

Ecuaciones lineales diofantinas aplicadas a programas lineales enteros

Iñaki Sebastián Liendo Infante

17 de junio de 2025

Índice general

1. Aspectos Teóricos	2
1.1. Prerrequisitos	2
1.1.1. Teoría de Números	3
1.1.2. Programación lineal	5
1.2. Fundamentos	5
2. El caso infinito	10
3. El caso finito	13

Capítulo 1

Aspectos Teóricos

En este capítulo cimentamos las bases teóricas necesarias para resolver instancias particulares de programas lineales enteros. En primer lugar, la sección de Prerrequisitos recopila resultados básicos de teoría de números y de programación lineal para refrescar la memoria del lector. En segundo lugar, la sección de Fundamentos comienza con definiciones y enunciados obtenidos de [BH09], los cuales utilizaremos para obtener resultados que, en pleno conocimiento del autor, son originales. El problema fundamental que permitirá construir incrementalmente nuestro algoritmo es

$$\max_{\mathbf{x} \in \mathbb{Z}^n} \mathbf{p}^T \mathbf{x}, \quad (1.1a)$$

$$\begin{aligned} \text{s.a. } & \mathbf{p}^T \mathbf{x} \leq u, \\ & \mathbf{x} \geq \mathbf{0}. \end{aligned} \quad (1.1b)$$

Por ello mismo, es razonable suponer que $\mathbf{p}_i \neq 0$ para cualquier $i \in \{1, \dots, n\}$. En la sección de Fundamentos analizaremos a profundidad este problema, cuyo punto de culminación será el Teorema 1.14. Veremos que es recomendable separar en dos partes el análisis de este problema: el caso $p_i < 0$ para alguna $i \in \{1, \dots, n\}$; y el caso $\mathbf{p} \geq \mathbf{0}$. Los siguientes dos capítulos examinarán respectivamente estos casos. Por el momento, cabe destacar que el segundo caso será de mayor interés y tendrá mayor aplicabilidad en problemas reales, pues es una instancia particular del Problema de la Mochila. No obstante, el caso $\mathbf{p}_i < 0$ también será de utilidad para exhibir casos particulares en donde el algoritmo de Ramificación y Acotamiento obtiene un rendimiento deficiente.

1.1. Prerrequisitos

En los siguientes capítulos usaremos extensivamente resultados básicos de teoría de números y de programación lineal, por lo que es provechoso recopilarlos en esta primera sección. En particular, destaca la importancia de las ecuaciones lineales diofantinas para la construcción de nuestro algoritmo. En esta sección el autor consideró pertinente no incluir demostraciones, pues los enunciados son mostrados en cualquier clase de álgebra superior, programación lineal, o investigación de operaciones, por ejemplo. La referencia principal para la parte de teoría de números es [Lav14], mientras que la de programación lineal es [Sch98].

1.1.1. Teoría de Números

Máximo común divisor y mínimo común múltiplo

En primer lugar, introducimos el símbolo de relación “ $|$ ” para indicar divisibilidad. Dados dos enteros a, b , decimos que b divide a a (y escribimos $b \mid a$) si y solo si existe un entero k tal que $a = k \cdot b$. Así también, denotamos el conjunto de divisores de a como

$$D(a) := \{b \in \mathbb{Z} : b \mid a\}.$$

Si a es distinto de cero, encontramos que $D(a)$ es finito, puesto que si $b \mid a$, entonces $|b| \leq |a|$, lo cual implica que $|D(a)| \leq 2|a|$. En caso de que a sea nulo, obtenemos $D(a) = \mathbb{Z}$. Observemos también que $\{-1, 1\} \subseteq D(a)$ para todo entero a .

Definición 1.1. Sean a_1, \dots, a_n enteros no todos iguales a cero, entonces definimos su máximo común divisor d como el elemento maximal del conjunto $\bigcap_{i=1}^n D(a_i)$, y escribimos $d = \text{mcd}\{a_1, \dots, a_n\}$. Si $d = 1$, entonces decimos que a_1, \dots, a_n son coprimos.

Puesto que $a_i \neq 0$ para alguna i en la definición anterior, encontramos que el conjunto $\bigcap_{i=1}^n D(a_i)$ es finito y, como también es no vacío, en efecto existe un elemento maximal. Es decir, el máximo común divisor d siempre está bien definido.

Observación. No porque una colección de enteros sea coprime ($\text{mcd}\{a_1, \dots, a_n\} = 1$) se sigue que estos enteros sean coprimos a pares ($\text{mcd}\{a_i, a_j\} = 1$ para todo i, j). Por ejemplo, los enteros 1, 3 y 3 son coprimos pero evidentemente 3 y 3 no lo son.

Definición 1.2. Decimos que $c \in \mathbb{Z}$ es una combinación lineal entera de un conjunto de enteros a_1, \dots, a_n si existen enteros x_1, \dots, x_n tales que $c = a_1x_1 + \dots + a_nx_n$.

El siguiente teorema, a pesar de su simpleza, es central para los resultados obtenidos en esta tesis.

Teorema 1.3. Sea d un entero y sean a_1, \dots, a_n una colección de enteros no todos iguales a cero. Entonces $d = \text{mcd}\{a_1, \dots, a_n\}$ si y solo si d es la mínima combinación lineal entera positiva de a_1, \dots, a_n .

Corolario 1.4. Si $d = \text{mcd}\{a_1, \dots, a_n\}$, entonces $\text{mcd}\{\frac{a_1}{d}, \dots, \frac{a_n}{d}\} = 1$.

Además del máximo común divisor, requeriremos al mínimo común múltiplo, empero en menor medida. Sea a un entero y denotamos el conjunto de sus múltiplos como

$$M(a) := \{x \in \mathbb{Z} : a \mid x\}.$$

Si a es nulo, entonces $M(a) = \{0\}$. En caso contrario encontramos que $M(a)$ es un conjunto infinito. Análogamente a la Definición 1.1, definimos el mínimo común múltiplo m de una colección de enteros $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ como el elemento minimal de $\mathbb{N} \cap \bigcap_{i=1}^n M(a_i)$. Escribimos $m = \text{mcm}\{a_1, \dots, a_n\}$. Para observar que está bien definido, basta mencionar que el producto $|a_1 \cdots a_n|$ es un elemento de la intersección y por lo tanto esta es no vacía.

Ecuaciones lineales diofantinas

Sea $c \in \mathbb{Z}$ y sean a_1, \dots, a_n enteros. Una ecuación lineal diofantina es una ecuación donde queremos encontrar enteros x_1, \dots, x_n que satisfagan

$$a_1x_1 + \dots + a_nx_n = c.$$

Será de nuestro interés en las siguientes secciones resolver iterativamente este tipo de ecuaciones. Por el momento basta mencionar que podemos enfocarnos en el caso $n = 2$ sin ninguna pérdida de generalidad. No obstante, los resultados se mantienen para cualquier $n \in \mathbb{N}$. Los siguientes enunciados abordan el problema de determinar existencia y unicidad para las ecuaciones lineales diofantinas, así como la construcción de sus soluciones.

Teorema 1.5 (Existencia). *Sean $a, b \in \mathbb{Z}$, no ambos cero. La ecuación $ax + by = c$ tiene solución si y solo si $\text{mcd}\{a, b\} \mid c$.*

Para construir el conjunto de soluciones a una ecuación lineal diofantina, encontramos primero una solución particular.

Definición 1.6. *Sea $d := \text{mcd}\{a, b\}$ y sean x', y' enteros tales que $ax' + by' = d$ (c.f. 1.3). Decimos entonces que x', y' son coeficientes de Bézout asociados a a, b , respectivamente.*

Observación. Los coeficientes de Bézout asociados a un par de enteros no son únicos. En efecto, si x', y' son coeficientes de Bézout de a, b , entonces $x' + b, y' - a$ también lo son:

$$a(x' + b) + b(y' - a) = ax' + by' + ab - ab = ax' + by' = d.$$

Para fines de esta tesis basta la existencia de estos coeficientes, por lo que decimos de manera indistinta “los coeficientes de Bézout” y “una elección de coeficientes de Bézout”.

Definamos $d := \text{mcd}\{a, b\}$ y supongamos que la ecuación $ax + by = c$ tiene solución. Entonces $d \mid c$, por lo que existe $c' \in \mathbb{Z}$ tal que $c = c' \cdot d$. Sean x', y' los coeficientes de Bézout asociados a a, b respectivamente. Así,

$$a(c' \cdot x') + b(c' \cdot y') = c'(ax' + by') = c'd = c,$$

por lo que $(c' \cdot x', c' \cdot y')$ es una solución particular de la ecuación $ax + by = c$.

Teorema 1.7 (Construcción). *Sea (x_0, y_0) una solución particular de la ecuación lineal diofantina $ax + by = c$. Entonces todas las soluciones de la ecuación están dadas por*

$$\begin{cases} x = x_0 + \frac{b}{d}t, \\ y = y_0 - \frac{a}{d}t, \end{cases} \quad (1.2)$$

donde $d := \text{mcd}\{a, b\}$ y $t \in \mathbb{Z}$.

1.1.2. Programación lineal

1.2. Fundamentos

Esta sección constituye el primer paso para la construcción de nuestro algoritmo. Se divide en dos partes. Primeramente damos a conocer las definiciones y enunciados provistos por [BH09], al mismo tiempo que hacemos un par de observaciones. Esta primera parte puede darse por concluida una vez citado el Teorema 1.12. Así también, es importante aclarar que el autor tradujo libremente algunos términos a falta de encontrar fuentes en español que hicieran uso de ellos. A saber, el autor decidió nombrar “vectores esencialmente enteros” a los *projectively rational vectors* y “capas enteras” a los *c-layers* en las Definiciones 1.8 y 1.10, respectivamente.

En la segunda parte de esta sección comenzamos con nuestro análisis del problema (1.1). La razón de considerarlo fundamental para esta tesis fue mencionado en el capítulo de Motivación, pero lo repetimos una vez más: en esta clase de problemas el vector es ortogonal a la única restricción, y esto implica que el problema relajado tenga una infinidad de soluciones. Hemos observado que, en presencia de este fenómeno, el algoritmo de Ramificación y Acotamiento no divide la región factible de manera óptima. Por ello investigamos formas alternativas para atacar este problema antes de hacer la separación de casos $\mathbf{p}_i < 0$ o $\mathbf{p} \geq 0$.

Definición 1.8. *Decimos que un vector $\mathbf{v} \in \mathbb{R}^n \setminus \{0\}$ es esencialmente entero si existe un vector $\mathbf{w} \in \mathbb{Z}^n$ y un escalar $k \in \mathbb{R}$ tal que $\mathbf{v} = k\mathbf{w}$. Además, decimos que \mathbf{w} es el múltiplo coprimo de \mathbf{v} si sus entradas son coprimas (c.f. Definición 1.1) y si su primera entrada \mathbf{v}_1 es no negativa.*

En otras palabras, decimos que \mathbf{v} es esencialmente entero si es un múltiplo real de un vector entero.

Ejemplo 1.9. *El vector $(-\sqrt{2}, 1/\sqrt{2})^T = \sqrt{2}(-1, 1/2)^T$ es esencialmente entero y $(2, -1)^T$ es su múltiplo coprimo. Contrariamente, el vector $(\sqrt{2}, \sqrt{3})^T$ no es esencialmente entero.*

Observación. Todo vector \mathbf{v} cuyas entradas son racionales ($\mathbf{v} \in \mathbb{Q}^n$) es esencialmente entero. En efecto, $\mathbf{v}_i = \frac{p_i}{q_i}$ para algunos enteros p_i y q_i con q_i distinto de cero. Si definimos $q := \text{mcm}\{q_1, \dots, q_n\} \neq 0$ y $\mathbf{w} := q\mathbf{v}$, se sigue que $\mathbf{v} = \frac{1}{q}\mathbf{w}$ y también $\mathbf{w} \in \mathbb{Z}^n$.

Observación. Todo vector \mathbf{v} esencialmente entero tiene a lo más dos vectores coprimos asociados. Sean $k \in \mathbb{R}$ y $\mathbf{w} \in \mathbb{Z}^n$ tales que $\mathbf{v} = k\mathbf{w}$. Entonces

$$\pm \frac{1}{\text{mcd}\{\mathbf{w}_1, \dots, \mathbf{w}_n\}} \mathbf{w}$$

son dos vectores cuyas entradas son coprimas, de acuerdo al Corolario 1.4. Si $\mathbf{w}_1 = 0$, estos representan el mismo vector, y si $\mathbf{w}_1 \neq 0$ entonces solo uno de estos dos vectores es el múltiplo coprimo de \mathbf{v} . Independientemente del caso, el múltiplo coprimo de todo vector esencialmente entero es único.

Porque todo número representable en cualquier sistema de aritmética finita es necesariamente racional, decidimos enfocar nuestro análisis en vectores esencialmente enteros. Desde

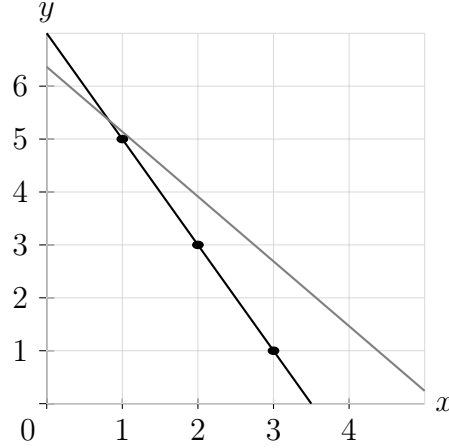


Figura 1.1: Representación de una capa entera (en negro) junto a un hiperplano afino que no es capa entera (en gris). La capa entera tiene como parámetros $\mathbf{v} = (2, 1)^T$ y $t = 1, 4$, mientras que los del hiperplano afino son $\mathbf{v} = (\sqrt{3}, \sqrt{2})^T$ y $t = 1, 4$.

el punto de vista puramente teórico, esta condición reduce drásticamente el tipo de programas lineales que podemos resolver. No obstante, esta clase de vectores es un poco más general que los considerados en otros textos de programación lineal, por ejemplo, [MT90] y [Sch98] toman en cuenta vectores puramente racionales. En [BH09] se revelan propiedades de los vectores esencialmente enteros que reproducimos aquí y que nos permitirán plantear ecuaciones lineales diofantinas cuyas soluciones otorgan candidatos para puntos óptimos de un problema lineal.

Definición 1.10. 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

$$H_{\mathbf{v},t} := \ker\{\mathbf{x} \mapsto \mathbf{v}^T \mathbf{x}\} + t\mathbf{v} = \{\mathbf{v}^\perp + t\mathbf{v} : \mathbf{v}^T \mathbf{v}^\perp = 0\} \quad (1.3)$$

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

Observemos que todo hiperplano afino $H_{\mathbf{v},t}$ es invariante ante reescalamientos en \mathbf{v} . Es decir, si $r \in \mathbb{R} \setminus \{0\}$ es un escalar, entonces $H_{\mathbf{v},t} = H_{r\mathbf{v},t/r}$. En particular, el conjunto de hiperplanos afinos asociados a un vector \mathbf{v} esencialmente entero es igual al conjunto de hiperplanos afinos asociados a su múltiplo coprimo \mathbf{w} . Ahora bien, cualquier vector coprimo induce una familia de capas enteras y, sorprendentemente, esa familia forma una cobertura de \mathbb{Z}^n , como lo indica el Teorema 1.12.

Lema 1.11. Sean $\mathbf{v}, \mathbf{x} \in \mathbb{R}^n$ con \mathbf{v} distinto de cero. Entonces $\mathbf{x} \in H_{\mathbf{v},t_{\mathbf{x}}}$, donde $t_{\mathbf{x}} := \frac{\mathbf{v}^T \mathbf{x}}{\|\mathbf{v}\|^2}$.

Teorema 1.12. 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 .

Pasemos a considerar el programa lineal (1.1) donde \mathbf{p} es un vector esencialmente entero y \mathbf{q} es su múltiplo coprimo. Supongamos que $\mathbf{p}_i \neq 0$ para todo $i \in \{1, \dots, n\}$, por lo que también se cumple que $\mathbf{q}_i \neq 0$. Comúnmente a la función objetivo (1.1a) le daremos el

nombre de utilidad y a la restricción (1.1b) la llamaremos restricción presupuestaria, así como presupuesto al lado derecho de esta restricción.

Observación. Debido a la restricción presupuestaria, encontramos que el politopo está acotado por arriba. Así pues, el problema o bien es infactible, o bien tiene una utilidad finita.

Cada escalar $t \in \mathbb{R}$ induce un hiperplano afino $H_{\mathbf{p},t}$ donde se cumple que todo punto $\mathbf{x} \in H_{\mathbf{p},t}$ tiene un mismo nivel de utilidad. Como observamos previamente,

$$\{H_{\mathbf{p},t} : t \in \mathbb{R}\} = \{H_{\mathbf{q},t} : t \in \mathbb{R}\}.$$

A causa del Teorema 1.12, somos capaces de caracterizar todos los puntos enteros a partir de \mathbf{q} . Aún más, obtenemos una enumeración de las capas enteras que cubren \mathbb{Z}^n , lo cual nos permite determinar si la k -ésima capa entera contiene puntos factibles para el problema.

El nivel de utilidad para la k -ésima capa entera es k . En efecto, si $\mathbf{x} \in H_{\mathbf{q},k\|\mathbf{q}\|^{-2}}$, tenemos

$$\mathbf{x} = \mathbf{q}^\perp + k\|\mathbf{q}\|^{-2}\mathbf{q},$$

donde \mathbf{q}^\perp es un vector ortogonal a \mathbf{q} . Por lo tanto,

$$\mathbf{q}^T \mathbf{x} = \mathbf{q}^T \mathbf{q}^\perp + k\|\mathbf{q}\|^{-2} \mathbf{q}^T \mathbf{q} = 0 + k\|\mathbf{q}\|^{-2} \|\mathbf{q}\|^2 = k.$$

Para respetar la restricción presupuestaria, podemos encontrar el entero η más grande que satisfaga $\mathbf{q}^T \mathbf{x} \leq u$ para todo $\mathbf{x} \in H_{\mathbf{q},\eta\|\mathbf{q}\|^{-2}}$. Diremos que η es el primer entero que satisface la restricción presupuestaria, o bien que $H_{\mathbf{q},\eta\|\mathbf{q}\|^{-2}}$ es la primera capa entera que satisface el presupuesto. De esta manera, encontramos que las capas enteras que satisfacen el presupuesto son parametrizadas por $k \in \{\eta, \eta - 1, \dots\}$. Debido a la observación anterior, se cumple inmediatamente que $\mathbf{q}^T \mathbf{x} = k$. Deducimos que si la η -ésima capa entera contiene puntos no negativos, entonces las soluciones se encuentran en esa capa. En caso contrario, descendemos a la $(\eta - 1)$ -ésima capa entera y buscamos puntos enteros no negativos, etcétera.

Lema 1.13. 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 $m \in \mathbb{R} \setminus \{0\}$. Entonces la primera capa entera $H_{\mathbf{q},\eta\|\mathbf{q}\|^{-2}}$ que satisface el presupuesto está parametrizada por $\eta := \lfloor u/m \rfloor$.

Demostración. Sea \mathbf{x} tal que $\mathbf{p}^T \mathbf{x} \leq u$. Entonces buscamos el mayor entero η que satisfaga $\mathbf{q}^T \mathbf{x} \leq u/m$ para todo $\mathbf{x} \in H_{\mathbf{q},\eta\|\mathbf{q}\|^{-2}}$. Por el Lema 1.11 sabemos que

$$\eta\|\mathbf{q}\|^{-2} = \frac{\mathbf{q}^T \mathbf{x}}{\|\mathbf{q}\|^2} \leq \frac{u/m}{\|\mathbf{q}\|^2},$$

de donde se sigue inmediatamente que $\eta = \lfloor u/m \rfloor$. □

Teorema 1.14. Sea $\mathbf{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea \mathbf{q} su múltiplo coprimo. Entonces se cumple lo siguiente con respecto al problema (1.1):

1. El problema es infactible si y solo si $\mathbf{q} > \mathbf{0}$ y $u < 0$.
2. Si $\mathbf{q}_i < 0$ para algún $i \in \{2, \dots, n\}$, entonces la η -ésima capa entera contiene un número infinito de puntos factibles.

3. Si el problema es factible y $\mathbf{q} > \mathbf{0}$, entonces la k -ésima capa entera contiene un número finito de puntos factibles, donde $k \in \{\eta, \eta - 1, \dots, 0\}$.

Demostración.

1. Supongamos que $\mathbf{q} \geq \mathbf{0}$ y $u < 0$. Si $\mathbf{x} \in \mathbb{Z}_{\geq \mathbf{0}}^n$ entonces $\mathbf{q}^T \mathbf{x} \geq 0 > u$ y por lo tanto \mathbf{x} no es factible. Luego,

$$\mathbb{Z}_{\geq \mathbf{0}}^n \cap \{\mathbf{x} : \mathbf{q}^T \mathbf{x} \leq u\} = \emptyset,$$

y el problema no es factible. Mostramos la otra implicación por contraposición. Si $u \geq 0$ observamos que $\mathbf{0}$ es factible. Se debe cumplir $u < 0$. Similarmente, si $\mathbf{q}_i < 0$ para algún $i \in \{2, \dots, n\}$, encontramos que $\lceil u/\mathbf{q}_i \rceil \mathbf{e}_i \in \mathbb{Z}^n$ es factible:

$$\mathbf{q}^T \left\lceil \frac{u}{\mathbf{q}_i} \right\rceil \mathbf{e}_i = \mathbf{q}_i \left\lceil \frac{u}{\mathbf{q}_i} \right\rceil \leq \mathbf{q}_i \frac{u}{\mathbf{q}_i} = u,$$

además, como $u < 0$, concluimos que $\lceil u/\mathbf{q}_i \rceil \mathbf{e}_i$ es no negativo.

2. Como \mathbf{q} es un vector cuyas entradas son coprimas, sabemos de una generalización del Teorema 1.5 que existe $\mathbf{x} \in \mathbb{Z}^n$ tal que $\mathbf{q}^T \mathbf{x} = \eta$. Definamos los siguientes conjuntos de índices

$$I^+ := \{i : q_i > 0\}, \quad I^- := \{i : q_i < 0\}.$$

Cabe resaltar que estos dos conjuntos forman una partición de $\{1, \dots, n\}$. Podemos escoger escalares positivos c_1, \dots, c_n que satisfagan simultáneamente

$$x_j + \sum_{i \in I^+} \mathbf{q}_i c_i \geq 0, \quad \forall j \in I^-, \tag{1.4}$$

$$x_i - \sum_{j \in I^-} \mathbf{q}_j c_j \geq 0, \quad \forall i \in I^+. \tag{1.5}$$

Definamos el vector $\mathbf{x}^+ \in \mathbb{Z}^n$ de manera que

$$\mathbf{x}_k^+ := \begin{cases} x_k + \sum_{i \in I^+} \mathbf{q}_i c_i, & k \in I^-, \\ x_k - \sum_{j \in I^-} \mathbf{q}_j c_j, & k \in I^+. \end{cases}$$

Se verifica que \mathbf{x}^+ es no negativo y, además,

$$\begin{aligned} \mathbf{q}^T \mathbf{x}^+ &= \mathbf{q}^T \mathbf{x} + \sum_{k \in I^-} \sum_{i \in I^+} \mathbf{q}_k \mathbf{q}_i c_i - \sum_{k \in I^+} \sum_{j \in I^-} \mathbf{q}_k \mathbf{q}_j c_j \\ &= \eta + \sum_{j \in I^-} \sum_{i \in I^+} \mathbf{q}_j \mathbf{q}_i c_i - \sum_{i \in I^+} \sum_{j \in I^-} \mathbf{q}_i \mathbf{q}_j c_i \\ &= \eta. \end{aligned}$$

Así pues, tenemos existencia. Para concluir que hay un número infinito de puntos, basta observar que si la elección de coeficientes c_1, \dots, c_n satisface ambas desigualdades (1.4) y (1.5), entonces cualquier múltiplo positivo de estos coeficientes también las satisface.

3. Se sigue que $u \geq 0$. Definamos

$$P_k := H_{\mathbf{q}, k\|\mathbf{q}\|^{-2}} \cap \mathbb{Z}_{\geq \mathbf{0}}^n = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{q}^T \mathbf{x} = k, \mathbf{x} \geq \mathbf{0}\}. \quad (1.6)$$

Observemos que $P_k = \emptyset$ para todo k negativo, pues $\mathbf{q} > \mathbf{0}$ y por lo tanto $\mathbf{q}^T \mathbf{x} \geq 0$ para cualquier \mathbf{x} no negativo. Esto implica que ningún punto sobre capas enteras con parámetros negativos es factible.

Sea $k \in \{\eta, \eta - 1, \dots, 0\}$. La capa entera $H_{\mathbf{q}, k\|\mathbf{q}\|^{-2}}$ interseca los ejes positivos en $\frac{k}{q_i} \mathbf{e}_i$. Definamos $\ell_i := \lceil k/q_i \rceil$. No es difícil ver que $H_{\mathbf{q}, k\|\mathbf{q}\|^{-2}}$ está contenido en el prisma cuyas aristas son $[0, \ell_i]$ y, por lo tanto,

$$P_k \subseteq \prod_{i=1}^n [0, \ell_i] \cap \mathbb{Z}^n = \prod_{i=1}^n ([0, \ell_i] \cap \mathbb{Z}).$$

Pero $|[0, \ell_i] \cap \mathbb{Z}| = \ell_i + 1$. Así,

$$|P_k| \leq \prod_{i=1}^n (\ell_i + 1) < \infty.$$

Entonces la k -ésima capa entera contiene un número finito de puntos factibles.

□

Corolario 1.15. Si $q_i < 0$ para algún $i \in \{2, \dots, n\}$, entonces el valor óptimo del problema (1.1) es $m\eta$ y existe una infinidad de soluciones.

Demostración. Por el Teorema anterior sabemos que existen una infinidad de soluciones, así que sea \mathbf{x}^* una de ellas. Entonces $\mathbf{q}^T \mathbf{x}^* = \eta$, pero $\mathbf{p} = m\mathbf{q}$, por lo que obtenemos $\mathbf{p}^T \mathbf{x}^* = m\eta$. □

Concluimos este capítulo con lo siguiente. Suponiendo que el problema (1.1) tiene solución, el Teorema 1.14 nos sugiere dividir nuestro análisis en dos casos: uno donde \mathbf{p}_i es negativo y por lo tanto hay una infinidad de soluciones en la η -ésima capa entera; y uno donde $\mathbf{p} > \mathbf{0}$, lo que implica la finitud de puntos factibles. Ciertamente el segundo caso es el más interesante, pues de alguna manera conocemos automáticamente el óptimo de los problemas que recaen en el primer caso. Efectivamente esta es una de las razones por las que el autor decidió ordenar de tal manera los casos: porque en el primero sabemos exactamente dónde buscar la solución. Sobra decir que las técnicas que desarrollemos en el siguiente capítulo, el del caso infinito, serán de gran utilidad para analizar el caso más interesante.

Capítulo 2

El caso infinito

Los puntos enteros que se encuentran en la η -ésima capa entera satisfacen la ecuación lineal diofantina

$$\mathbf{q}^T \mathbf{x} = q_1 x_1 + q_2 x_2 + \cdots + q_n x_n = \eta. \quad (2.1)$$

En la sección de Teoría de Números mostramos bajo qué condiciones existen soluciones a este tipo de ecuaciones y también cómo construirlas cuando solamente tenemos dos incógnitas. Por conveniencia definamos $g_1 := \text{mcd}\{q_1, \dots, q_n\} = 1$ y $\omega_1 := \eta$. De manera análoga a una formulación de programación dinámica hacia adelante, podemos definir también $g_2 := \text{mcd}\left\{\frac{q_2}{g_1}, \dots, \frac{q_n}{g_1}\right\}$, con lo que la ecuación anterior es equivalente a la ecuación

$$\frac{q_1}{g_1} x_1 + g_2 \underbrace{\left(\frac{q_2}{g_2 \cdot g_1} x_2 + \cdots + \frac{q_n}{g_2 \cdot g_1} x_n \right)}_{:= \omega_2} = \omega_1. \quad (2.2)$$

No es difícil observar que $\text{mcd}\left\{\frac{q_1}{g_1}, g_2\right\} = 1$ y por lo tanto existen soluciones enteras para todo $\omega_1 \in \mathbb{Z}$. Como estos coeficientes son coprimos, encontramos que sus coeficientes de Bézout asociados (c.f. Definición 1.6) x'_1, ω'_2 son soluciones particulares de la ecuación

$$\frac{q_1}{g_1} x_1 + g_2 \omega_2 = 1,$$

con lo que las soluciones de la ecuación (2.2) están dadas por

$$\begin{cases} x_1 = \omega_1 x'_1 + g_2 t_1, \\ \omega_2 = \omega_1 \omega'_2 - \frac{q_1}{g_1} t_1, \end{cases}$$

donde $t_1 \in \mathbb{Z}$. Como la restricción de no negatividad se debe satisfacer ($x_1 \geq 0$), encontramos que

$$t_1 \geq \left\lceil -\frac{\omega_1 x'_1}{g_2} \right\rceil.$$

Siguiendo el razonamiento de la formulación dinámica en (2.2), fijamos t_1 y resolvemos la ecuación

$$\frac{q_2}{g_2 \cdot g_1} x_2 + \frac{q_3}{g_2 \cdot g_1} x_3 + \cdots + \frac{q_n}{g_2 \cdot g_1} x_n = \omega_2.$$

Por construcción, los coeficientes de las incógnitas en el lado izquierdo de la ecuación son coprimos y por lo tanto existen una infinidad de soluciones para todo $\omega_2 \in \mathbb{Z}$. Por el mismo razonamiento que el anterior, encontramos que las soluciones son

$$\begin{cases} x_2 = \omega_2 x'_2 + g_3 t_2, \\ \omega_3 = \omega_2 \omega'_3 - \frac{q_2}{g_2 \cdot g_1} t_2, \end{cases}$$

donde $t_2 \in \mathbb{Z}$ es un parámetro, ω_3 y g_3 están definidos de forma análoga al paso anterior, y x'_2, ω'_3 son los coeficientes de Bézout asociados a $\frac{q_2}{g_2 \cdot g_1}$ y g_3 , respectivamente. Por la restricción de no negatividad ($x_2 \geq 0$), se debe cumplir

$$t_2 \geq \left\lceil -\frac{\omega_2 x'_2}{g_3} \right\rceil.$$

De manera general, en el i -ésimo paso de la formulación dinámica para $i \in \{1, \dots, n-2\}$, encontramos

$$\begin{cases} x_i = \omega_i x'_i + g_{i+1} t_i, \\ \omega_{i+1} = \omega_i \omega'_{i+1} - \frac{q_i}{\prod_{j=1}^i g_j} t_i, \end{cases} \quad (2.3)$$

donde $t_i \in \mathbb{Z}$ satisface, debido a la restricción de no negatividad,

$$t_i \geq \left\lceil -\frac{\omega_i x'_i}{g_{i+1}} \right\rceil. \quad (2.4)$$

Finalmente, en el último paso, obtenemos la ecuación lineal diofantina

$$\frac{q_{n-1}}{\prod_{j=1}^{n-2} g_j} x_{n-1} + \frac{q_n}{\prod_{j=1}^{n-2} g_j} x_n = \omega_{n-1}. \quad (2.5)$$

Nuevamente, los coeficientes de las incógnitas son coprimos. Por lo tanto, las soluciones están dadas por

$$\begin{cases} x_{n-1} = \omega_{n-1} x'_{n-1} + \frac{q_n}{\prod_{j=1}^{n-2} g_j} t_{n-1}, \\ x_n = \omega_{n-1} x'_n - \frac{q_{n-1}}{\prod_{j=1}^{n-2} g_j} t_{n-1}, \end{cases} \quad (2.6)$$

Para que ahora se satisfagan las condiciones de no negatividad de x_{n-1} y de x_n , encontramos que $t_{n-1} \in \mathbb{Z}$ debe cumplir ciertas desigualdades según los signos de q_{n-1} y de q_n . Por conveniencia, definamos

$$b_1 := -\frac{\omega_{n-1} x'_{n-1}}{q_n} \cdot \prod_{j=1}^{n-2} g_j, \quad b_2 := \frac{\omega_{n-1} x'_n}{q_{n-1}} \cdot \prod_{j=1}^{n-2} g_j.$$

Entonces se verifica que

$$t_{n-1} \in \begin{cases} [\lceil b_1 \rceil, \lceil b_2 \rceil] & \text{si } 0 < q_{n-1}, q_n, \\ [\lceil b_2 \rceil, \lceil b_1 \rceil] & \text{si } q_{n-1}, q_n < 0, \\ [\lceil \max\{b_1, b_2\} \rceil, \infty) & \text{si } q_{n-1} < 0 < q_n, \\ (-\infty, \lfloor \min\{b_1, b_2\} \rfloor] & \text{si } q_n < 0 < q_{n-1}. \end{cases} \quad (2.7)$$

Como supusimos que el problema es factible, existe un vector de parámetros $\mathbf{t} \in \mathbb{Z}^{n-1}$ que satisface las desigualdades (2.4) y (2.7) y por lo tanto que provee una solución al problema (1.1). Para encontrar estos parámetros, usamos la técnica de *backtracking*, en donde hacemos una elección de $t_1, \dots, t_{n-2} \in \mathbb{Z}$ que satisfagan (2.4) y determinamos si existe $t_{n-1} \in \mathbb{Z}$ que satisfaga (2.7). En caso de que no exista tal parámetro, cambiamos nuestra elección de t_1, \dots, t_{n-2} . Ciertamente la decisión más simple es realizar el cambio $t_{n-2} \leftarrow t_{n-2} - 1$. Cabe destacar que si los signos de q_{n-1} y q_n son distintos, entonces no es necesario realizar *backtracking*, pues el algoritmo termina en la primera iteración. Independientemente del caso, eventualmente obtendremos un vector de parámetros \mathbf{t} que satisfaga las desigualdades necesarias y, por lo tanto, eventualmente obtendremos un punto entero óptimo.

Capítulo 3

El caso finito

Debido a que $\mathbf{p} > \mathbf{0}$, resulta valioso mencionar que el problema (1.1) es una instancia particular del famoso Problema de la Mochila

$$\max_{\mathbf{x} \in \mathbb{Z}^n} \mathbf{u}^T \mathbf{x}, \quad (3.1a)$$

$$\text{s.a. } \mathbf{w}^T \mathbf{x} \leq c, \quad (3.1b)$$

$$\mathbf{x} \geq \mathbf{0}, \quad (3.1c)$$

donde los vectores positivos $\mathbf{u}, \mathbf{w} \in \mathbb{Z}^n$ son conocidos como vector de útiles y vector de pesos, respectivamente. Puesto que no acotamos \mathbf{x} , el problema recibe el nombre de Problema de la Mochila no Acotado. Pero también como $\mathbf{u} = \mathbf{w}$, el problema también puede ser considerado como un Problema de la Suma de Conjuntos no Acotado. En nuestro análisis de resultados comparamos los tiempos de terminación de nuestro algoritmo con los de Ramificación y Acotamiento, MTU2 ([MT90]), y una formulación alternativa de programación dinámica.

De acuerdo al Teorema 1.14, el número de puntos factibles sobre la η -ésima capa entera es finito y, por lo tanto, puede ser cero. No obstante, al igual que en la sección anterior, somos capaces de caracterizar todos los puntos enteros que se encuentran en cualquier capa entera. Consecuentemente, si determinamos que no hay ningún punto factible en la η -ésima capa entera, descendemos a la $(\eta - 1)$ -ésima capa entera y realizamos el mismo análisis.

Además, observemos que en realidad es suficiente con descender hasta la 0-ésima capa entera, pues los puntos enteros sobre capas menores tienen utilidades negativas. De acuerdo al Teorema 1.14, estos no pueden ser factibles. Concluimos entonces que basta con analizar las capas enteras con parámetros $k \in \{\eta, \eta - 1, \dots, 0\}$ y terminamos una vez que encontremos un punto no negativo.

Así pues, sea $k \in \{\eta, \eta - 1, \dots, 0\}$. Al igual que en el caso anterior, deseamos resolver la ecuación lineal diofantina

$$\mathbf{q}^T \mathbf{x} = q_1 x_1 + q_2 x_2 + \dots + q_n x_n = k.$$

Implementamos la misma estrategia para plantear una formulación dinámica,

$$\frac{q_1}{g_1} x_1 + g_2 \omega_2 = \omega_1.$$

No obstante, en este caso podemos interpretar ω_2 de tal manera que obtengamos más información. Así como $\omega_1 := k$ es el presupuesto disponible en un inicio, ω_2 es el presupuesto disponible después de utilizar parte de él para adquirir $x_1 \geq 0$ unidades. Por lo tanto, es posible agregar la restricción $\omega_2 \geq 0$. Similarmente, en el i -ésimo paso de la formulación dinámica, somos capaces de agregar la restricción de que el presupuesto restante ω_{i+1} sea no negativo. Combinando esto con la no negatividad de x_i , obtenemos de (2.3),

$$\left\lceil -\frac{\omega_i x'_i}{g_{i+1}} \right\rceil \leq t_i \leq \left\lfloor \frac{\omega_i \omega'_{i+1}}{q_i} \prod_{j=1}^i g_j \right\rfloor. \quad (3.2)$$

para todo $i \in \{1, \dots, n-2\}$. Después, como $0 < q_{n-1}, q_n$, se sigue de (2.6),

$$\left\lceil -\frac{\omega_{n-1} x'_{n-1}}{q_n} \cdot \prod_{j=1}^{n-2} g_j \right\rceil \leq t_{n-1} \leq \left\lfloor \frac{\omega_{n-1} x'_n}{q_{n-1}} \cdot \prod_{j=1}^{n-2} g_j \right\rfloor. \quad (3.3)$$

De igual manera que el caso infinito, hacemos *backtracking* en caso de encontrarnos con que $t_i \in \mathbb{Z}$ no puede satisfacer (3.2) si $i \in \{1, \dots, n-2\}$, o si $t_{n-2} \in \mathbb{Z}$ no puede satisfacer (3.3). En este caso, puede ser que en cualquier nivel t_i no se satisfaga la desigualdad y por lo tanto que necesitemos cambiar uno de t_1, \dots, t_{i-1} . Ciertamente, la elección más simple es realizar el cambio $t_{i-1} \leftarrow t_{i-1} \pm 1$ siempre y cuando continúe satisfaciendo sus cotas correspondientes.

El número de elecciones $t_1, \dots, t_{n-1} \in \mathbb{Z}$ es finito para la k -ésima capa entera. Decidimos, finalmente, descender a la $(k-1)$ -capa entera y repetir el proceso si en ninguna de esas elecciones se satisfacen ambas (3.2) y (3.3). Evidentemente, $\mathbf{0} \in \mathbb{Z}^n$ es factible y se encuentra en la 0-ésima capa, por lo que este proceso está asegurado en terminar si es que el problema es factible, lo cual supusimos desde un inicio.

Con respecto a la complejidad algorítmica de este procedimiento podemos decir lo siguiente. Supongamos que modificamos el algoritmo para que encuentre todas las soluciones. Definamos

$$P_k := H_{\mathbf{q}, k \|\mathbf{q}\|^{-2}} \cap \mathbb{Z}_{\geq \mathbf{0}}^n = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{q}^T \mathbf{x} = k, \mathbf{x} \geq \mathbf{0}\}, \quad (3.4)$$

y sea $T(n)$ el tiempo requerido para encontrar todos los puntos en P_k o determinar que este conjunto es vacío¹. Es razonable suponer que $T(n)$ es exponencial en n . En efecto, cada par (x_i, ω_{i+1}) genera un intervalo de factibilidad $[t_i^{\min}, t_i^{\max}]$. Este intervalo ciertamente depende de las elecciones previas de t_1, \dots, t_{i-1} . Para encontrar todos los puntos en P_k , el algoritmo recorre todas las posibilidades:

$$\prod_{i=1}^{\tau_1} \min_{t_1, \dots, t_{i-1}} \{t_i^{\max} - t_i^{\min}\} \leq T(n) \leq \prod_{i=1}^{\tau_2} \max_{t_1, \dots, t_{i-1}} \{t_i^{\max} - t_i^{\min}\}, \quad (3.5)$$

donde $1 \leq \tau_1 \leq n$ es el entero más grande que asegura que $\min_{t_1, \dots, t_{i-1}} \{t_i^{\max} - t_i^{\min}\}$ sea positivo para todo $i \in \{1, \dots, \tau_1\}$. Definimos τ_2 de manera análoga. Se cumple que $\tau_1 \leq \tau_2$.

¹Estamos suponiendo implícitamente que el tiempo no depende del lado derecho k , por lo que depende exclusivamente de la dimensión del politopo. Es la creencia del autor que en realidad el tiempo es linealmente decreciente en k puesto que la probabilidad de que haya puntos enteros en P_k es mayor a medida que k aumenta. Si bien los resultados numéricos apuntan a que esta hipótesis es cierta, el autor prefirió decir que el tiempo es constante a falta de un mejor argumento teórico.

Sean ℓ_{\min}, ℓ_{\max} las longitudes del intervalo de factibilidad más pequeño y del más grande en todos los niveles, respectivamente. Es decir, definimos

$$\ell_{\min} := \min_{1 \leq i \leq \tau_1} \left\{ \min_{t_1, \dots, t_{i-1}} \{t_i^{\max} - t_i^{\min}\} \right\}, \quad (3.6)$$

$$\ell_{\max} := \max_{1 \leq i \leq \tau_2} \left\{ \max_{t_1, \dots, t_{i-1}} \{t_i^{\max} - t_i^{\min}\} \right\}. \quad (3.7)$$

Si P_k es vacío, se sigue que no existe ningún intervalo factible en el nivel n , lo que implica que $\tau_2 < n$. En caso contrario, el algoritmo recorre hasta el último nivel, por lo que $\tau_1 = \tau_2 = n$. De (3.5), obtenemos

$$\ell_{\min}^n \leq T(n) \leq \ell_{\max}^n. \quad (3.8)$$

En el peor de los casos, nuestro algoritmo recorre todas las capas enteras. Se sigue que

$$\text{Tiempo de ejecución} = \mathcal{O} \left(\sum_{k=1}^{\eta} T(n) \right) = \mathcal{O}(\eta \cdot T(n)) = \mathcal{O}(\eta \cdot c^n), \quad (3.9)$$

para alguna $c > 1$.

Ahora bien, este razonamiento aplica a la modificación del algoritmo en donde decidimos buscar todas las soluciones posibles. En realidad solo nos interesa encontrar un punto óptimo, por lo que podemos concluir que una cota superior para la complejidad de nuestro algoritmo es (3.9). Concluimos esta sección diciendo haremos uso del mismo razonamiento para determinar la complejidad algorítmica de nuestro método en la segunda fase de su construcción. Finalmente, observemos también que, para problemas del tipo (1.1), la solución siempre se encuentra razonablemente cerca de la frontera presupuestaria $\mathbf{p}^T \mathbf{x} = u$, así que a excepción de casos degenerados, nunca recorre nuestro algoritmo todas las capas enteras.

Bibliografía

- [BH09] Robert F. Bodi and Katrin Herr. Symmetries in integer programs. *arXiv: Combinatorics*, 2009.
- [Lav14] Carmen Gómez Laveaga. *Álgebra Superior: Curso completo*. Programa Universitario del Libro de Texto. Facultad de Ciencias, Universidad Nacional Autónoma de México, Ciudad de México, México, primera edición edition, 2014. Primera reimpresión: julio de 2015.
- [MT90] Silvano Martello and Paolo Toth. *Knapsack problems: algorithms and computer implementations*. John Wiley & Sons, Inc., USA, 1990.
- [Sch98] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, Chichester, UK, 1998.