PUNTO Y LÍNEA SOBRE EL PLANO

Ecuaciones lineales diofantinas aplicadas a programas lineales enteros

Iñaki Liendo

Coloquio de matemáticas

11 de septiembre de 2025

1. MOTIVACIÓN

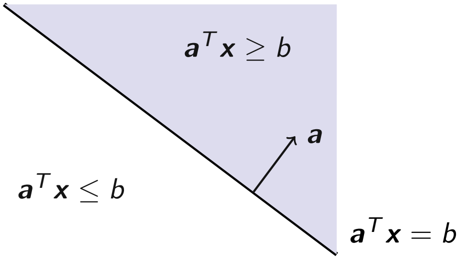
Definición

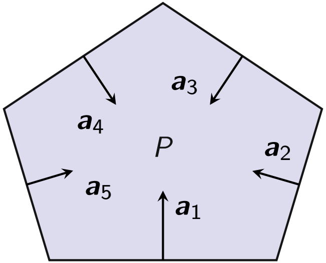
Sea $\boldsymbol{a} \in \mathbb{R}^n$ un vector no nulo y sea $b \in \mathbb{R}$ un escalar. Llamamos **hiperplano afino** al conjunto de vectores $\boldsymbol{x} \in \mathbb{R}^n$ que satisfacen $\boldsymbol{a}^T\boldsymbol{x} = b$. Llamamos **semi-espacios afinos** a los conjuntos de vectores $\boldsymbol{x},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

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


$a^T x \geq b$
a
$a^T x \leq b$
$a^T x = b$


a_3
a_4
P
a_2
a_5
a_1

Definición

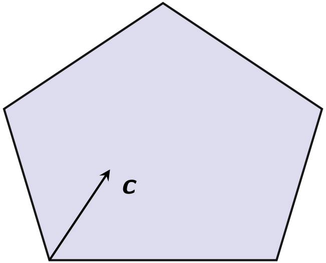
Sea $P \subseteq \mathbb{R}^n$ un poliedro y sea $\boldsymbol{c} \in \mathbb{R}^n$ un vector. Llamamos **problema lineal** al problema de maximización

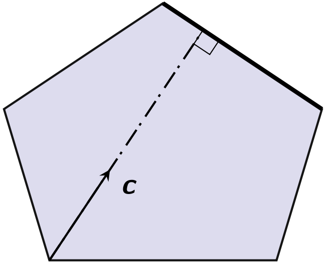
$$z^* := \max_{\boldsymbol{x}}\{\boldsymbol{c}^T \boldsymbol{x} : \boldsymbol{x} \in P\}.$$

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

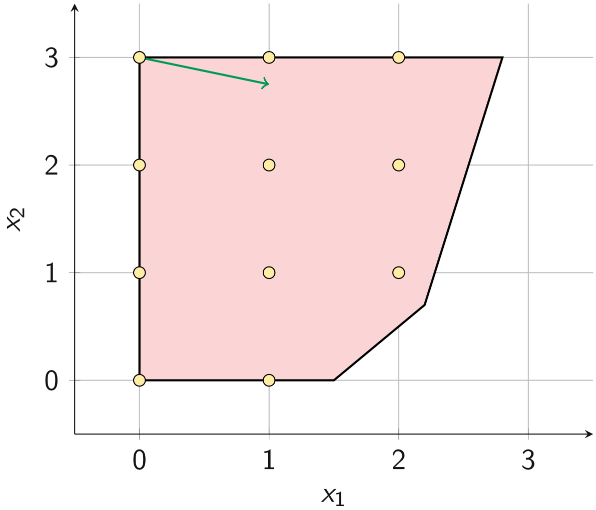
Al problema lineal

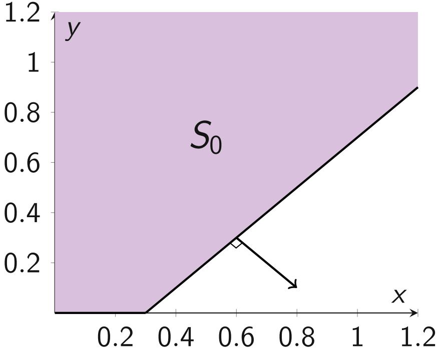
$$z^* := \max_{\boldsymbol{x}}\{\boldsymbol{c}^T\boldsymbol{x} : \boldsymbol{x} \in P\}.$$

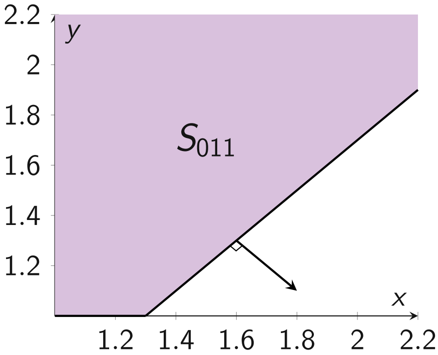
lo llamamos **problema relajado** del **problema lineal entero**

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

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
S_0
x
0.2 0.4 0.6 0.8 1 1.2

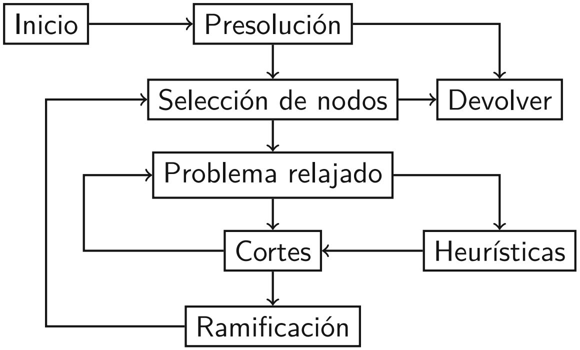


2.2
y
2
1.8
S_{011}
1.6
1.4
1.2
x
1.2 1.4 1.6 1.8 2 2.2

Ramificación y Acotamiento genera la cadena de subproblemas autosimilares

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

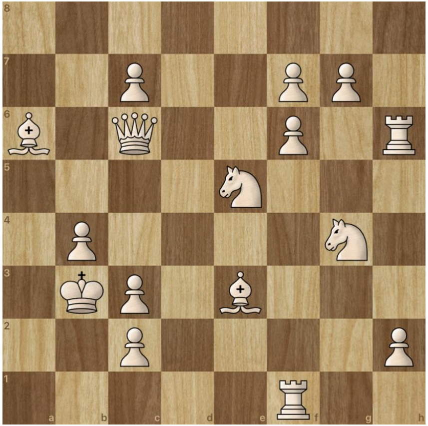
y este método jamás terminará con una solución.


Inicio
Presolución
Selección de nodos
Devolver
Problema relajado
Cortes
Heurísticas
Ramificación

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

$$
\begin{aligned}
\max_{\boldsymbol{x}\in\mathbb{Z}^n} \quad & \boldsymbol{p}^T\boldsymbol{x}, && \text{(1a)}\\
\text{s.a.} \quad & \boldsymbol{p}^T\boldsymbol{x} \le u, && \text{(1b)}\\
& \boldsymbol{x} \ge \mathbf{0}.
\end{aligned}
$$

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 $\boldsymbol{v} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ 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

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

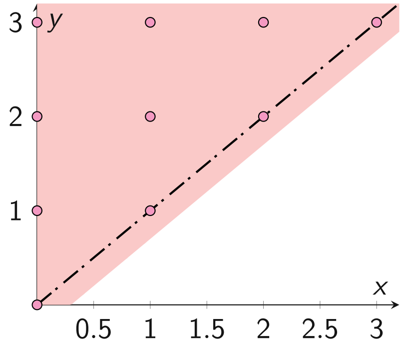
Teorema de infactibilidad (*)

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 (1.1b) es negativo.

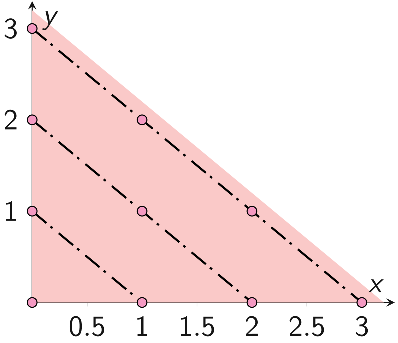
Teorema de factibilidad

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:

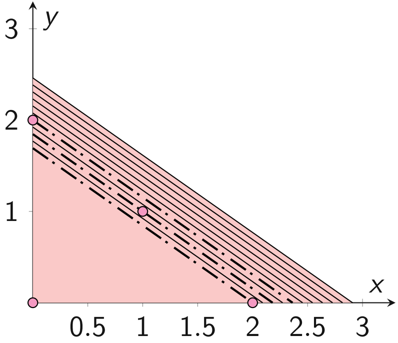
1. Si $q_i < 0$ para algún $i \in \{1, \dots, n\}$, entonces la η-ésima capa entera $H_{\boldsymbol{q},\eta\|\boldsymbol{q}\|^{-2}}$ contiene un número infinito de puntos factibles.
2. Si $\boldsymbol{q} > \mathbf{0}$ entonces, para todo $k \in \{\eta, \eta - 1, \dots, 0\}$, la k-ésima capa entera $H_{\boldsymbol{q},k\|\boldsymbol{q}\|^{-2}}$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

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

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

$$q_1 x_1' + q_2 x_2' = \mathrm{mcd}\{q_1, q_2\} = 1,$$

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 $t_1, \ldots, t_{n-1} \in \mathbb{Z}$ son parámetros libres.

Para que se satisfagan las condiciones de no negatividad de $x_1, \ldots, x_n$, 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 $\boldsymbol{q}$ 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 $\boldsymbol{q} > \mathbf{0}$, 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 $\boldsymbol{\nu} \in \mathbb{Z}^n$ como

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

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 $\boldsymbol{q} \in \mathbb{Z}^n$ un vector con entradas coprimas. Luego, **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 $\boldsymbol{t} \in \mathbb{Z}^{n-1}$.

Lema

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

Definición

Decimos que un subconjunto Λ de $\mathbb{R}^n$ 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, decimos que Λ es una **red** si existen vectores $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ linealmente independientes tales que

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

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

Ejemplo

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

Teorema

El conjunto de vectores

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

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

Definición

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

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

¿Cuál es el tamaño de una órbita? ¿Se puede hacer más grande?

Lema

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

Definición

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

4. SEGUNDO INTENTO DE CLASIFICACIÓN

Corolario

La matriz

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

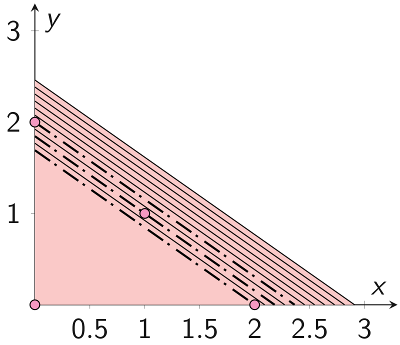
es unimodular, es decir, su determinante es ± 1.

- Podemos "traducir" las descomposiciones $\boldsymbol{q} \mapsto U_{\boldsymbol{q}}$ y $\tilde{\boldsymbol{q}} \mapsto U_{\tilde{\boldsymbol{q}}}$ por medio de $U_{\boldsymbol{q}} U_{\tilde{\boldsymbol{q}}}^{-1}$.
- $\implies$ **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 $q_1, \ldots, q_n$ coprimos, encontrar el mayor entero que **no** puede ser expresado como $q_1 x_1 + \cdots + q_n x_n$, donde $x_1, \ldots, x_n$ son no negativos.



$$11x + 13y \leq 32$$

Teorema

El número de Frobenius F satisface

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

donde

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

6. MÚLTIPLES RESTRICCIONES

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

$$\begin{aligned}
\max_{\boldsymbol{x}\in\mathbb{Z}^n} \quad & \boldsymbol{q}^T\boldsymbol{x}, && \text{(2a)}\\
\text{s.a.} \quad & \boldsymbol{q}^T\boldsymbol{x} \leq \eta, && \text{(2b)}\\
& A\boldsymbol{x} = \boldsymbol{b}, && \text{(2c)}\\
& \boldsymbol{x} \geq \boldsymbol{0}.
\end{aligned}$$

Podemos suponer, sin pérdida de generalidad, que $A \in \mathbb{Z}^{m\times n}$ y $\boldsymbol{b} \in \mathbb{Z}^m$ (¿por qué?).

7. UNA FORMULACIÓN ADYACENTE

Teorema

El problema (2) es equivalente al problema

$$\begin{aligned} \max_{k\in\mathbb{Z},\boldsymbol{t}\in\mathbb{Z}^{n-1}} \quad & k, && \text{(3a)}\\ \text{s.a.} \quad & k \le \eta, && \text{(3b)}\\ & AM\boldsymbol{t} = \boldsymbol{b} - kA\boldsymbol{\nu}, && \text{(3c)}\\ & M\boldsymbol{t} \ge -k\boldsymbol{\nu}. && \text{(3d)} \end{aligned}$$

Intuición.

Sabemos que la transformación lineal

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

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

Teorema (*)

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

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

8. UNA FORMULACIÓN ALTERNATIVA

Como los renglones de $A \in \mathbb{Z}^{m \times n}$ son linealmente independientes, existe una matriz unimodular $U \in \mathbb{Z}^{n \times n}$ que satisface $AU = [H \mid \mathbf{0}]$, donde $H \in \mathbb{Z}^{m \times m}$ es triangular inferior y no singular.

Introducimos el problema de maximización:

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

donde

$$\tilde{\boldsymbol{y}} := U \begin{pmatrix} \tilde{\boldsymbol{y}}_m \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = U_m \tilde{\boldsymbol{y}}_m + U_{n-m}\tilde{\boldsymbol{y}}_{n-m}.$$

Para toda $k \in \mathbb{Z}$ se cumple

$$AU \begin{pmatrix} H^{-1}\left(\boldsymbol{b} - kA\boldsymbol{\nu}\right) \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = [H, \mathbf{0}] \begin{pmatrix} H^{-1}\left(\boldsymbol{b} - kA\boldsymbol{\nu}\right) \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = \boldsymbol{b} - kA\boldsymbol{\nu},$$

lo cual sugiere definir

$$\tilde{\boldsymbol{y}}_m := H^{-1}(\boldsymbol{b} - kA\boldsymbol{\nu}).$$

Debemos asegurarnos que $\tilde{\boldsymbol{y}}_m$ sea entero. Definimos el conjunto de factibilidad del subproblema de maximización como

$$\mathcal{F} := \{k \in \mathbb{Z} \colon H^{-1}\left(\boldsymbol{b} - kA\boldsymbol{\nu}\right) \in \mathbb{Z}^m, k \leq \eta\}$$

Supongamos que $\mathcal{F} \neq \emptyset$ (¿por qué?), entonces tiene un elemento maximal k^* que es solución del subproblema de maximización. Dada esta solución, buscamos resolver el subproblema de factibilidad:

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

Ya tenemos determinado $\tilde{\boldsymbol{y}}_m$, falta encontrar $\tilde{\boldsymbol{y}}_{n-m}$:

$$\begin{aligned} M\boldsymbol{t} = \tilde{\boldsymbol{y}} = U_m\tilde{\boldsymbol{y}}_m + U_{n-m}\tilde{\boldsymbol{y}}_{n-m} \\ \iff [M \mid -U_{n-m}] \begin{pmatrix} \boldsymbol{t} \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = U_m\tilde{\boldsymbol{y}}_m. \end{aligned}$$

Debido a la forma normal de Smith, existen dos matrices unimodulares $S \in \mathbb{Z}^{n\times n}$ y $T \in \mathbb{Z}^{(2n-m-1)\times(2n-m-1)}$ que satisfacen

$$S[M \mid -U_{n-m}]T = D \in \mathbb{Z}^{n\times(2n-m-1)},$$

donde D es una matriz diagonal cuyas n primeras entradas son distintas de cero y las restantes $n-m-1$ son cero. Si multiplicamos S por la izquierda en ambos lados de la ecuación anterior, tenemos

$$DT^{-1}\begin{pmatrix} \boldsymbol{t} \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = SU_m\tilde{\boldsymbol{y}}_m.$$

Si D_{ii} no divide a $(SU_m\tilde{\boldsymbol{y}}_m)_i$ para algua $1 \leq i \leq n$, la primera ecuación del subproblema de factibilidad no tiene solución en los enteros. ¿Qué hacemos?

Supongamos que $D_{ii} \mid (SU_m \tilde{\boldsymbol{y}}_m)_i$ para todo $1 \leq i \leq n$. Obtenemos n soluciones enteras $\boldsymbol{r} \in \mathbb{Z}^n$ y $n - m - 1$ variables libres $\boldsymbol{s} \in \mathbb{Z}^{n-m-1}$:

$$T^{-1} \begin{pmatrix} \boldsymbol{t} \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = \begin{pmatrix} \boldsymbol{r} \\ \boldsymbol{s} \end{pmatrix}.$$

Por lo tanto, nuestro vector $\boldsymbol{t}$ es una función afina de $\boldsymbol{s}$, es decir, $\boldsymbol{t} = \boldsymbol{t}(\boldsymbol{s})$. ¿Qué implica esto para el subproblema de factibilidad?

Consideremos el conjunto de vectores $\boldsymbol{s} \in \mathbb{Z}^{n-m-1}$ que inducen a que $\boldsymbol{t}(\boldsymbol{s})$ satisfaga la desigualdad en el subproblema de factibilidad:

$$\mathcal{S} := \{\boldsymbol{s} \in \mathbb{Z}^{n-m-1} : M\boldsymbol{t}(\boldsymbol{s}) \geq -k^*\boldsymbol{\nu}\}$$

Consideremos el conjunto de vectores $\boldsymbol{s} \in \mathbb{Z}^{n-m-1}$ que inducen a que $\boldsymbol{t}(\boldsymbol{s})$ satisfaga la desigualdad en el subproblema de factibilidad:

$$\mathcal{S} := \{\boldsymbol{s} \in \mathbb{Z}^{n-m-1} : M\boldsymbol{t}(\boldsymbol{s}) \geq -k^*\boldsymbol{\nu}\}$$

1. Encontrar $s \in \mathcal{S}$ es un problema difícil de resolver.

Consideremos el conjunto de vectores $\boldsymbol{s} \in \mathbb{Z}^{n-m-1}$ que inducen a que $\boldsymbol{t}(\boldsymbol{s})$ satisfaga la desigualdad en el subproblema de factibilidad:

$$\mathcal{S} := \{\boldsymbol{s} \in \mathbb{Z}^{n-m-1} : M\boldsymbol{t}(\boldsymbol{s}) \geq -k^{*}\boldsymbol{\nu}\}$$

1. Encontrar $s \in \mathcal{S}$ es un problema difícil de resolver.
2. Calcular $|\mathcal{S}|$ es un problema difícil de resolver.

Consideremos el conjunto de vectores $\boldsymbol{s} \in \mathbb{Z}^{n-m-1}$ que inducen a que $\boldsymbol{t}(\boldsymbol{s})$ satisfaga la desigualdad en el subproblema de factibilidad:

$$\mathcal{S} := \{\boldsymbol{s} \in \mathbb{Z}^{n-m-1} : M\boldsymbol{t}(\boldsymbol{s}) \geq -k^*\boldsymbol{\nu}\}$$

1. Encontrar $s \in \mathcal{S}$ es un problema difícil de resolver.
2. Calcular $|\mathcal{S}|$ es un problema difícil de resolver.
3. Decidir $\mathcal{S} = \emptyset$ es un problema difícil de resolver.

¿Cómo sustituir el problema (3) por un problema lineal entero general?

$$
\begin{aligned}
\max_{\boldsymbol{x}\in\mathbb{Z}^n} \quad & \boldsymbol{q}^T\boldsymbol{x}, && \text{(6a)}\\
\text{s.a.} \quad & A\boldsymbol{x} = \boldsymbol{b}, && \text{(6b)}\\
& \boldsymbol{x} \geq \mathbf{0}.
\end{aligned}
$$

9. GRACIAS