

PUNTO Y LÍNEA SOBRE EL PLANO

ECUACIONES LINEALES DIOFANTINAS APLICADAS A
PROGRAMAS LINEALES ENTEROS

IÑAKI LIENDO

COLOQUIO DE MATEMÁTICAS

9 DE SEPTIEMBRE DE 2025

1. MOTIVACIÓN

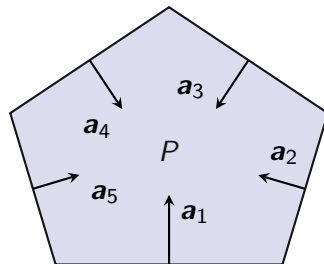
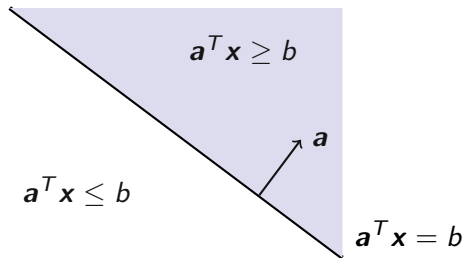
Definición

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

Definición

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

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



Definición

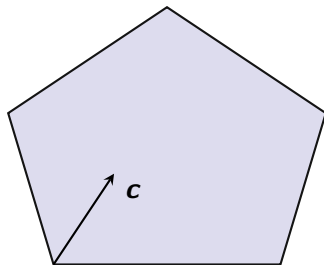
Sea $P \subseteq \mathbb{R}^n$ un poliedro y sea $\mathbf{c} \in \mathbb{R}^n$ un vector. Llamamos **problema lineal** al problema de maximización

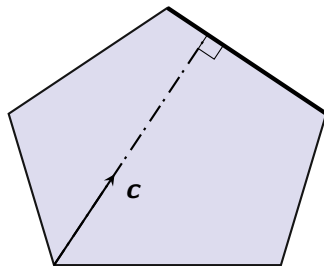
$$z^* := \max_{\mathbf{x}} \{\mathbf{c}^T \mathbf{x} : \mathbf{x} \in P\}.$$

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 $\{\mathbf{x}^* \in P : \mathbf{c}^T \mathbf{x}^* = z^*\}$ contiene al menos un vértice de P .





Definición

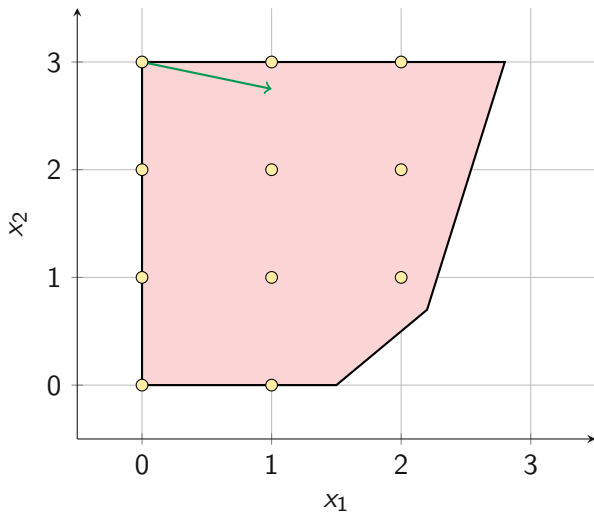
Al problema lineal

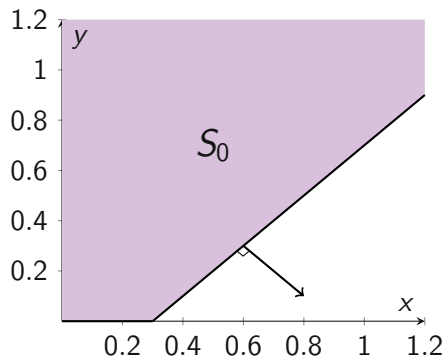
$$z^* := \max_{\mathbf{x}} \{\mathbf{c}^T \mathbf{x} : \mathbf{x} \in P\}.$$

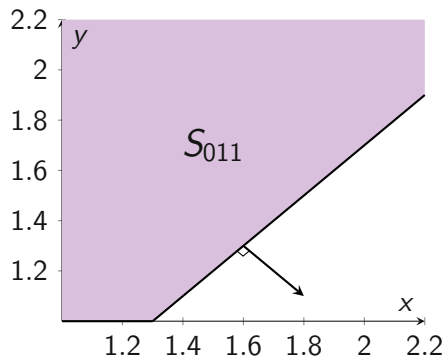
lo llamamos **problema relajado** del **problema lineal entero**

$$z_{PE}^* := \max_{\mathbf{x}} \{\mathbf{c}^T \mathbf{x} : \mathbf{x} \in P \cap \mathbb{Z}^n\}.$$

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



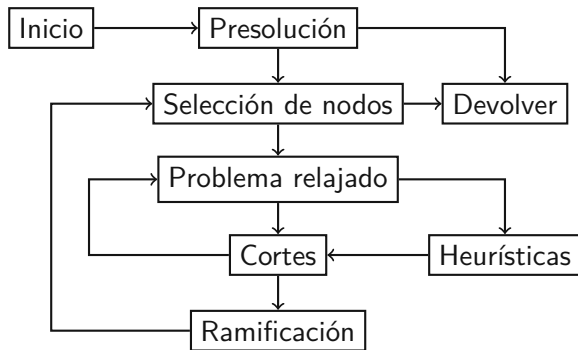




Ramificación y Acotamiento genera la cadena de subproblemas autosimilares

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

y este método jamás terminará con una solución.

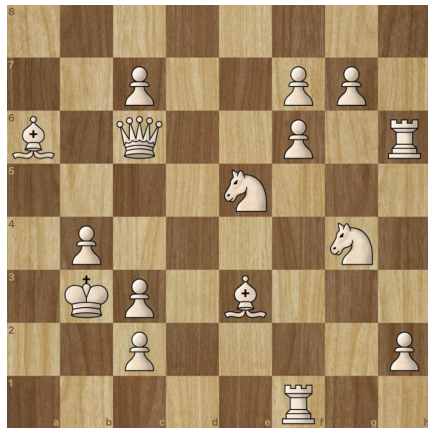


En general, Ramificación y Acotamiento es ineficiente (o incluso falla) cuando una restricción del problema es ortogonal al vector objetivo. La instancia minimal que reproduce esta ineficiencia es

$$\max_{\mathbf{x} \in \mathbb{Z}^n} \quad \mathbf{p}^T \mathbf{x}, \quad (1a)$$

$$\begin{aligned} \text{s.a.} \quad & \mathbf{p}^T \mathbf{x} \leq u, \\ & \mathbf{x} \geq \mathbf{0}. \end{aligned} \quad (1b)$$

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.

- Contando 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 $\mathbf{v} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ es **esencialmente entero** si existen un vector $\mathbf{w} \in \mathbb{Z}^n$ y un escalar $m \neq 0$ tales que $\mathbf{v} = m\mathbf{w}$. Además, decimos que \mathbf{w} es el **múltiplo coprimo** de \mathbf{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 $(\sqrt{2}, \sqrt{3})$ no es esencialmente entero (¿por qué?).

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

Definición

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

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

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

Teorema de cobertura

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

Lema de utilidad (*)

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

Lema de satisfacción (*)

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

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

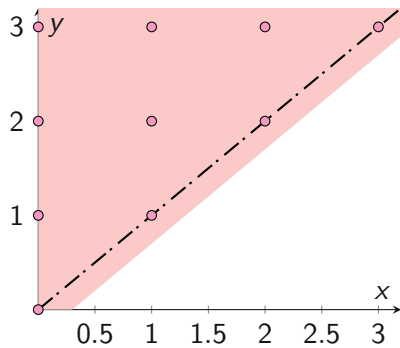
Teorema de infactibilidad (*)

Sea $\mathbf{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea \mathbf{q} su múltiplo coprimo. Entonces el problema (1) es infactible si y solo si $\mathbf{q} \geq \mathbf{0}$ y el lado derecho u de (1.1b) es negativo.

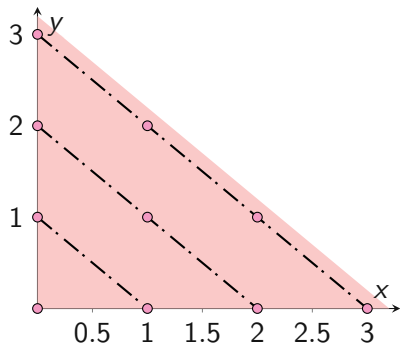
Teorema de factibilidad

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

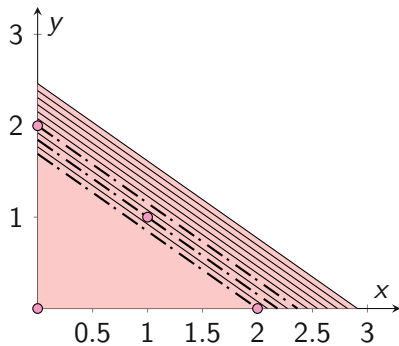
1. Si $q_i < 0$ para algún $i \in \{1, \dots, n\}$, entonces la η -ésima capa entera $H_{\mathbf{q}, \eta \|\mathbf{q}\|}^{-2}$ contiene un número infinito de puntos factibles.
 2. Si $\mathbf{q} > \mathbf{0}$ entonces, para todo $k \in \{\eta, \eta - 1, \dots, 0\}$, la k -ésima capa entera $H_{\mathbf{q}, k \|\mathbf{q}\|}^{-2}$ 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 $H_{\mathbf{q}, k\|\mathbf{q}\|^{-2}}$ con $0 \leq k \leq \eta$. Por el lema de utilidad, estas soluciones satisfacen la **ecuación lineal diofantina**

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

Para $n = 2$, todas las soluciones enteras de esta ecuación están dadas por

$$\begin{cases} x_1 = kx'_1 + q_2 t, \\ x_2 = kx'_2 - q_1 t, \end{cases}$$

donde $t \in \mathbb{Z}$ es un parámetro libre y x'_1, x'_2 son **coeficientes de Bézout** de q_1, q_2 . Estos coeficientes satisfacen

$$q_1 x'_1 + q_2 x'_2 = \text{mcd}\{q_1, q_2\} = 1,$$

y se pueden calcular por medio del algoritmo extendido de Euclides.

Resolviendo la ecuación en $n \geq 2$ incógnitas de manera recursiva 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 $t_1, \dots, t_{n-1} \in \mathbb{Z}$ son parámetros libres.

Para que se satisfagan las condiciones de no negatividad de x_1, \dots, x_n , debe ser el caso que

$$t_i \geq -\frac{\omega_i x'_i}{g_{i+1}},$$

para todo $1 \leq i \leq n-2$. Si \mathbf{q} tiene alguna entrada negativa, basta* que se satisfaga

$$t_{n-1} \geq \max \left\{ -\frac{\omega_{n-1} x'_{n-1}}{q_n} \cdot \prod_{j=1}^{n-1} g_j, \frac{\omega_{n-1} x'_n}{q_{n-1}} \cdot \prod_{j=1}^{n-1} g_j \right\}.$$

Si $\mathbf{q} > \mathbf{0}$, entonces se debe satisfacer

$$-\frac{\omega_{n-1} x'_{n-1}}{q_n} \cdot \prod_{j=1}^{n-2} g_j \leq t_{n-1} \leq \frac{\omega_{n-1} x'_n}{q_{n-1}} \cdot \prod_{j=1}^{n-2} g_j.$$

Definamos $\nu \in \mathbb{Z}^n$ como

$$\nu_i := x'_i \cdot \prod_{j=2}^{\min\{i, n-1\}} \omega'_j.$$

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

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

Entonces...

Proposición

Sea $\mathbf{q} \in \mathbb{Z}^n$ un vector con entradas coprimas. Luego, **todas** las soluciones enteras de la ecuación lineal diofantina

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

son de la forma

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

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

Lema

El vector $\boldsymbol{\nu} \in \mathbb{Z}^n$ satisface $\mathbf{q}^T \boldsymbol{\nu} = 1$, y la matriz M es tal que $\ker\{M^T\} = \text{gen}\{\mathbf{q}\}$.

Definición

Decimos que un subconjunto Λ de \mathbb{R}^n es un **grupo aditivo** si

1. $\mathbf{0} \in \Lambda$, y
2. si $\mathbf{x}, \mathbf{y} \in \Lambda$, entonces $\mathbf{x} + \mathbf{y} \in \Lambda$, y también $-\mathbf{x} \in \Lambda$.

Además, decimos que Λ es una **red** si existen vectores $\mathbf{v}_1, \dots, \mathbf{v}_n$ linealmente independientes tales que

$$\Lambda = \{\lambda_1 \mathbf{v}_1 + \dots + \lambda_n \mathbf{v}_n : \lambda_i \in \mathbb{Z}\}.$$

A los vectores $\mathbf{v}_1, \dots, \mathbf{v}_n$ los llamamos la **base de la red** Λ .

Ejemplo

\mathbb{Z}^n es una red que tiene por base los vectores canónicos $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$.

Teorema

El conjunto de vectores

$$\{\boldsymbol{\nu}, \boldsymbol{m}_1, \dots, \boldsymbol{m}_{n-1}\}$$

forma una base de la red \mathbb{Z}^n , donde \boldsymbol{m}_i denota la i -ésima columna de la matriz $M \in \mathbb{Z}^{n \times (n-1)}$.

Geométricamente, \boldsymbol{q} induce una descomposición de \mathbb{Z}^n como la suma directa de las subredes Λ_p y Λ_h , donde

$$\Lambda_p := \{k\boldsymbol{\nu} : k \in \mathbb{Z}\}, \quad \Lambda_h := \{M\boldsymbol{t} : \boldsymbol{t} \in \mathbb{Z}^{n-1}\}.$$

Por las propiedades de $\boldsymbol{\nu}$ y de M , tenemos que $\boldsymbol{q}^T \boldsymbol{x} = k$ para todo $\boldsymbol{x} \in \Lambda_p$ y $\boldsymbol{q}^T \boldsymbol{x} = 0$ para todo $\boldsymbol{x} \in \Lambda_h$.

3. PRIMER INTENTO DE CLASIFICACIÓN

Corolario (*)

Sea \mathbf{q} un vector con entradas coprimas y sea $\tilde{\mathbf{q}}$ un vector con las entradas de \mathbf{q} permutadas. Entonces $\ker\{M^T\} \cong \ker\{\tilde{M}^T\}$.

Definición

Sea $\mathbf{q} \in \mathbb{Z}^n$ un con entradas coprimas, entonces definimos su **órbita** como

$$\text{orb}(\mathbf{q}) := \{P\mathbf{q} : P \in \mathbb{Z}^{n \times n} \text{ es matriz de permutación}\}.$$

Lema

Sea $\mathbf{q} \in \mathbb{Z}^n$ un vector con entradas coprimas y sea $\tilde{\mathbf{q}} \in \text{orb}(\mathbf{q})$. Entonces las redes $\tilde{\Lambda}_h$ y Λ_h son isomorfas. Similarmente, las redes $\tilde{\Lambda}_p$ y Λ_p son isomorfas.

Definición

Sean $\mathbf{p}, \tilde{\mathbf{p}} \in \mathbb{R}^n$ vectores esencialmente enteros con entradas distintas de cero. Entonces decimos que \mathbf{p} y $\tilde{\mathbf{p}}$ son equivalentes si y solo si $\text{orb}(\mathbf{q}) = \text{orb}(\tilde{\mathbf{q}})$, donde \mathbf{q} y $\tilde{\mathbf{q}}$ son sus respectivos múltiplos coprimos. En este caso escribimos $\mathbf{p} \sim \tilde{\mathbf{p}}$.

4. SEGUNDO INTENTO DE CLASIFICACIÓN

Corolario

La matriz

$$U_{\mathbf{q}} := [\boldsymbol{\nu} \mid \mathbf{m}_1 \mid \cdots \mid \mathbf{m}_{n-1}] \in \mathbb{Z}^{n \times n}$$

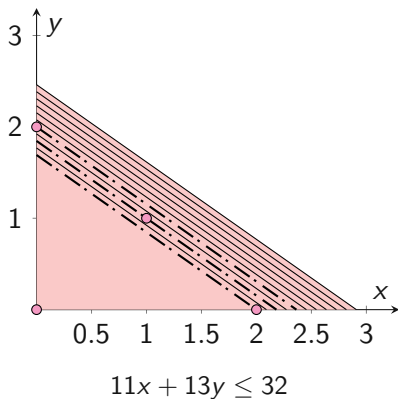
es unimodular, es decir, su determinante es ± 1 .

- Podemos “traducir” las descomposiciones $\mathbf{q} \mapsto U_{\mathbf{q}}$ y $\tilde{\mathbf{q}} \mapsto U_{\tilde{\mathbf{q}}}$ por medio de $U_{\mathbf{q}} U_{\tilde{\mathbf{q}}}^{-1}$.
- \implies **Todos** los vectores coprimos inducen descomposiciones similares.
- \implies **Todos** los vectores esencialmente enteros pertenecen a la misma clase de equivalencia.
- **Pero** $\Lambda_p \not\cong \tilde{\Lambda}_p$ y $\Lambda_h \not\cong \tilde{\Lambda}_h$.

5. PROBLEMA DE FROBENIUS

Problema

Dados enteros q_1, \dots, q_n coprimos, encontrar el mayor entero que **no** puede ser expresado como $q_1x_1 + \dots + q_nx_n$, donde x_1, \dots, x_n son no negativos.



Teorema

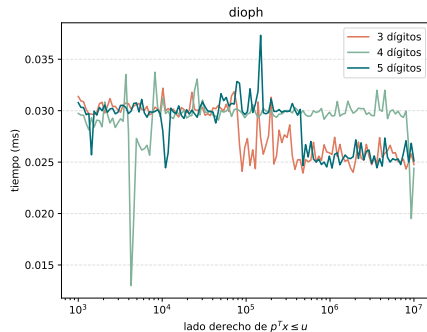
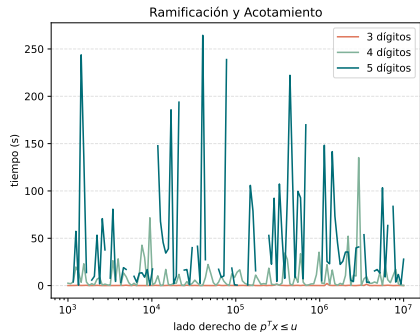
El numero de Frobenius F satisface

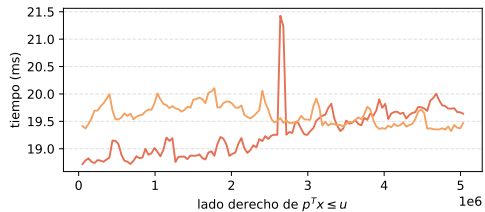
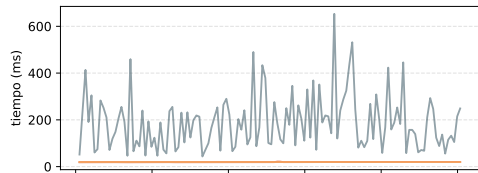
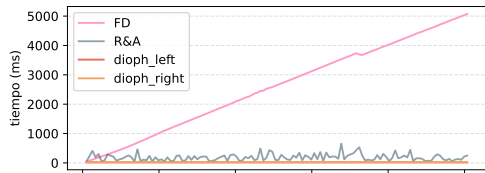
$$F \leq \frac{n}{2} \cdot \|M\|_F \cdot \max_{1 \leq j \leq n} \left\{ q_j^2 \sqrt{q_j^{-2} + \|q\|_2^{-2}} \right\},$$

donde

$$\|M\|_F^2 := \sum_{i=1}^n \sum_{j=1}^{n-1} M_{ij}^2 = \text{tr}(M^T M).$$

6. ALGUNOS RESULTADOS NUMÉRICOS





n	FD	R&A	dioph_left	dioph_right
1,000	1.27 (± 0.1)	0.11 (± 0.02)	0.01 (± 0.00)	0.01 (± 0.00)
2,000	10.37 (± 0.02)	0.14 (± 0.02)	0.04 (± 0.00)	0.04 (± 0.00)
5,000	160.56 (± 0.39)	1.67 (± 0.20)	0.25 (± 0.00)	0.27 (± 0.00)
10,000		2.12 (± 0.33)	1.06 (± 0.00)	1.16 (± 0.00)
20,000		7.68 (± 0.34)	4.60 (± 0.01)	4.99 (± 0.01)
30,000		19.19 (± 1.18)	10.74 (± 0.02)	11.55 (± 0.01)
40,000		24.33 (± 0.19)	19.47 (± 0.02)	20.99 (± 0.08)
50,000		38.94 (± 0.18)	30.89 (± 0.03)	33.45 (± 0.04)
60,000		51.96 (± 0.53)	45.07 (± 0.05)	48.55 (± 0.05)
70,000		81.03 (± 1.26)	61.89 (± 0.04)	66.35 (± 0.10)
80,000		116.62 (± 0.93)	81.42 (± 0.06)	87.73 (± 0.12)
90,000		141.68 (± 2.10)	103.96 (± 0.04)	111.55 (± 0.12)
100,000		170.40 (± 1.75)	129.44 (± 0.05)	139.65 (± 0.16)

7. MÚLTIPLES RESTRICCIONES

Sea $A \in \mathbb{Q}^{m \times n}$ una matriz con renglones linealmente independientes y sea $\mathbf{b} \in \mathbb{Q}^m$ un vector. Definamos el problema

$$\max_{\mathbf{x} \in \mathbb{Z}^n} \quad \mathbf{q}^T \mathbf{x}, \quad (2a)$$

$$\text{s.a.} \quad \mathbf{q}^T \mathbf{x} \leq \eta, \quad (2b)$$

$$A\mathbf{x} = \mathbf{b}, \quad (2c)$$

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

Podemos suponer, sin pérdida de generalidad, que $A \in \mathbb{Z}^{m \times n}$ y $\mathbf{b} \in \mathbb{Z}^m$.

Teorema

El problema (2) es equivalente al problema

$$\max_{k \in \mathbb{Z}, \mathbf{t} \in \mathbb{Z}^{n-1}} k, \quad (3a)$$

$$\text{s.a. } k \leq \eta, \quad (3b)$$

$$A\mathbf{M}\mathbf{t} = \mathbf{b} - kA\boldsymbol{\nu}, \quad (3c)$$

$$\mathbf{M}\mathbf{t} \geq -k\boldsymbol{\nu}. \quad (3d)$$

Intuición.

Sabemos que la transformación lineal

$$(k, \mathbf{t}) \mapsto \mathbf{x} := k\boldsymbol{\nu} + \mathbf{M}\mathbf{t}$$

es un isomorfismo entre las redes $\Lambda_p \oplus \Lambda_h$ y $\mathbb{Z}^n \dots$



Teorema (*)

Sea (k_{PR}^*, t_{PR}^*) el óptimo del problema relajado de (3) y supongamos que k_{PR}^* no es entero. Entonces el subproblema generado al añadir la restricción $k \geq \lceil k_{PR}^* \rceil$ es infactible.

Siempre es mejor priorizar ramificaciones en k_{PR}^* puesto que nos deshacemos de manera inmediata subproblemas infactibles.

8. GRACIAS
