Y LÍNEA SOBRE EL PLANO

Ecuaciones lineales diofantinas aplicadas a programas lineales enteros

Iñaki Liendo
Coloquio de matemáticas
8 de septiembre de 2025

1. MOTIVACIÓN

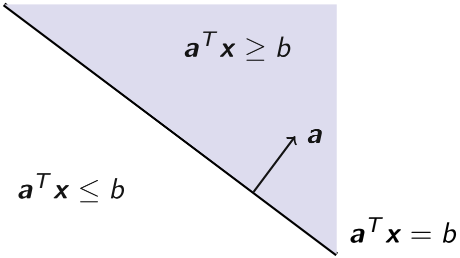
Definición

Sea $\boldsymbol{a} \in \mathbb{R}^n$ un vector no nulo y sea $b \in \mathbb{R}$ un escalar. Llamamos **hiperplano afino** al conjunto de vectores $\boldsymbol{x} \in \mathbb{R}^n$ que satisfacen $\boldsymbol{a}^T \boldsymbol{x} = b$. Llamamos **semi-espacios afinos** a los conjuntos de vectores $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$ que satisfacen $\boldsymbol{a}^T \boldsymbol{x} \geq b$ y $\boldsymbol{a}^T \boldsymbol{y} \leq b$.

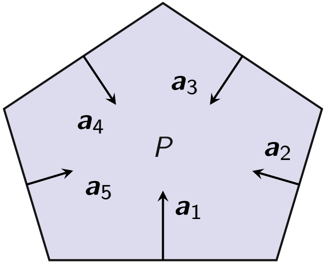
Definición

Sea $A \in \mathbb{R}^{m \times n}$ una matriz con renglones linealmente independientes y sea $\boldsymbol{b} \in \mathbb{R}^m$ un vector. Llamamos **poliedro** al conjunto definido por

$$P := \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} \leq \boldsymbol{b}\} = \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}_i^T \boldsymbol{x} \leq b_i, 1 \leq i \leq m\}.$$



$\boldsymbol{a}^T\boldsymbol{x} \geq b$
$\boldsymbol{a}$
$\boldsymbol{a}^T\boldsymbol{x} \leq b$
$\boldsymbol{a}^T\boldsymbol{x} = b$



$\boldsymbol{a}_3$
$\boldsymbol{a}_4$
P
$\boldsymbol{a}_2$
$\boldsymbol{a}_5$
$\boldsymbol{a}_1$

Definición

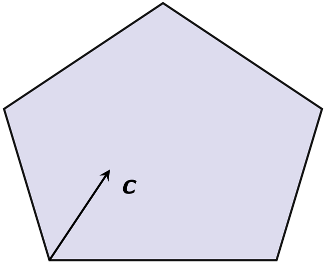
Sea $P \subseteq \mathbb{R}^m$ un poliedro y sea $\boldsymbol{c} \in \mathbb{R}^n$ un vector. Llamamos **problema lineal** al problema de maximización

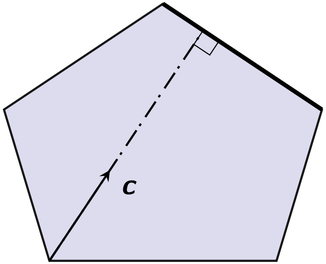
$$z^* := \max_{\boldsymbol{x}} \{\boldsymbol{c}^T \boldsymbol{x} : \boldsymbol{x} \in P\}.$$

Nota: Un problema lineal puede ser infactible porque P es vacío (y entonces z^* no está bien definida) o puede ser no acotado porque $z^* = \infty$.

Teorema

Supongamos que el valor óptimo z^* existe y es finito. Entonces el conjunto de soluciones óptimas $\{\boldsymbol{x}^* \in P : \boldsymbol{c}^T \boldsymbol{x}^* = z^*\}$ contiene al menos un vértice de P.


c


c

Definición

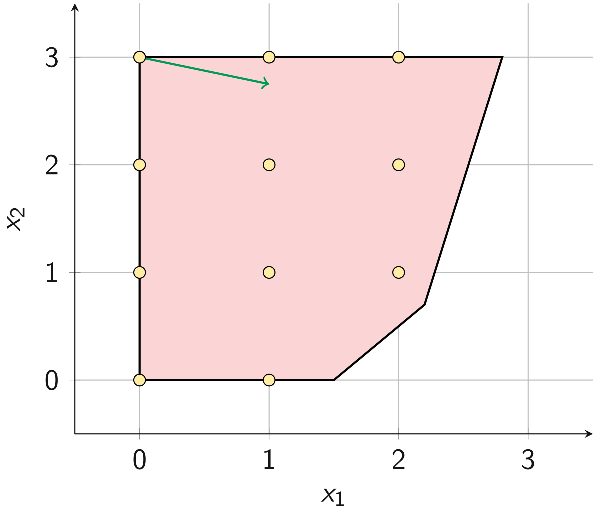
Al problema lineal

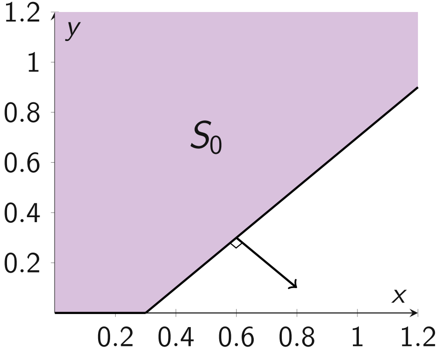
$$z^* := \max_{\boldsymbol{x}}\{\boldsymbol{c}^T\boldsymbol{x} : \boldsymbol{x} \in P\}.$$

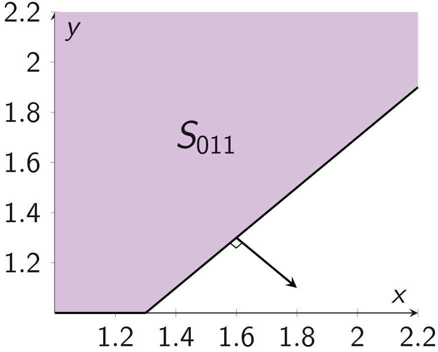
lo llamamos **problema relajado** del **problema lineal entero**

$$z^*_{\mathrm{PE}} := \max_{\boldsymbol{x}}\{\boldsymbol{c}^T\boldsymbol{x} : \boldsymbol{x} \in P \cap \mathbb{Z}^n\}.$$

Nota: Como $P \cap \mathbb{Z}^n \subseteq P$, tenemos $z^*_{\mathrm{PE}} \leq z^*$.


3
2
1
0
0
1
2
3
x_1
x_2


1.2
1
0.8
0.6
0.4
0.2
y
S0
x
0.2
0.4
0.6
0.8
1
1.2


2.2
2
1.8
1.6
1.4
1.2
y
S_{011}
x
1.2
1.4
1.6
1.8
2
2.2

Ramificación y Acotamiento genera la cadena de subproblemas autosimilares

$$S_0, S_{011}, S_{01111}, S_{0111111}, \ldots,$$

y este método jamás terminará con una solución.

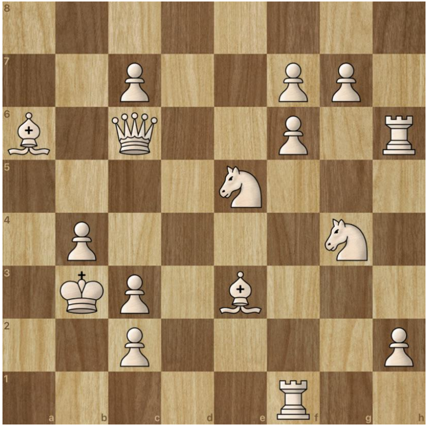
En general, Ramificación y Acotamiento es ineficiente (o incluso falla) cuando una restricción del problema es ortogonal al vector objetivo. La instancia minimal que reproduce esta ineficiencia es

$$\max_{\boldsymbol{x} \in \mathbb{Z}^n} \quad \boldsymbol{p}^T \boldsymbol{x}, \tag{1a}$$

$$\text{s.a.} \quad \boldsymbol{p}^T \boldsymbol{x} \leq u, \tag{1b}$$

$$\boldsymbol{x} \geq \mathbf{0}.$$

Aún más general, Ramificación y Acotamiento es ineficiente cuando el problema contiene múltiples simetrías:



- Sin contar rotaciones o reflexiones del tablero, cada solución tiene al menos

$$8! \times (2!)^3 \times 1! \times 1! = 322{,}560$$

  soluciones equivalentes.
- Contanto rotaciones y reflexiones del tablero, cada solución tiene al menos

$$4 \times 2 \times 322{,}560 = 2{,}580{,}480$$

  soluciones equivalentes.
- Las simetrías dependen de la formulación que utilicemos. Si la formulación induce a que las soluciones equivalentes se encuentren en árboles disjuntos, entonces estos jamás serán podados y Ramificación y Acotamiento es más ineficiente.
- ¿Cuántas soluciones distintas (no equivalentes) existen?

2. FUNDAMENTOS

Definición

Decimos que un vector $\boldsymbol{v} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ es **esencialmente entero** si existen un vector $\boldsymbol{w} \in \mathbb{Z}^n$ y un escalar $m \neq 0$ tales que $\boldsymbol{v} = m\boldsymbol{w}$. Además, decimos que $\boldsymbol{w}$ es el **múltiplo coprimo** de $\boldsymbol{v}$ si sus entradas son coprimas y si su primera entrada no nula es positiva.

Ejemplo

El vector $(-\sqrt{2}, 1/\sqrt{2}) = 2\sqrt{2}(-2, 1)$ es esencialmente entero y $(2, -1)$ es su múltiplo coprimo. En contraste, el vector $\left(\sqrt{2}, \sqrt{3}\right)$ no es esencialmente entero (¿por qué?).

- **Ejercicio:** Todo vector racional $\boldsymbol{v} \in \mathbb{Q}^n$ no nulo es esencialmente entero.
- $\implies$ Todo número representable en un sistema de aritmética finita es esencialmente entero.

Definición

Sea $\boldsymbol{v} \in \mathbb{R}^n$ un vector esencialmente entero y sea $t \in \mathbb{R}$ un escalar. Decimos que su hiperplano afino asociado

$$H_{\boldsymbol{v},t} := \ker\left\{\boldsymbol{x} \mapsto \boldsymbol{v}^T\boldsymbol{x}\right\} + t\boldsymbol{v} = \{\boldsymbol{v}^\perp + t\boldsymbol{v} : \boldsymbol{v}^T\boldsymbol{v}^\perp = 0\}$$

es una **capa entera** si contiene al menos un punto entero.

Teorema de cobertura

Sea $\boldsymbol{v} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{w}$ su múltiplo coprimo. Entonces la familia de capas enteras $\{H_{\boldsymbol{w},k\|\boldsymbol{w}\|^{-2}} : k \in \mathbb{Z}\}$ cubre a $\mathbb{Z}^n$.

Lema de utilidad (*)

Sea $\boldsymbol{v} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{w}$ su múltiplo coprimo. Entonces $\boldsymbol{w}^T \boldsymbol{x} = k$ para todo $\boldsymbol{x} \in H_{\boldsymbol{w}, k\|\boldsymbol{w}\|^{-2}}$.

Lema de satisfacción (*)

Sea $\boldsymbol{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{q}$ su múltiplo coprimo, de manera que $\boldsymbol{p} = m\boldsymbol{q}$ para algún escalar $m \neq 0$. Entonces la primera capa entera $H_{\boldsymbol{q}, \eta\|\boldsymbol{q}\|^{-2}}$ que satisface la restricción $\boldsymbol{p}^T \boldsymbol{x} \leq u$ está parametrizada por

$$\eta := \begin{cases} \lceil u/m \rceil, & m < 0, \\ \lfloor u/m \rfloor, & m > 0. \end{cases}$$

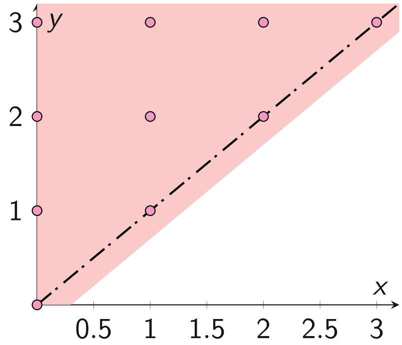
Teorema de infactibilidad (*)

Sea $\boldsymbol{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{q}$ su múltiplo coprimo. Entonces el problema (1) es infactible si y solo si $\boldsymbol{q} \geq \mathbf{0}$ y el lado derecho u de (1b) es negativo.

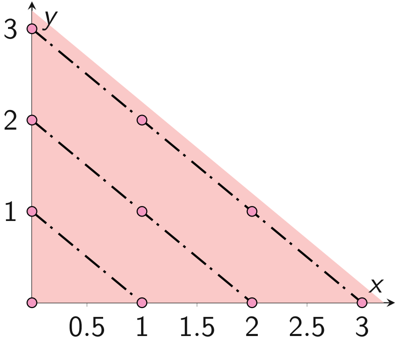
Teorema de factibilidad

Sea $\boldsymbol{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{q}$ su múltiplo coprimo, de manera que $\boldsymbol{p} = m\boldsymbol{q}$ para alguna $m > 0$. Supongamos que el problema (1) es factible. Entonces se satisface lo siguiente:

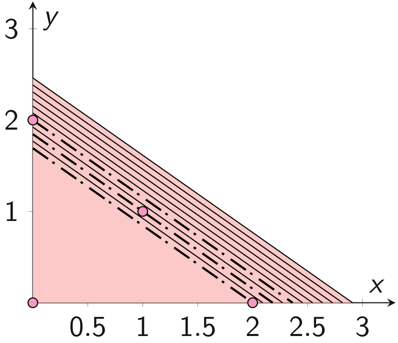
1. Si $q_i < 0$ para algún $i \in \{1, \dots, n\}$, entonces la η-ésima capa entera $H_{\boldsymbol{q},\eta\|\boldsymbol{q}\|^{-2}}$ contiene un número infinito de puntos factibles.
2. Si $\boldsymbol{q} > \mathbf{0}$ entonces, para todo $k \in \{\eta, \eta - 1, \dots, 0\}$, la k-ésima capa entera $H_{\boldsymbol{q},k\|\boldsymbol{q}\|^{-2}}$ contiene un número finito de puntos factibles.



$$x - y \leq 3.2$$



$x + y \leq 3.2$



$1.1x + 1.3y \leq 3.2$

Por el teorema de factibilidad (o el de cobertura), las soluciones se encuentran en una capa entera $H_{\boldsymbol{q},k\|\boldsymbol{q}\|^{-2}}$ con $0 \leq k \leq \eta$. Por el lema de utilidad, estas soluciones satisfacen la **ecuación lineal diofantina**

$$\boldsymbol{q}^T \boldsymbol{x} = q_1 x_1 + \cdots + q_n x_n = k.$$

Podemos resolver recursivamente esta ecuación. Utilizando una formulación hacia adelante, obtenemos...

$$x_i = k \cdot \prod_{j=2}^{i} \omega_j' \cdot x_i' - \sum_{j=1}^{i-1} m_{ij} x_i' t_j + g_{i+1} t_i$$

para $1 \leq i \leq n-2$, y también,

$$x_{n-1} = k \cdot \prod_{j=2}^{n-1} \omega_j' \cdot x_{n-1}' - \sum_{j=1}^{n-2} m_{n-1,j} x_{n-1}' t_j + \frac{q_n}{\prod_{j=1}^{n-1} g_j} t_{n-1},$$

$$x_n = k \cdot \prod_{j=2}^{n-1} \omega_j' \cdot x_n' - \sum_{j=1}^{n-2} m_{n-1,j} x_n' t_j - \frac{q_{n-1}}{\prod_{j=1}^{n-1} g_j} t_{n-1},$$

donde las constantes desconocidas son **números enteros mágicos** y $t_1, \ldots, t_{n-1} \in \mathbb{Z}$ son parámetros libres.

Si definimos $\boldsymbol{\nu} \in \mathbb{Z}^n$ como

$$\nu_i := x_i' \cdot \prod_{j=2}^{\text{mín}\,\{i,n-1\}} \omega_j'.$$

y también definimos la matriz $M \in \mathbb{Z}^{n\times(n-1)}$ a través de

$$M_{ij} := \begin{cases} -m_{ij}x_i', & j < i, \\ g_{i+1}, & i = j < n-1, \\ \frac{q_n}{\prod_{k=1}^{n-1} g_k}, & i = j = n-1, \\ -\frac{q_{n-1}}{\prod_{k=1}^{n-1} g_k}, & i = n, j = n-1, \\ 0, & \text{e.o.c.}, \end{cases}$$

encontramos que...

Proposición

Sea $\boldsymbol{q} \in \mathbb{Z}^n$ un vector con entradas coprimas y última entrada no nula. Entonces **todas** las soluciones enteras de la ecuación lineal diofantina

$$\boldsymbol{q}^T \boldsymbol{x} = q_1 x_1 + \cdots + q_n x_n = k$$

son de la forma

$$\boldsymbol{x} = k\boldsymbol{\nu} + M\boldsymbol{t},$$

donde $\boldsymbol{t} \in \mathbb{Z}^{n-1}$.

3. PROBLEMA DE FROBENIUS

Hola mundo

4. MÚLTIPLES RESTRICCIONES

Hola mundo