Ecuaciones lineales diofantinas aplicadas a programas lineales enteros

Iñaki Sebastian Liendo Infante

28 de enero de 2026

Sobre Ramificación y Acotamiento

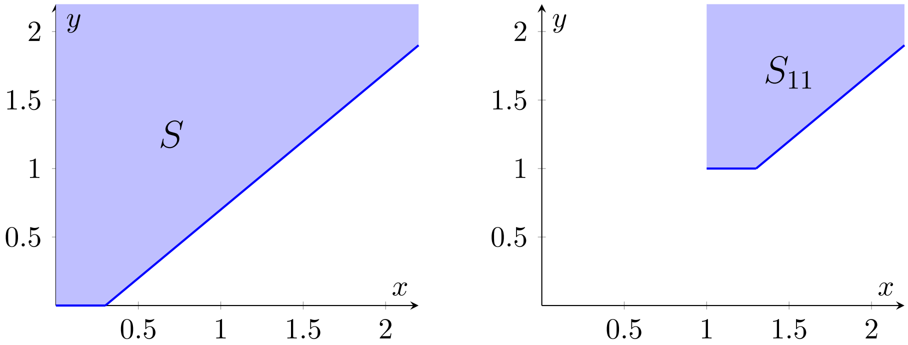
Utilizado para resolver programas lineales enteros o programas lineales mixtos.

- Interés académico: ¿$P \subsetneq NP$?, ¿$P = NP$-completo?
- Interés comercial: Nvidia, IBM, Gurobi, FICO, Artelys, Cardinal Operations, Alibaba MindOpt, MOSEK,...

Ejemplo patológico

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

Ejemplo patológico



Problema Simétrico

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

Algunas definiciones

Definición

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

Definición

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

$$H_{\boldsymbol{p},t} \coloneqq \ker\{\boldsymbol{x} \mapsto \boldsymbol{p}^T \boldsymbol{x}\} + t\boldsymbol{p}$$

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

Algunos ejemplos

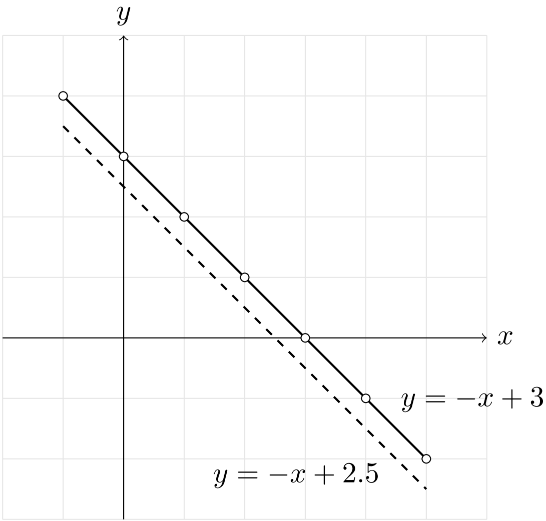
Ejemplo

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

Ejemplo

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

Algunos ejemplos



Algunos resultados

Teorema

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

Lema

Sea $\boldsymbol{p} \in \mathbb{R}^n$ *un vector esencialmente entero y sea* $\boldsymbol{q}$ *su múltiplo coprimo. Entonces* $\boldsymbol{q}^T\boldsymbol{x} = q_1x_1 + \cdots + q_nx_n = k$ *para todo* $\boldsymbol{x} \in H_{\boldsymbol{q},k/\|\boldsymbol{q}\|^2}$*.*

Construcción de soluciones

Teorema

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

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

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

Redes e isomorfismos

Lema

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

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

y

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

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

Redes e isomorfismos

Definición

Un subconjunto Λ del espacio vectorial $(\mathbb{R}^n, +, \cdot)$ es un **grupo aditivo** si

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

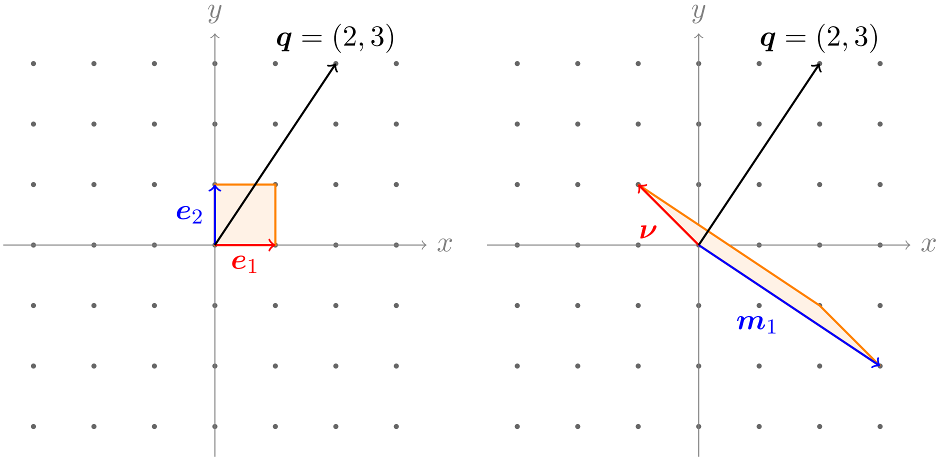
Además, Λ es una **red** si existen vectores $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ linealmente independientes tales que

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

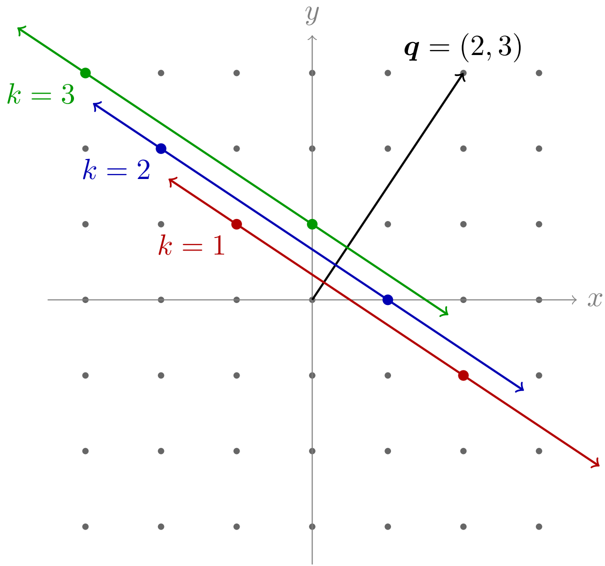
A los vectores $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ los llamamos la **base de la red** Λ.

Teorema

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



Base: $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ Base: $\{(-1, 1),\ (3, -2)\}$


y
$\boldsymbol{q} = (2, 3)$
$k = 3$
$k = 2$
$k = 1$
x

Redes e isomorfismos

Tenemos la descomposición en subredes

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

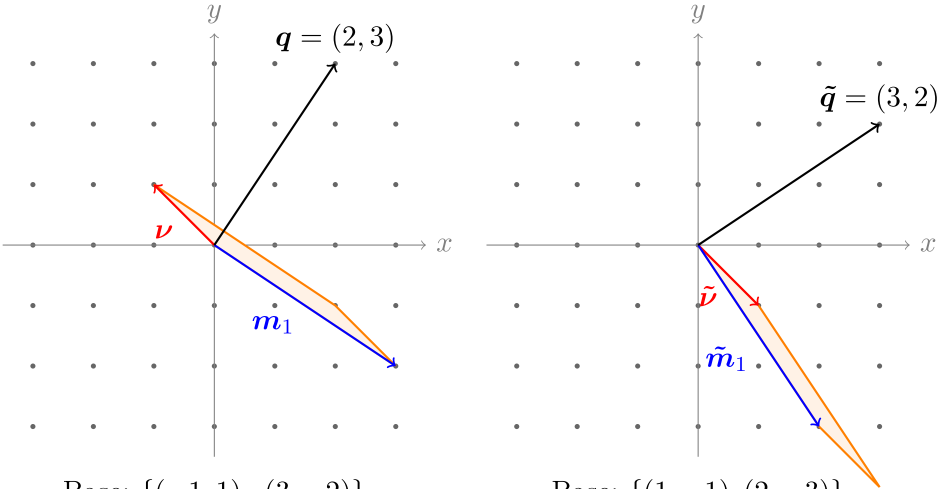
¿Qué propiedades de estas subredes se mantienen si cambiamos de un vector coprimo $\boldsymbol{q} \in \mathbb{Z}^n$ a otro $\tilde{\boldsymbol{q}} \in \mathbb{Z}^n$?

Órbitas e isomorfismos

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

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

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



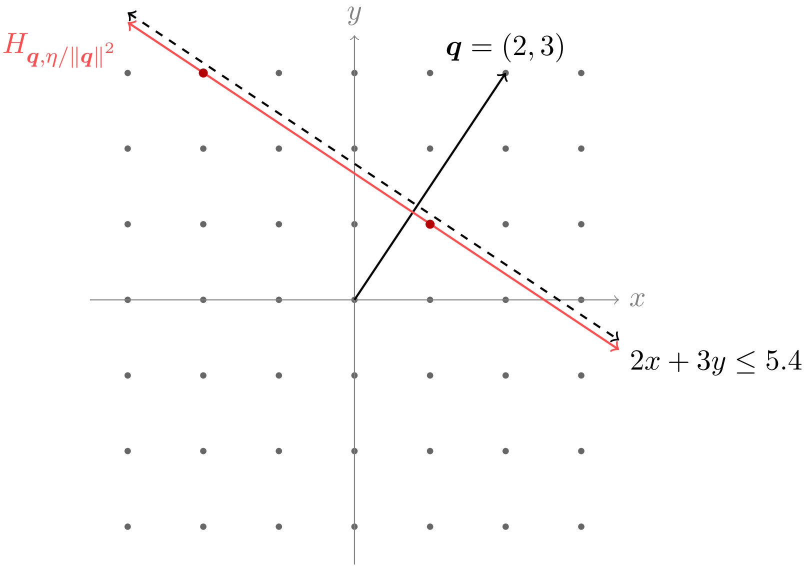
Base: $\{(-1,1),\ (3,-2)\}$ Base: $\{(1,-1),(2,-3)\}$

Sobre la restricción presupuestaria

Lema

Sea $\boldsymbol{p} \in \mathbb{R}^n$ 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 $H_{\boldsymbol{q},\eta/\|\boldsymbol{q}\|^2}$ en satisfacer la restricción presupuestaria está parametrizada por

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


y
x
$H_{\boldsymbol{q},\eta/\|\boldsymbol{q}\|^2}$
$\boldsymbol{q} = (2,3)$
$2x + 3y \leq 5.4$

Sobre la factibilidad

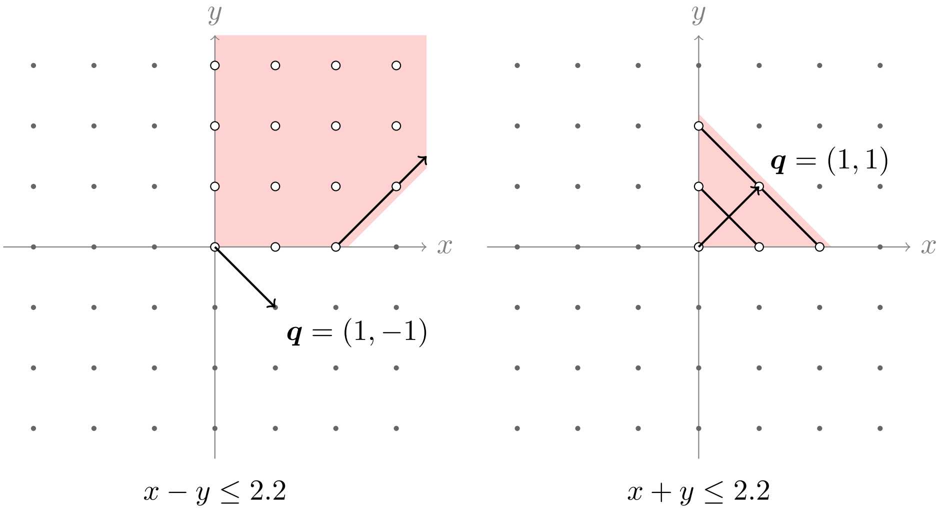
Teorema

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

Teorema

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

1. *si* $q_i < 0$ *para algún* $i \in \{1, \ldots, n\}$, *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* $k \in \{\eta, \eta - 1, \ldots, 0\}$, *la* k*-ésima capa entera* $H_{\boldsymbol{q}, k/\|\boldsymbol{q}\|^2}$ *contiene un número finito de puntos factibles.*



y
x
$\boldsymbol{q} = (1, -1)$
$x - y \leq 2.2$
y
x
$\boldsymbol{q} = (1, 1)$
$x + y \leq 2.2$

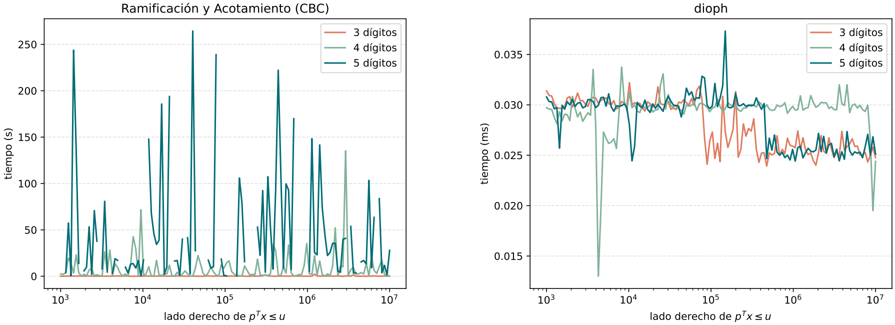
El caso infinito

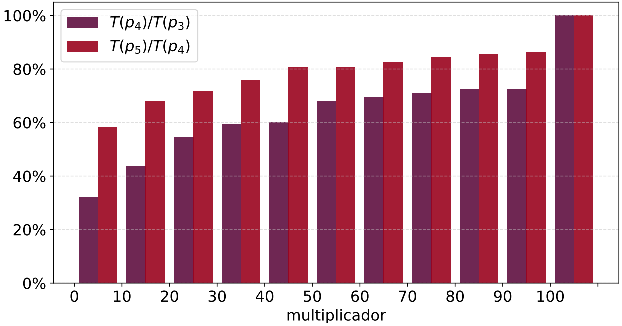
Una medida de eficiencia para los cortes de R&A en (PS) es

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

donde

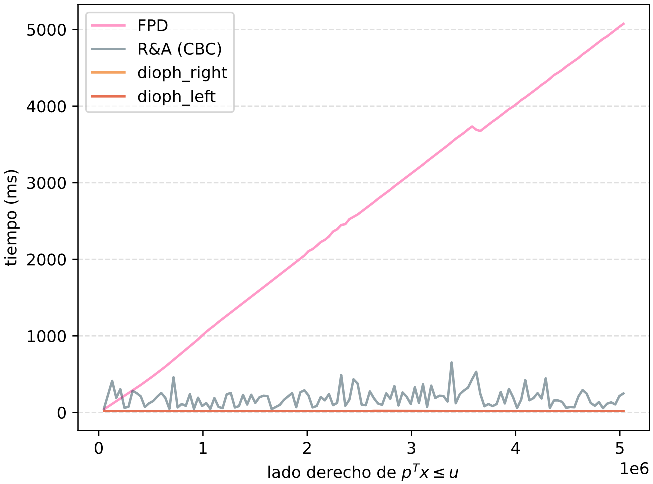
- $\boldsymbol{x}^*$ es la solución a un subproblema relajado obtenido por R&A,
- $\lceil x_i^* \rceil$ es la i-ésima entrada de la solución del siguiente subproblema con restricción añadida $x_i \geq \lceil x_i^* \rceil$,
- $\boldsymbol{x}$ es la solución de (PS) más cercana a $\boldsymbol{x}^*$,
-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

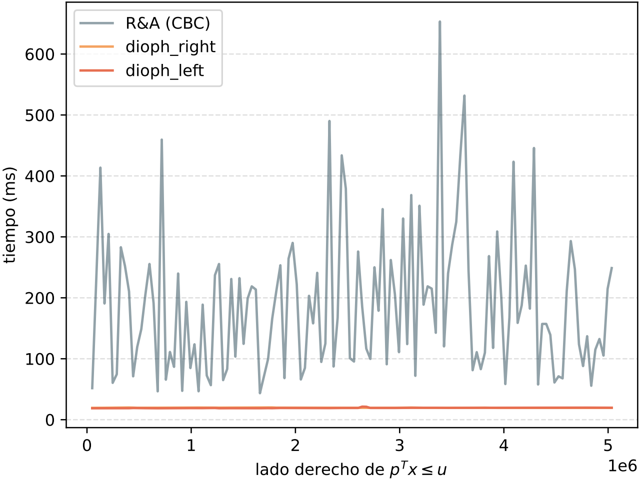

Ramificación y Acotamiento (CBC)
tiempo (s)
lado derecho de $p^T x \leq u$
3 dígitos
4 dígitos
5 dígitos
dioph
tiempo (ms)
lado derecho de $p^T x \leq u$
3 dígitos
4 dígitos
5 dígitos

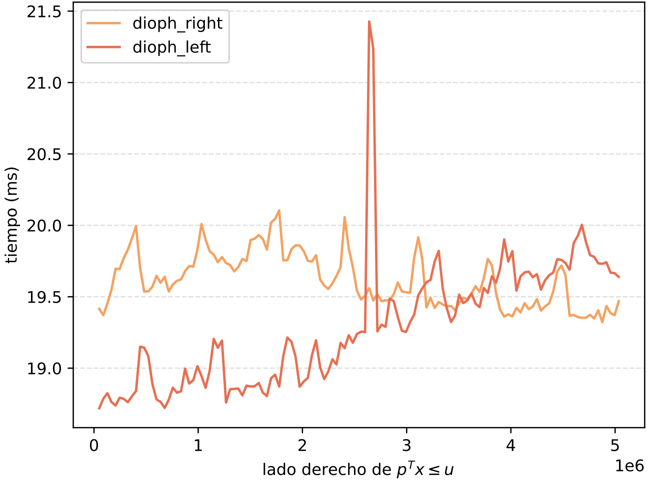


$T(p_4)/T(p_3)$
$T(p_5)/T(p_4)$
100%
80%
60%
40%
20%
0%
0
10
20
30
40
50
60
70
80
90
100
multiplicador

El caso finito (variando el presupuesto)




R&A (CBC)
dioph_right
dioph_left
tiempo (ms)
600
500
400
300
200
100
0
0
1
2
3
4
5
1e6
lado derecho de $p^T x \leq u$



dioph_right
dioph_left
21.5
21.0
20.5
20.0
19.5
19.0
tiempo (ms)
0
1
2
3
4
5
1e6
lado derecho de $p^T x \leq u$

El caso finito (variando la dimensión)

(a) Tamaños pequeños (milisegundos). Valores: media ± desviación estándar.

n	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 ± desviación estándar.

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

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

El Problema Diofantino de Frobenius

Problema

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

Múltiples restricciones (caso particular)

Teorema

Sea $\boldsymbol{q} \in \mathbb{Z}^n$ *un vector coprimo,* $A \in \mathbb{Q}^{m\times n}$ *una matriz con renglones linealmente independientes y* $\boldsymbol{b} \in \mathbb{Q}^m$ *un vector. Entonces los siguientes dos problemas son equivalentes*

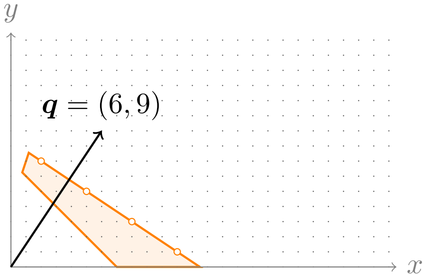
$$
\begin{aligned}
\max_{x\in\mathbb{Z}^n} \quad & \boldsymbol{q}^T\boldsymbol{x}, \\
s.a. \quad & \boldsymbol{q}^T\boldsymbol{x} \leq \eta, \\
& A\boldsymbol{x} = \boldsymbol{b}, \\
& \boldsymbol{x} \geq \boldsymbol{0}.
\end{aligned}
\qquad\qquad
\begin{aligned}
\max_{(k,\boldsymbol{t})\in\mathbb{Z}^n} \quad & k, \\
s.a. \quad & k \leq \eta, \\
& AM\boldsymbol{t} = \boldsymbol{b} - kA\boldsymbol{\nu}, \\
& M\boldsymbol{t} \geq -k\boldsymbol{\nu}.
\end{aligned}
$$

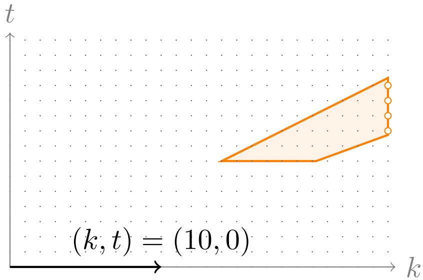
Un ejemplo

$$
\begin{aligned}
\max_{(x,y)\in\mathbb{Z}^2} \quad & 2x+3y \\
\text{s.a.} \quad & 2x+3y \leq 25, \\
& -3x+4y \leq 4, \\
& x+y \geq 7, \\
& x \geq 0, \\
& y \geq 0.
\end{aligned}
$$

$$
\begin{aligned}
\max_{(k,t)\in\mathbb{Z}^2} \quad & k, \\
\text{s.a.} \quad & k \leq 25, \\
& 4k-11t \leq 4, \\
& t \geq 7, \\
& 2t \leq k, \\
& 3t \geq k.
\end{aligned}
$$

Un ejemplo





Sobre los cortes de Ramificación y Acotamiento

Teorema

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

Sobre la separabilidad del Problema Equivalente

Podemos separar (PE) en un problema de maximización

$$\begin{aligned}
\max_{k\in\mathbb{Z},\tilde{\boldsymbol{y}}\in\mathbb{Z}^n} \quad & k, \\
\text{s.a.} \quad & k \leq \eta, \\
& A\tilde{\boldsymbol{y}} = \boldsymbol{b} - kA\boldsymbol{\nu},
\end{aligned}$$

y uno de factibilidad

$$\begin{aligned}
M\boldsymbol{t} &= \tilde{\boldsymbol{y}}, \\
M\boldsymbol{t} &\geq -k^*\boldsymbol{\nu},
\end{aligned}$$

donde k^* es la solución del problema de maximización.

Múltiples restricciones (caso general)

$$
\begin{aligned}
\max_{\boldsymbol{x} \in \mathbb{Z}^n} \quad & \boldsymbol{q}^T \boldsymbol{x}, \\
\text{s.a.} \quad & A\boldsymbol{x} = \boldsymbol{b}, \\
& \boldsymbol{x} \geq \boldsymbol{0}.
\end{aligned}
$$

Conclusión

- Clasificación de programas lineales enteros a partir de isomorfismo de redes.
- Nuevas cotas superiores para el número de Frobenius.
- Generalización para resolver programas lineales enteros con múltiples restricciones.
- Introducción de (PE) que se deshace de subproblemas infactibles rápidamente.
- Exhibición de casos patológicos de Ramificación y Acotamiento.
- Medidas de eficiencia de cortes en Ramificación y Acotamiento.
- Desarrollo de algoritmos basados en métodos diofantinos que superan **una implementación** de Ramificación y Acotamiento en **ciertas instancias**.