

Ecuaciones lineales diofantinas aplicadas a programas lineales enteros

Iñaki Sebastian Liendo Infante

26 de enero de 2026

Tabla de contenidos

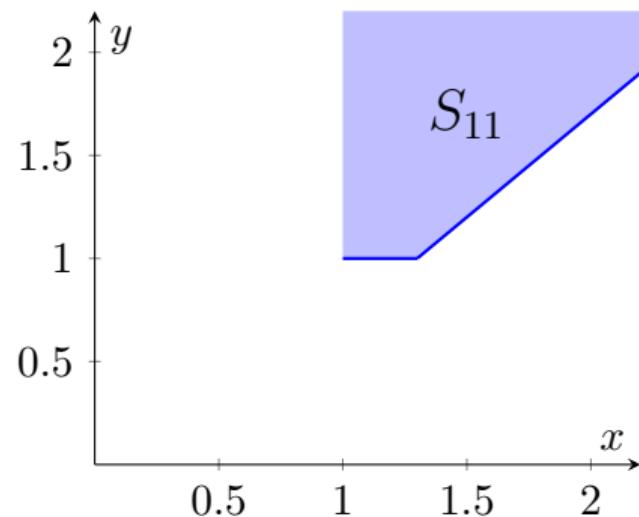
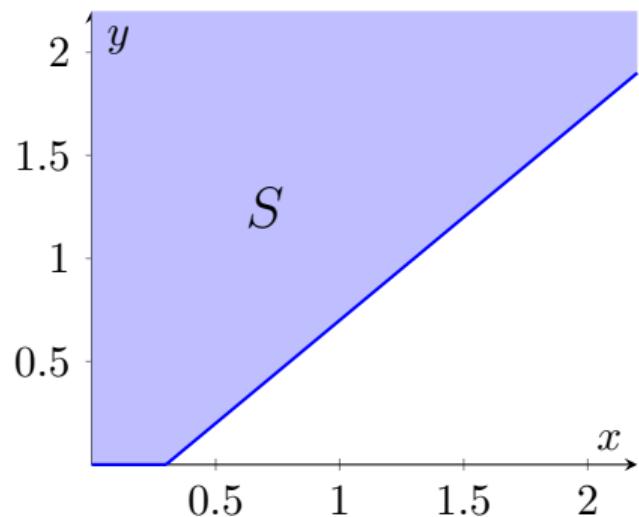
Contexto

Conclusion

Ejemplo minimal

$$\begin{aligned} \max_{(x,y) \in \mathbb{Z}^2} \quad & x - y, \\ \text{s.a.} \quad & x - y \leq 0.3, \\ & x, y \geq 0. \end{aligned}$$

Ejemplo minimal



Problema simétrico

$$\begin{aligned} & \max_{\boldsymbol{x} \in \mathbb{Z}^n} \quad \boldsymbol{p}^T \boldsymbol{x}, \\ & \text{s.a.} \quad \boldsymbol{p}^T \boldsymbol{x} \leq u, \\ & \quad \boldsymbol{x} \geq \mathbf{0}. \end{aligned}$$

Algunas definiciones

Definición

Un vector $\mathbf{p} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ es **esencialmente entero** si existe un vector $\mathbf{q} \in \mathbb{Z}^n$ y un escalar $m \in \mathbb{R} \setminus \{0\}$ tal que $\mathbf{p} = m\mathbf{q}$. Decimos que \mathbf{q} es el **múltiplo coprimo** de \mathbf{p} si sus entradas son coprimas y si su primera entrada no nula es positiva.

Definición

Sea $\mathbf{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea $t \in \mathbb{R}$ un escalar. El hiperplano afín

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

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

Algunos ejemplos

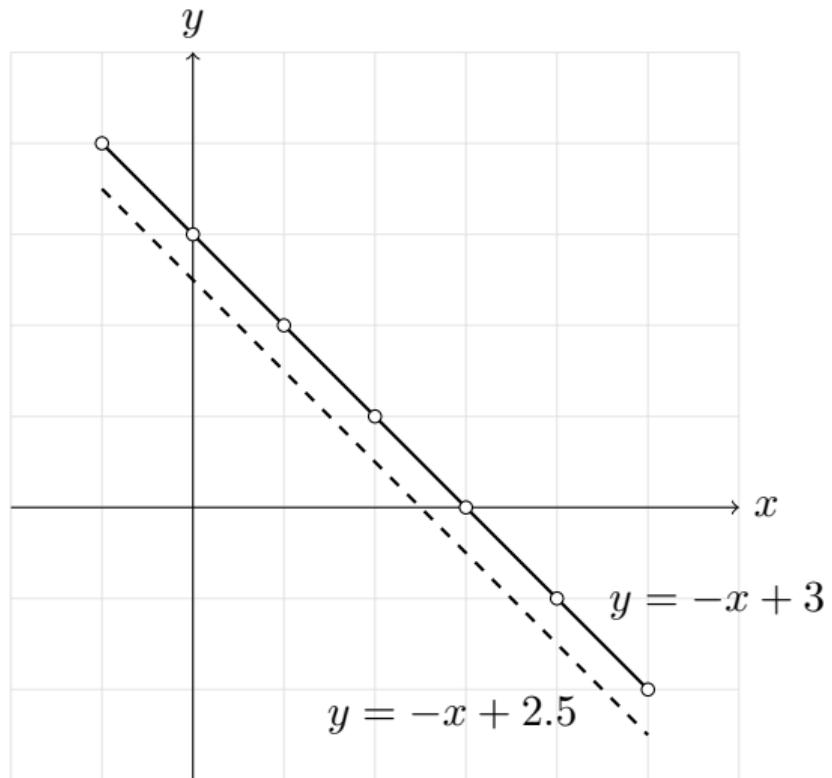
Ejemplo

El vector $(-\sqrt{2}, 1/\sqrt{2}) = -\frac{1}{\sqrt{2}}(2, -1)$ es esencialmente entero.

Ejemplo

El vector $(\sqrt{2}, \sqrt{3})$ no es esencialmente entero. Supongamos que existe un escalar $m \neq 0$ y enteros a, b tales que $m(a, b) = (\sqrt{2}, \sqrt{3})$. Luego, $a/b = \sqrt{2/3}$, pero el lado izquierdo es racional mientras que el derecho es irracional (!)

Algunos ejemplos



Algunos resultados

Teorema

Sea $\mathbf{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea \mathbf{q} su múltiplo coprimo. Entonces la familia de hiperplanos afines $\{H_{\mathbf{w},k/\|\mathbf{w}\|^2} : k \in \mathbb{Z}\}$ cubre a \mathbb{Z}^n .

Lema

Sea $\mathbf{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea \mathbf{q} su múltiplo coprimo. Entonces $\mathbf{q}^T \mathbf{x} = q_1 x_1 + \cdots + q_n x_n = k$ para todo $\mathbf{x} \in H_{\mathbf{q},k/\|\mathbf{q}\|^2}$.

Construcción de soluciones

Teorema

Sea $\mathbf{q} \in \mathbb{Z}^n$ un vector coprimo. Entonces todas las soluciones enteras de la ecuación lineal diofantina $\mathbf{q}^T \mathbf{x} = k$ son de la forma

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

donde $\mathbf{t} \in \mathbb{Z}^{n-1}$ es un vector de variables libres, y el vector $\boldsymbol{\nu} \in \mathbb{Z}^n$ junto con la matriz $M \in \mathbb{Z}^{n \times (n-1)}$ pueden calcularse en tiempo polinomial a partir de \mathbf{q} .

Construcción de soluciones

Lema

Sea $\mathbf{q} \in \mathbb{Z}^n$ un vector coprimo. Entonces

$$\mathbf{q}^T \boldsymbol{\nu} = 1,$$

y

$$\mathbf{q}^T \mathbf{m}_i = 0,$$

para toda columna \mathbf{m}_i de $M = [\mathbf{m}_1 \mid \cdots \mid \mathbf{m}_{n-1}]$.

Construcción de soluciones

Definición

Un subconjunto Λ del espacio vectorial $(\mathbb{R}^n, +, \cdot)$ 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 $-\mathbf{x} \in \Lambda$.

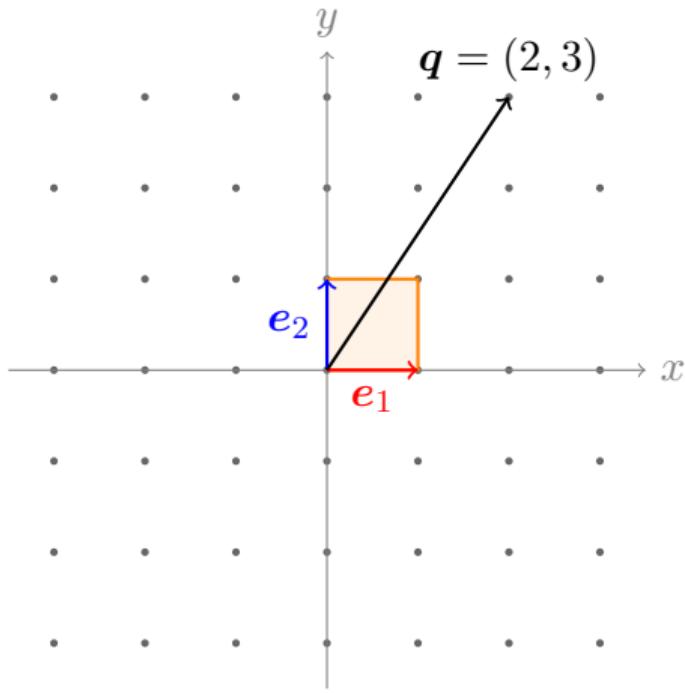
Además, Λ es una **red** si existen vectores $\mathbf{v}_1, \dots, \mathbf{v}_n$ linealmente independientes tales que

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

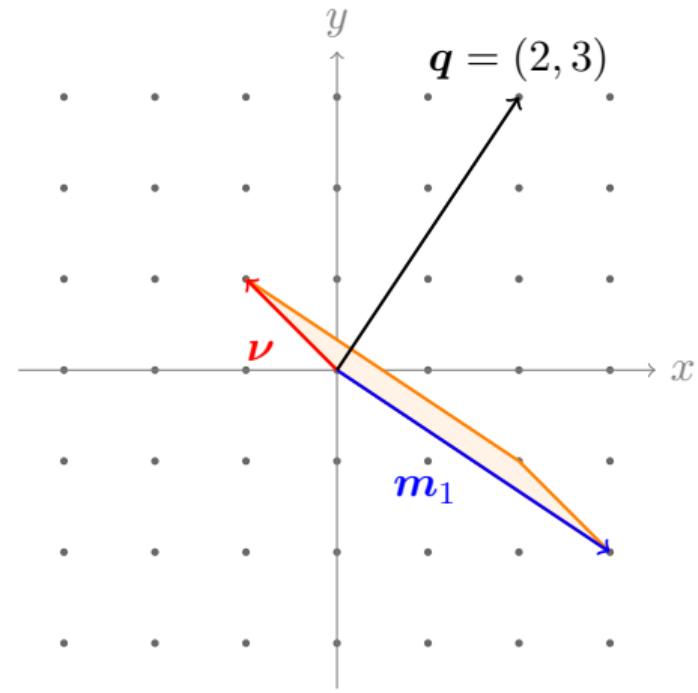
A los vectores $\mathbf{v}_1, \dots, \mathbf{v}_n$ los llamamos la **base de la red** Λ .

Teorema

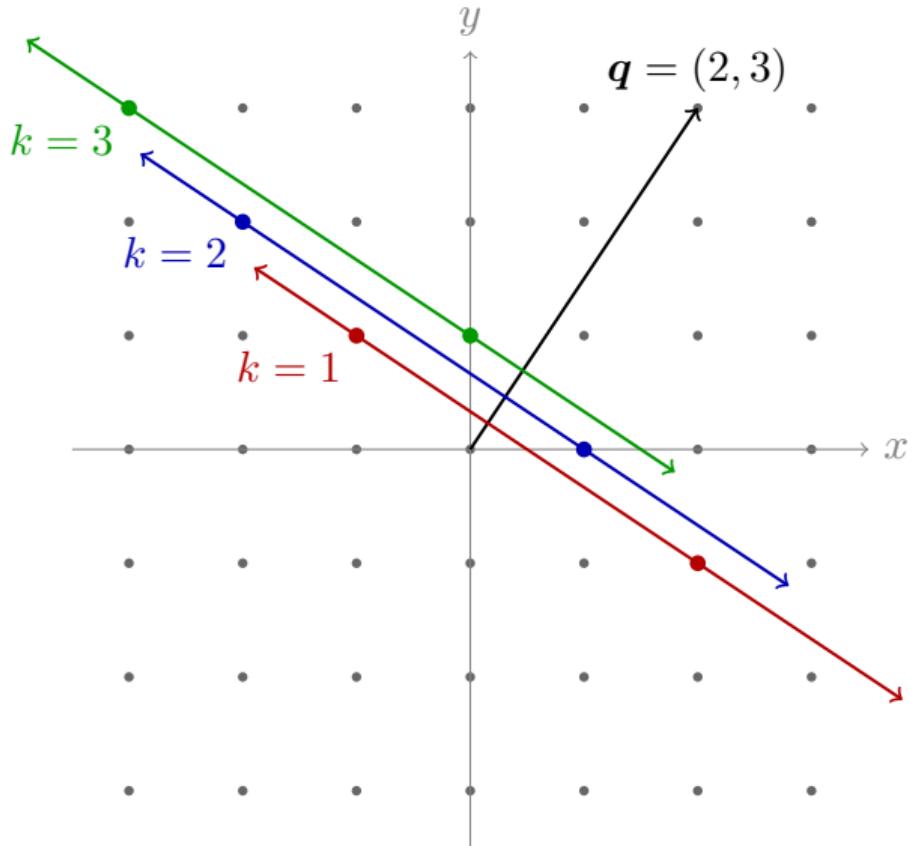
Sea $\mathbf{q} \in \mathbb{Z}^n$ un vector coprimo. Entonces los vectores $\{\mathbf{v}, \mathbf{m}_1, \dots, \mathbf{m}_{n-1}\}$ forman una base de la red \mathbb{Z}^n .



Base: $\{e_1, e_2\}$



Base: $\{(-1, 1), (3, -2)\}$



Tenemos la descomposición en subredes

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

¿Qué propiedades de estas subredes se mantienen si cambiamos de un vector coprimo $\boldsymbol{q} \in \mathbb{Z}^n$ a otro $\tilde{\boldsymbol{q}} \in \mathbb{Z}^n$?

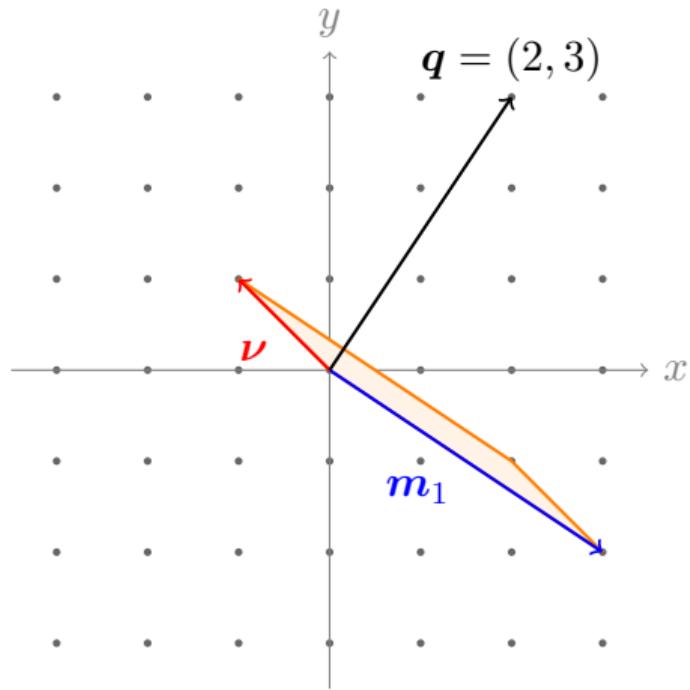
Definición

La **órbita** de un vector coprimo $\mathbf{q} \in \mathbb{Z}^n$ es

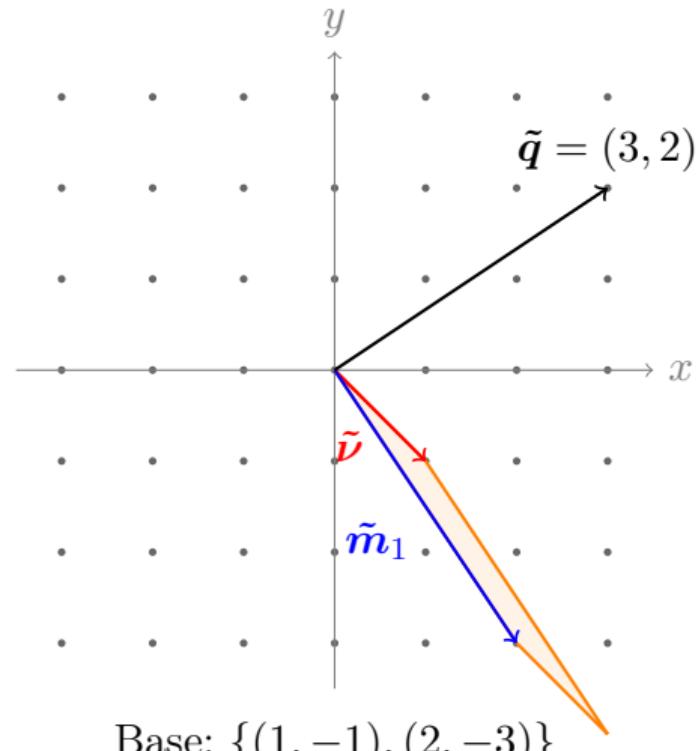
$$\text{orb}(\mathbf{q}) := \{P\mathbf{q} : P \in \mathbb{Z}^{n \times n} \text{ es matriz de permutación}\}.$$

Teorema

Sea $\mathbf{q} \in \mathbb{Z}^n$ un vector coprimo y sea $\tilde{\mathbf{q}} \in \text{orb}(\mathbf{q})$. Entonces $\tilde{\Lambda}_p \cong \Lambda_p$ y $\tilde{\Lambda}_h \cong \Lambda_h$.



Base: $\{(-1, 1), (3, -2)\}$



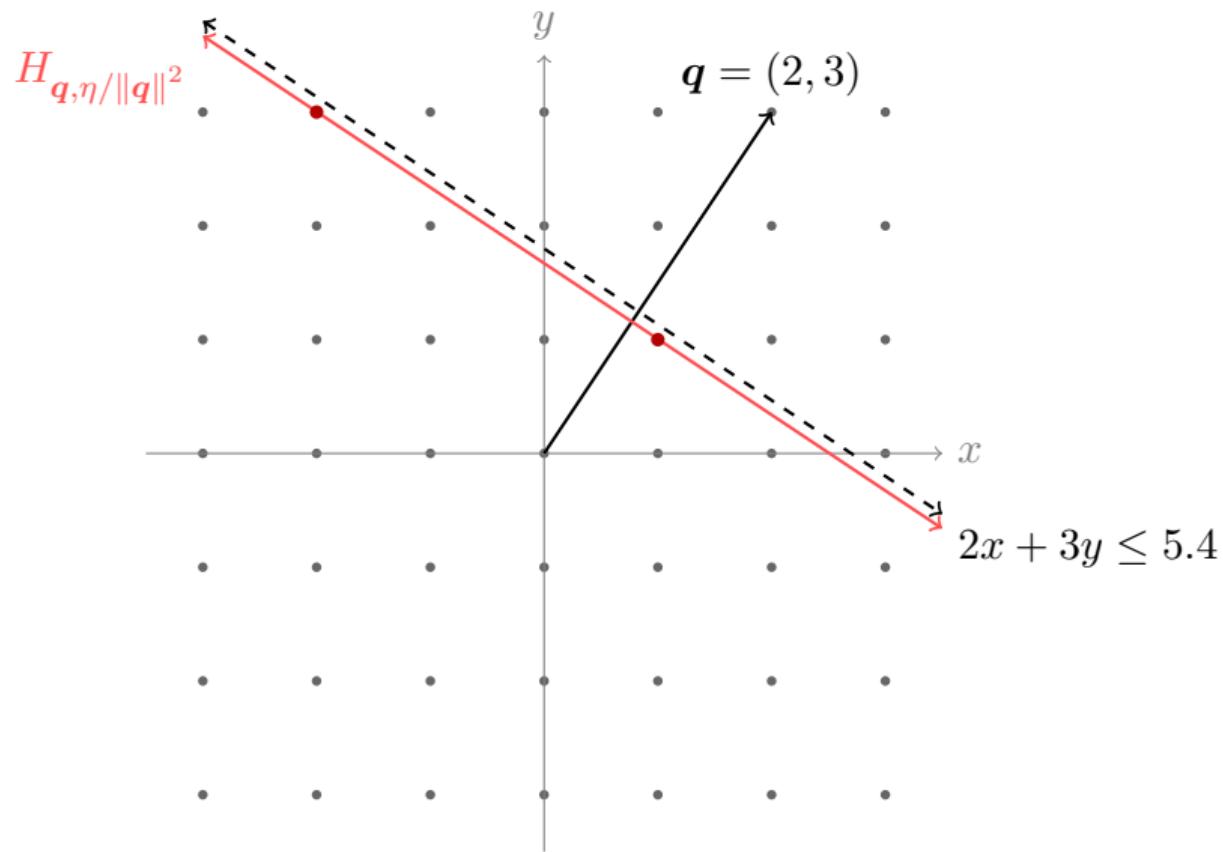
Base: $\{(1, -1), (2, -3)\}$

Sobre la restricción presupuestaria

Lema

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 $H_{\mathbf{q}, \eta/\|\mathbf{q}\|^2}$ en satisfacer la restricción presupuestaria está parametrizada por

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



Sobre la factibilidad

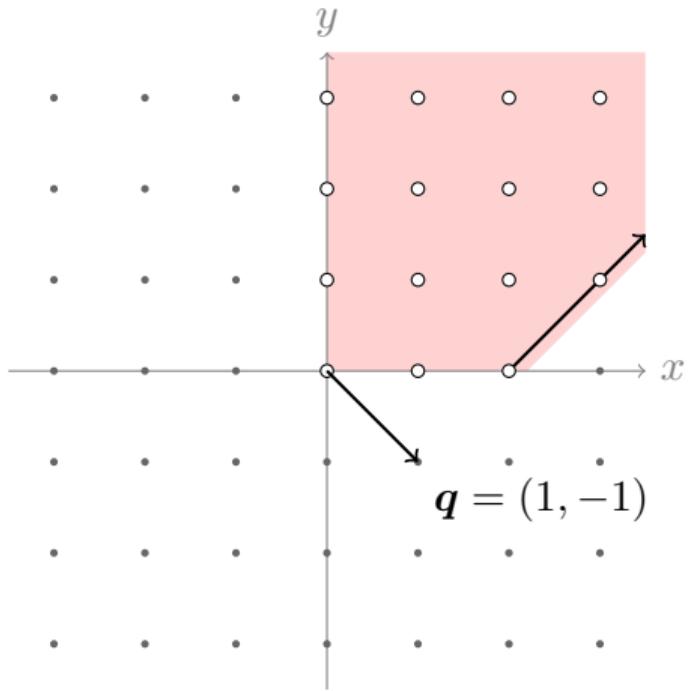
Teorema

Sea $\mathbf{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea \mathbf{q} su múltiplo coprimo. Entonces el problema (PS) es infactible si y solo si $\mathbf{q} \geq \mathbf{0}$ y $u < 0$.

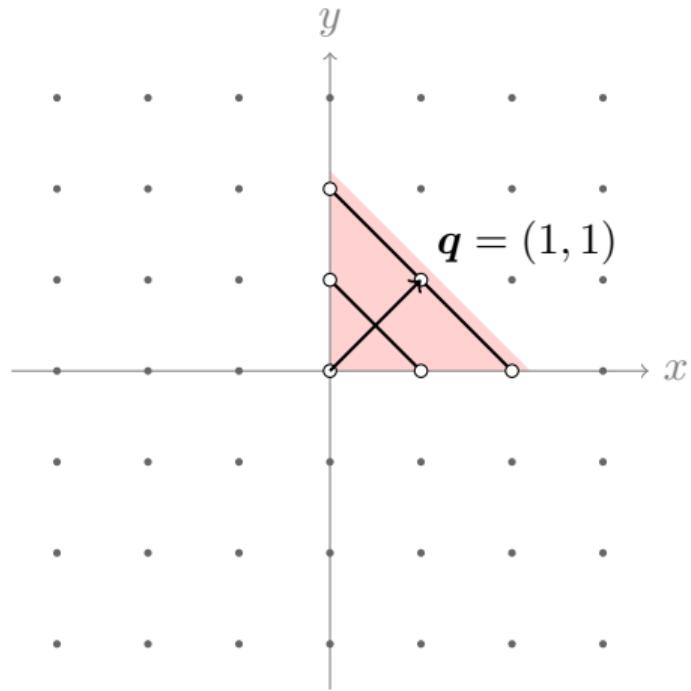
Teorema

Sea $\mathbf{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea \mathbf{q} su múltiplo coprimo. Si (PS) es factible, es cierto que

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.



$$x - y \leq 2.2$$



$$x + y \leq 2.2$$

El caso infinito

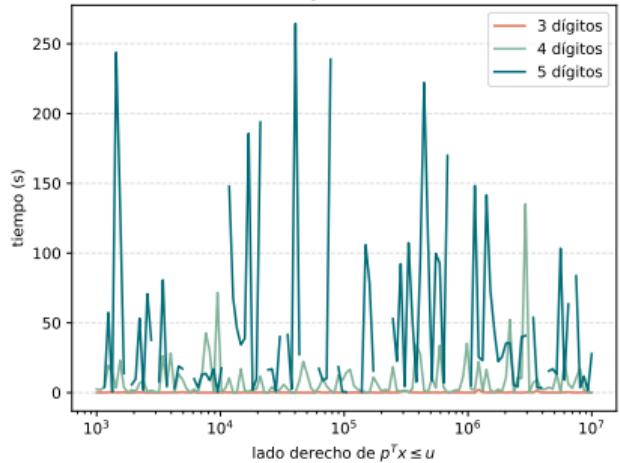
Una medida de eficiencia para los cortes de R&A en (PS) es

$$\left| \frac{x_i^* - x_i}{x_i^* - \lceil x_i^* \rceil} \right| \geq |\mathbf{e}_i^T M \boldsymbol{\delta}|,$$

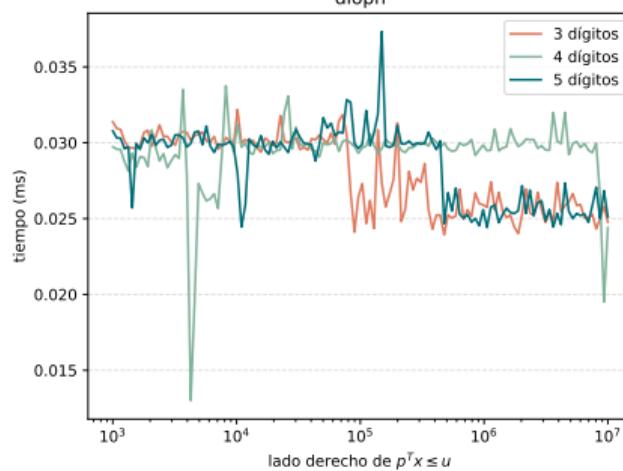
donde

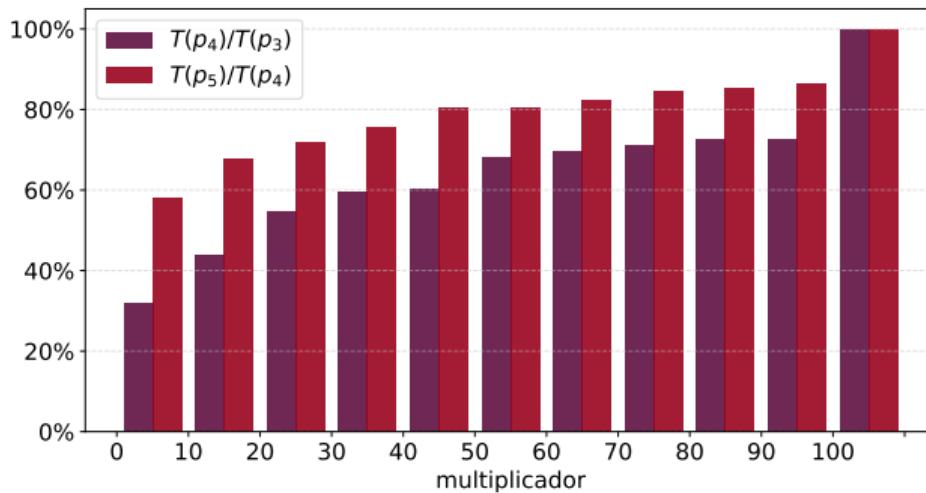
- \mathbf{x}^* es la solución a un subproblema relajado obtenido por R&A,
- $\lceil x_i^* \rceil$ es la i -ésima entrada de la solución del siguiente subproblema con restricción añadida $x_i \geq \lceil x_i^* \rceil$,
- \mathbf{x} es la solución la solución de (PS) más cercana a \mathbf{x}^* ,
- $\|\boldsymbol{\delta}\|_\infty \leq 0.5$.

Ramificación y Acotamiento (CBC)

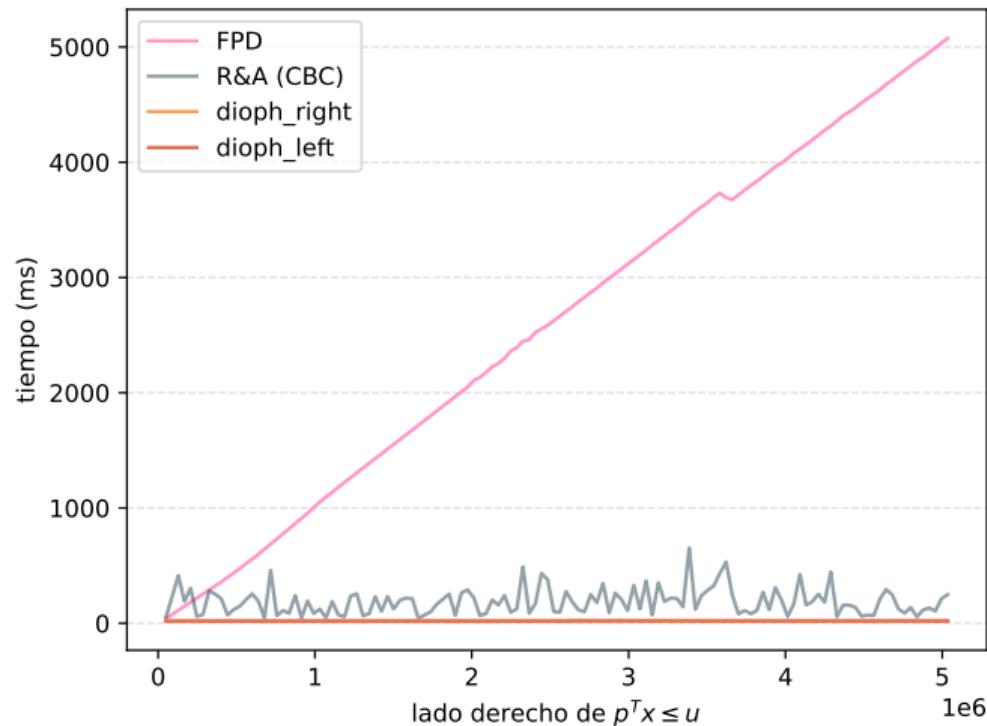


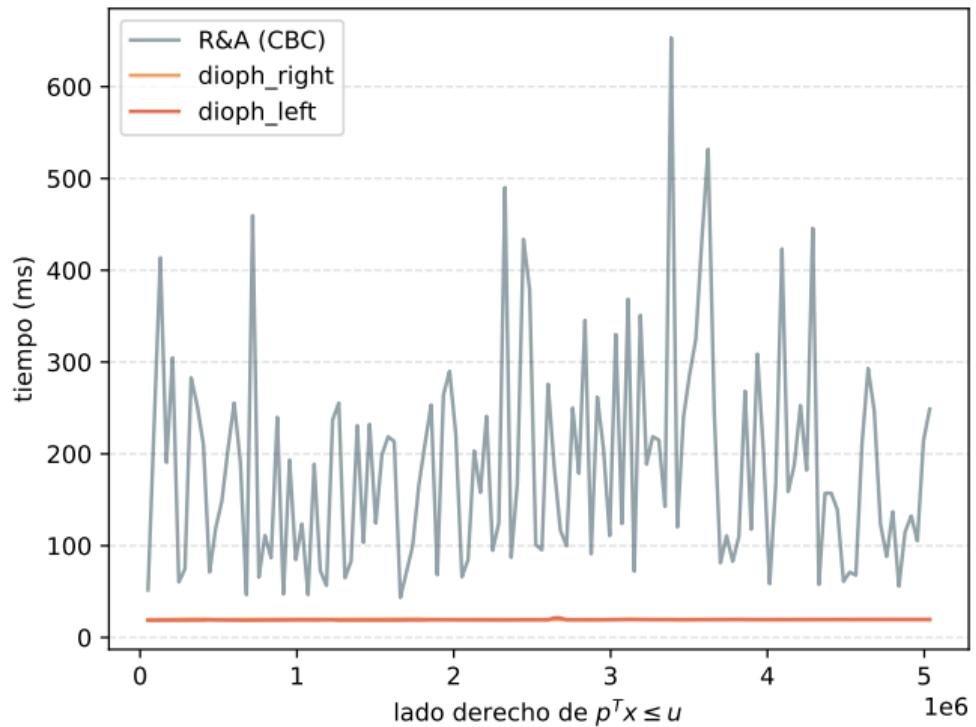
dioph

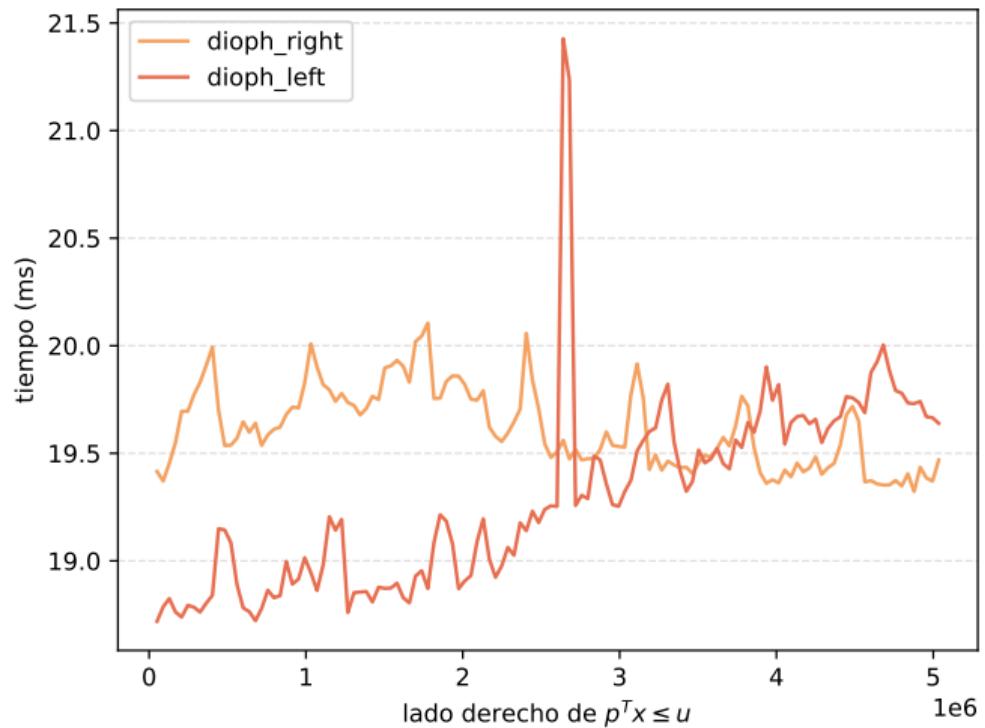




El caso finito (variando el presupuesto)







El caso finito (variando la dimensión)

(a) Tamaños pequeños (milisegundos). Valores: media \pm desviación estandar.

<i>n</i>	FPD	CBC	dioph_left	dioph_right
50	0.16 (± 0.01)	23.29 (± 17.05)	0.31 (± 0.01)	0.31 (± 0.01)
100	1.14 (± 0.02)	9.57 (± 1.01)	0.64 (± 0.01)	0.66 (± 0.01)
200	8.98 (± 0.04)	23.01 (± 4.06)	1.42 (± 0.01)	1.44 (± 0.01)
500	142.68 (± 0.46)	126.82 (± 19.39)	4.53 (± 0.01)	4.67 (± 0.02)

(b) Tamaños grandes (segundos). Valores: media \pm desviación estándar.

<i>n</i>	FPD	CBC	dioph_left	dioph_right
1,000	1.27 (± 0.01)	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)
150,000			299.15 (± 0.13)	

Eventualidad de una sola ecuación lineal diofantina

Teorema

Sea $\mathbf{q} \in \mathbb{Z}^n$ un vector coprimo con entradas estrictamente positivas. Entonces la ecuación lineal diofantina $\mathbf{q}^T \mathbf{x} = k$ tiene soluciones enteras no negativas si $k \in \mathbb{Z}$ satisface

$$k \geq \frac{n\sqrt{n-1}}{2} \|M\| \max_{1 \leq j \leq n} \{q_j^2 \sqrt{q_j^{-2} + \|\mathbf{q}\|^{-2}}\}.$$

El Problema Diofantino de Frobenius

Problema

Dado un vector $\mathbf{q} \in \mathbb{Z}^n$ coprimo con entradas estrictamente positivas, encontrar el entero F más grande tal que $\mathbf{q}^T \mathbf{x} \neq F$ para todo $\mathbf{x} \in \mathbb{Z}^n$ con $\mathbf{x} \geq \mathbf{0}$.

Conclusion

Summarize key takeaways.