Ecuaciones lineales diofantinas aplicadas a programas lineales enteros

Iñaki Sebastián Liendo Infante

25 de junio de 2025

Índice general

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

$$\begin{aligned} \max_{\boldsymbol{x}\in\mathbb{Z}^n} \quad & \boldsymbol{p}^T\boldsymbol{x}, && \text{(1.1a)} \\ \text{s.a.} \quad & \boldsymbol{p}^T\boldsymbol{x} \leq u, && \text{(1.1b)} \\ & \boldsymbol{x} \geq \boldsymbol{0}. \end{aligned}$$

Por ello mismo, es razonable suponer que $\boldsymbol{p}_i \neq 0$ para cualquier $i \in \{1, \ldots, n\}$. 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 $i \in \{1, \ldots, n\}$; y el caso $\boldsymbol{p} \geq \boldsymbol{0}$. 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 $\boldsymbol{p}_i < 0$ 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

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

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 $a_1, \ldots, a_n$ 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 $d = \operatorname{mcd}\{a_1, \ldots, a_n\}$. Si $d = 1$, entonces decimos que $a_1, \ldots, a_n$ 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 coprima ($\operatorname{mcd}\{a_1, \ldots, a_n\} = 1$) se sigue que estos enteros sean coprimos a pares ($\operatorname{mcd}\{a_i, a_j\} = 1$ 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 $a_1, \ldots, a_n$ si existen enteros $x_1, \ldots, x_n$ tales que $c = a_1x_1 + \cdots + a_nx_n$.*

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 $a_1, \ldots, a_n$ una colección de enteros no todos iguales a cero. Entonces $d = \operatorname{mcd}\{a_1, \ldots, a_n\}$ si y solo si d es la mínima combinación lineal entera positiva de $a_1, \ldots, a_n$.*

Corolario 1.4. *Si $d = \operatorname{mcd}\{a_1, \ldots, a_n\}$, entonces $\operatorname{mcd}\left\{\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right\} = 1$.*

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

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

Si a es nulo, entonces $M(a) = \{0\}$. En caso contrario encontramos que $M(a)$ es un conjunto infinito. Ánalogamente a la Definición 1.1, definimos el mínimo común múltiplo m de una colección de enteros $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ como el elemento minimal de $\mathbb{N} \cap \bigcap_{i=1}^{n} M(a_i)$. Escribimos $m = \operatorname{mcm}\{a_1, \ldots, a_n\}$. 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 $a_1, \ldots, a_n$ enteros. Una ecuación lineal diofantina es una ecuación donde queremos encontrar enteros $x_1, \ldots, x_n$ que satisfagan

$$a_1 x_1 + \cdots + a_n x_n = c.$$

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* $\mathrm{mcd}\{a, b\} \mid c$.

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

Definición 1.6. *Sea $d \coloneqq \mathrm{mcd}\{a, b\}$ 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 $d \coloneqq \mathrm{mcd}\{a, b\}$ 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*

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

donde $d \coloneqq \mathrm{mcd}\{a, b\}$ 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 $\boldsymbol{p}_i < 0$ o $\boldsymbol{p} \geq \boldsymbol{0}$.

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

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

Ejemplo 1.9. *El vector $\left(-\sqrt{2}, 1/\sqrt{2}\right)^T = \sqrt{2}(-1, 1/2)^T$ 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 $\boldsymbol{v}$ cuyas entradas son racionales ($\boldsymbol{v} \in \mathbb{Q}^n$) es esencialmente entero. En efecto, $\boldsymbol{v}_i = \frac{p_i}{q_i}$ para algunos enteros p_i y q_i con q_i distinto de cero. Si definimos $q \coloneqq \text{mcm}\{q_1, \ldots, q_n\} \neq 0$ y $\boldsymbol{w} \coloneqq q\boldsymbol{v}$, se sigue que $\boldsymbol{v} = \frac{1}{q}\boldsymbol{w}$ y también $\boldsymbol{w} \in \mathbb{Z}^n$.

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

$$\pm \frac{1}{\text{mcd}\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}} \boldsymbol{w}$$

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

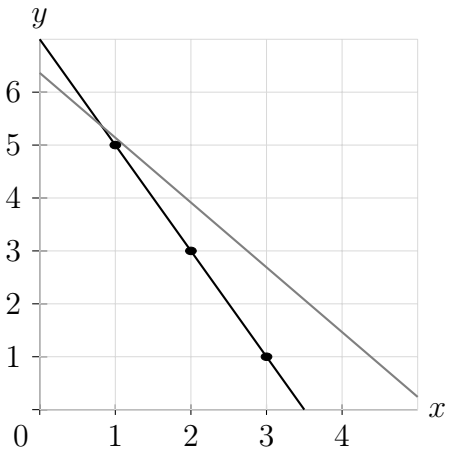

Figura 1.1: Representación de una capa entera (en negro) junto a un hiperplano afino que no es capa entera (en gris). La capa entera tiene como parámetros $\boldsymbol{v} = (2,1)^T$ y $t = 1{,}4$, mientras que los del hiperplano afino son $\boldsymbol{v} = (\sqrt{3}, \sqrt{2})^T$ y $t = 1{,}4$.

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

$$H_{\boldsymbol{v},t} \coloneqq \ker\{\boldsymbol{x} \mapsto \boldsymbol{v}^T\boldsymbol{x}\} + t\boldsymbol{v} = \{\boldsymbol{v}^\perp + t\boldsymbol{v} : \boldsymbol{v}^T\boldsymbol{v}^\perp = 0\} \tag{1.3}$$

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

Observemos que todo hiperplano afino $H_{\boldsymbol{v},t}$ es invariante ante reescalamientos en $\boldsymbol{v}$. Es decir, si $r \in \mathbb{R} \setminus \{0\}$ es un escalar, entonces $H_{\boldsymbol{v},t} = H_{r\boldsymbol{v},t/r}$. En particular, el conjunto de hiperplanos afinos asociados a un vector $\boldsymbol{v}$ esencialmente entero es igual al conjunto de hiperplanos afinos asociados a su múltiplo coprimo $\boldsymbol{w}$. 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 $\boldsymbol{v}, \boldsymbol{x} \in \mathbb{R}^n$ con $\boldsymbol{v}$ distinto de cero. Entonces $\boldsymbol{x} \in H_{\boldsymbol{v},t_{\boldsymbol{x}}}$, donde $t_{\boldsymbol{x}} \coloneqq \frac{\boldsymbol{v}^T\boldsymbol{x}}{\|\boldsymbol{v}\|^2}$.*

Teorema 1.12. *Sea $\boldsymbol{v} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{w}$ su múltiplo coprimo. Entonces la familia de capas enteras $\left\{H_{\boldsymbol{w},k\|\boldsymbol{w}\|^{-2}} : k \in \mathbb{Z}\right\}$ cubre a $\mathbb{Z}^n$.*

Pasemos a considerar el programa lineal (1.1) donde $\boldsymbol{p}$ es un vector esencialmente entero y $\boldsymbol{q}$ es su múltiplo coprimo. 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 $H_{\boldsymbol{p},t}$ donde se cumple que todo punto $\boldsymbol{x} \in H_{\boldsymbol{p},t}$ tiene un mismo nivel de utilidad. Como observamos previamente,

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

A causa del Teorema 1.12, somos capaces de caracterizar todos los puntos enteros a partir de $\boldsymbol{q}$. 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 $\boldsymbol{x} \in H_{\boldsymbol{q},k\|\boldsymbol{q}\|^{-2}}$, tenemos

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

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

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

Para respetar la restricción presupuestaria, podemos encontrar el entero η más grande que satisfaga $\boldsymbol{q}^T\boldsymbol{x} \leq u$ para todo $\boldsymbol{x} \in H_{\boldsymbol{q},\eta\|\boldsymbol{q}\|^{-2}}$. Diremos que η es el primer entero que satisface la restricción presupuestaria, o bien que $H_{\boldsymbol{q},\eta\|\boldsymbol{q}\|^{-2}}$ es la primera capa entera que satisface el presupuesto. De esta manera, encontramos que las capas enteras que satisfacen el presupuesto son parametrizadas por $k \in \{\eta, \eta-1, \ldots\}$. Debido a la observación anterior, se cumple inmediatamente que $\boldsymbol{q}^T\boldsymbol{x} = k$. 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 $\boldsymbol{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{q}$ su múltiplo coprimo, de manera que $\boldsymbol{p} = m\boldsymbol{q}$ para algún escalar $m \in \mathbb{R} \setminus \{0\}$. Entonces la primera capa entera $H_{\boldsymbol{q},\eta\|\boldsymbol{q}\|^{-2}}$ que satisface el presupuesto está parametrizada por $\eta \coloneqq \lfloor u/m \rfloor$.*

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

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

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

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

1. *El problema es infactible si y solo si $\boldsymbol{q} > \boldsymbol{0}$ y $u < 0$.*
2. *Si $\boldsymbol{q}_i < 0$ para algún $i \in \{2, \ldots, n\}$, entonces la η-ésima capa entera contiene un número infinito de puntos factibles.*
3. *Si el problema es factible y $\boldsymbol{q} > \boldsymbol{0}$, entonces la k-ésima capa entera contiene un número finito de puntos factibles, donde $k \in \{\eta, \eta-1, \ldots 0\}$.*

Demostración.

1. Supongamos que $\boldsymbol{q} \geq 0$ y $u < 0$. Si $\boldsymbol{x} \in \mathbb{Z}^n_{\geq \mathbf{0}}$ entonces $\boldsymbol{q}^T\boldsymbol{x} \geq 0 > u$ y por lo tanto $\boldsymbol{x}$ no es factible. Luego,
$$\mathbb{Z}^n_{\geq \mathbf{0}} \cap \{\boldsymbol{x} : \boldsymbol{q}^T\boldsymbol{x} \leq u\} = \emptyset,$$
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 $\boldsymbol{q}_i < 0$ para algún $i \in \{2, \ldots, n\}$, encontramos que $\lceil u/\boldsymbol{q}_i \rceil \boldsymbol{e}_i \in \mathbb{Z}^n$ es factible:
$$\boldsymbol{q}^T \left\lceil \frac{u}{\boldsymbol{q}_i} \right\rceil \boldsymbol{e}_i = \boldsymbol{q}_i \left\lceil \frac{u}{\boldsymbol{q}_i} \right\rceil \leq \boldsymbol{q}_i \frac{u}{\boldsymbol{q}_i} = u,$$
además, como $u < 0$, concluimos que $\lceil u/\boldsymbol{q}_i \rceil \boldsymbol{e}_i$ es no negativo.

2. Como $\boldsymbol{q}$ es un vector cuyas entradas son coprimas, sabemos de una generalización del Teorema 1.5 que existe $\boldsymbol{x} \in \mathbb{Z}^n$ tal que $\boldsymbol{q}^T\boldsymbol{x} = \eta$. Definamos los siguientes conjuntos de índices
$$I^+ \coloneqq \{i : q_i > 0\}, \quad I^\circ \coloneqq \{\ell : q_\ell = 0\}. \quad I^- \coloneqq \{j : q_j < 0\}.$$
Podemos suponer sin pérdida de generalidad que I° es vacío. En efecto, si $x_\ell < 0$ para algún $\ell \in I^\circ$, al redefinir $x_\ell \leftarrow 0$ se satisface $\boldsymbol{q}^T\boldsymbol{x} = \eta$.

   Entonces, ambos conjuntos I^+ e I^- forman una partición de $\{1, \ldots, n\}$. Podemos escoger escalares positivos $c_1, \ldots, c_n$ que satisfagan simultáneamente
$$x_j + \sum_{i \in I^+} \boldsymbol{q}_i c_i \geq 0, \quad \forall j \in I^-, \tag{1.4}$$
$$x_i - \sum_{j \in I^-} \boldsymbol{q}_j c_i \geq 0, \quad \forall i \in I^+. \tag{1.5}$$
   Definamos el vector $\boldsymbol{x}^+ \in \mathbb{Z}^n$ de manera que
$$\boldsymbol{x}^+_k \coloneqq \begin{cases} x_k + \sum_{i \in I^+} \boldsymbol{q}_i c_i, & k \in I^-, \\ x_k - \sum_{j \in I^-} \boldsymbol{q}_j c_k, & k \in I^+. \end{cases}$$
   Se verifica que $\boldsymbol{x}^+$ es no negativo y, además,
$$\begin{aligned} \boldsymbol{q}^T\boldsymbol{x}^+ &= \boldsymbol{q}^T\boldsymbol{x} + \sum_{k \in I^-} \sum_{i \in I^+} \boldsymbol{q}_k \boldsymbol{q}_i c_i - \sum_{k \in I^+} \sum_{j \in I^-} \boldsymbol{q}_k \boldsymbol{q}_j c_k \\ &= \eta + \sum_{j \in I^-} \sum_{i \in I^+} \boldsymbol{q}_j \boldsymbol{q}_i c_i - \sum_{i \in I^+} \sum_{j \in I^-} \boldsymbol{q}_i \boldsymbol{q}_j c_i \\ &= \eta. \end{aligned}$$
   Así pues, tenemos existencia. Para concluir que hay un número infinito de puntos, basta observar que si la elección de coeficientes $c_1, \ldots, c_n$ 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

$$P_k \coloneqq H_{\boldsymbol{q},k\|\boldsymbol{q}\|^{-2}} \cap \mathbb{Z}^n_{\geq \mathbf{0}} = \left\{ \boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{q}^T \boldsymbol{x} = k, \boldsymbol{x} \geq \mathbf{0} \right\}. \tag{1.6}$$

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

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

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

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.

□

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 $\boldsymbol{p}_i$ es negativo y por lo tanto hay una infinidad de soluciones en la η-ésima capa entera; y uno donde $\boldsymbol{p} > \mathbf{0}$, 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.

1.2.1. Una ecuación lineal diofantina

De acuerdo al Teorema 1.14, las soluciones del problema (1.1) se encuentran en una capa entera $H_{\boldsymbol{q},k\|\boldsymbol{q}\|^{-2}}$. Así, los puntos $\boldsymbol{x} \in \mathbb{Z}^n$ que se encuentran sobre esa capa satisfacen la ecuación lineal diofantina

$$\boldsymbol{q}^T \boldsymbol{x} = \boldsymbol{q}_1 \boldsymbol{x}_1 + \boldsymbol{q}_2 \boldsymbol{x}_2 + \cdots + \boldsymbol{q}_n \boldsymbol{x}_n = k. \tag{1.7}$$

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. Partimos de la observación que podemos resolver recursivamente esta ecuación. Definamos, por conveniencia, $g_1 \coloneqq \operatorname{mcd}\{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_n\}$ y también $\omega_1 \coloneqq k$. Como $\boldsymbol{q}$ es un vector coprimo, sabemos que $g_1 = 1$. Además, definamos

$$\omega_2 \coloneqq \frac{\boldsymbol{q}_2}{g_2 \cdot g_1} \boldsymbol{x}_1 + \cdots + \frac{\boldsymbol{q}_n}{g_2 \cdot g_1} \boldsymbol{x}_n,$$

donde $g_2 \coloneqq \operatorname{mcd}\{\boldsymbol{q}_2/g_1, \ldots, \boldsymbol{q}_n/g_1\}$. Así, la ecuación (1.7)es equivalente a

$$\frac{q_1}{g_1}\boldsymbol{x}_1 + g_2\omega_2 = \omega_1. \tag{1.8}$$

Observemos que

$$\operatorname{mcd}\left\{\frac{\boldsymbol{q}_1}{g_1}, g_2\right\} = \operatorname{mcd}\left\{\frac{\boldsymbol{q}_1}{g_1}, \operatorname{mcd}\left\{\frac{\boldsymbol{q}_2}{g_1}, \ldots, \frac{\boldsymbol{q}_n}{g_1}\right\}\right\} = \operatorname{mcd}\left\{\frac{\boldsymbol{q}_1}{g_1}, \frac{\boldsymbol{q}_2}{g_1}, \ldots, \frac{\boldsymbol{q}_n}{g_1}\right\} = 1.$$

Por lo tanto, existen soluciones enteras para todo $\omega_1 \in \mathbb{Z}$. Como $\boldsymbol{q}_1/g_1$ y g_2 son coprimos, encontramos que sus coeficientes de Bézout asociados (c.f. Definición 1.6) x_1', ω_2' son soluciones particulares de la ecuación

$$\frac{q_1}{g_1}\boldsymbol{x}_1 + g_2\omega_2 = 1.$$

Deducimos que las soluciones de la ecuación (1.8) están dadas por

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

donde $t_1 \in \mathbb{Z}$ es una variable libre.

Observación. Los coeficientes de Bézout x_1' y ω_2' dependen exclusivamente de $\boldsymbol{q}$ y no del punto $\boldsymbol{x}$. En efecto, x_1' está asociado a $\boldsymbol{q}_1/g_1$ y ω_2' está asociado a g_2. Pero ambos g_1 y g_2 son el máximo común divisor de $\boldsymbol{q}_1, \ldots \boldsymbol{q}_n$ y $\boldsymbol{q}_1/g_1, \ldots, \boldsymbol{q}_n/g_1$, respectivamente.

Para el siguiente paso de la recursión fijamos t_1 y resolvemos la ecuación

$$\frac{\boldsymbol{q}_2}{g_2 \cdot g_1}\boldsymbol{x}_2 + \frac{\boldsymbol{q}_3}{g_2 \cdot g_1}\boldsymbol{x}_3 + \cdots + \frac{\boldsymbol{q}_n}{g_2 \cdot g_1}\boldsymbol{x}_n = \omega_2. \tag{1.9}$$

Como $g_2 = \operatorname{mcd}\{\boldsymbol{q}_2/g_1, \ldots, \boldsymbol{q}_n/g_1\}$, sabemos del Corolario 1.4 que

$$\operatorname{mcd}\left\{\frac{\boldsymbol{q}_2}{g_2 \cdot g_1}, \ldots, \frac{\boldsymbol{q}_n}{g_2 \cdot g_1}\right\} = 1.$$

En el mismo espíritu que el primer paso de la recursión, definimos

$$\omega_3 \coloneqq \frac{\boldsymbol{q}_3}{g_3 \cdot g_2 \cdot g_1}\boldsymbol{x}_3 + \cdots + \frac{\boldsymbol{q}_n}{g_3 \cdot g_2 \cdot g_1}\boldsymbol{x}_n,$$

donde

$$g_3 \coloneqq \operatorname{mcd}\left\{\frac{\boldsymbol{q}_3}{g_2 \cdot g_1}, \ldots, \frac{\boldsymbol{q}_n}{g_2 \cdot g_1}\right\}.$$

Por lo que la ecuación (1.9) es equivalente a

$$\frac{\boldsymbol{q}_2}{g_2 \cdot g_1}\boldsymbol{x}_2 + g_3\omega_3 = \omega_2. \tag{1.10}$$

Nuevamente, tenemos

$$\operatorname{mcd}\left\{\frac{\boldsymbol{q}_2}{g_2 \cdot g_1}, g_3\right\} = 1,$$

y entonces (1.10) tiene una infinidad de soluciones para todo $\omega_2 \in \mathbb{Z}$, las cuales están dadas por

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

donde $t_2 \in \mathbb{Z}$ es una variable libre, y x_2', ω_3' son los coeficientes de Bézout asociados a $\frac{\boldsymbol{q}_2}{g_2 \cdot g_2}$ y g_3, respectivamente.

De manera general, para $i \in \{1, \ldots, n-2\}$, el i-ésimo paso de la recursión provee las soluciones

$$\begin{cases} \boldsymbol{x}_i = \omega_i x_i' + g_{i+1} t_i, \\ \omega_{i+1} = \omega_i \omega_{i+1}' - \frac{\boldsymbol{q}_i}{\prod_{j=1}^{i} g_j} t_i, \end{cases} \tag{1.11}$$

donde $t_i \in \mathbb{Z}$ es la i-ésima variable libre. Es valioso mencionar, otra vez, que los coeficientes de Bézout x_i', ω_{i+1}' dependen exclusivamente de $\boldsymbol{q}$ a través de sus entradas $\boldsymbol{q}_i$ y de los máximos común divisores entre ellas. Es decir, ni x_i' ni ω_{i+1}' dependen de la elección $\boldsymbol{x} \in \mathbb{Z}^n$.

En el último paso obtenemos la ecuación lineal diofantina

$$\frac{q_{n-1}}{\prod_{j=1}^{n-1} g_j} \boldsymbol{x}_{n-1} + \frac{q_n}{\prod_{j=1}^{n-1} g_j} \boldsymbol{x}_n = \omega_{n-1}. \tag{1.12}$$

Por construcción, los coeficientes de $\boldsymbol{x}_{n-1}$ y $\boldsymbol{x}_n$ son coprimos. Las soluciones están dadas por

$$\begin{cases} \boldsymbol{x}_{n-1} = \omega_{n-1} x_{n-1}' + \frac{\boldsymbol{q}_n}{\prod_{j=1}^{n-1} g_j} t_{n-1}, \\ \boldsymbol{x}_n = \omega_{n-1} x_n' - \frac{\boldsymbol{q}_{n-1}}{\prod_{j=1}^{n-1} g_j} t_{n-1}, \end{cases} \tag{1.13}$$

donde x_{n-1}', x_n' son los coeficientes de Bézout asociados a $\frac{\boldsymbol{q}_n}{\prod_{j=1}^{n-1} g_j}$ y $\frac{\boldsymbol{q}_{n-1}}{\prod_{j=1}^{n-1} g_j}$, respectivamente.

Finalmente, por la restricción de no negatividad $\boldsymbol{x} \geq 0$ en el problema (1.1), podemos acotar nuestra elección de variables libres $t_i \in \mathbb{Z}$ a partir de (1.11). De la primera igualdad encontramos que necesariamente se debe satisfacer

$$t_i \geq \left\lceil -\frac{\omega_i x_i'}{g_{i+1}} \right\rceil, \tag{1.14}$$

para $i \in \{1, \ldots, n-2\}$. Para determinar intervalos de no negatividad de x_{n-1} y x_n, observamos de (1.13) que dependemos de los signos de $\boldsymbol{q}_{n-1}$ y de $\boldsymbol{q}_n$. Mucho tendremos que decir en los siguientes dos capítulos sobre cómo acotar mejor $t_1, \ldots, t_{n-1}$ para asegurar la no negatividad de $\boldsymbol{x}$. Así pues, relegamos la discusión cuando analicemos separadamente el caso infinito y el caso finito.

Ahora bien, hemos encontrado una relación entre el vector de soluciones $\boldsymbol{x} \in \mathbb{Z}^n$ y el vector de variables libres $\boldsymbol{t} \in \mathbb{Z}^{n-1}$. Hemos manejado esta relación de manera recursiva a través de (1.11). Resultará conveniente encontrar una forma cerrada a la relación de recurrencia inducida. Para ello, recordemos que $\boldsymbol{x}$ se encuentra sobre la capa entera $H_{\boldsymbol{q}, k\|\boldsymbol{q}\|^{-2}}$ y por lo tanto satisface (1.7). Recordemos, también, que en el primer paso definimos $\omega_1 \coloneqq k$. Combinando estos dos últimos puntos, obtenemos

$$\begin{cases} \omega_1 & = k, \\ \omega_{i+1} & = \omega_i \cdot \omega_{i+1}' - \frac{\boldsymbol{q}_i}{\prod_{\ell=1}^{i} g_\ell} \cdot t_i. \end{cases} \tag{1.15}$$

Lema 1.15. *La forma cerrada de la relación de recurrencia (1.15) está dada por*

$$\omega_i = k \cdot \prod_{j=2}^{i} \omega'_j - \sum_{j=1}^{i-1} \frac{\boldsymbol{q}_j}{\prod_{\ell=1}^{j} g_\ell} \cdot \prod_{\ell=j+2}^{i} \omega'_\ell \cdot t_j. \tag{1.16}$$

Donde, por conveniencia, le asignamos el valor de 0 a la suma vacía y el valor de 1 al producto vacío.

Demostración. Lo demostramos inductivamente. Observemos que

$$\omega_1 = k \cdot \prod_{j=2}^{1} \omega'_j - \sum_{j=1}^{0} \frac{\boldsymbol{q}_j}{\prod_{\ell=1}^{j} g_\ell} \cdot \prod_{\ell=j+2}^{1} \omega'_\ell \cdot t_j = k,$$

debido a que definimos el producto vacío como 1 y la suma vacía como 0. Supongamos inductivamente que (1.16) se satisface para alguna $i \in \mathbb{N}$. Entonces, tenemos

$$\begin{aligned}
\omega_{i+1} &= k \cdot \prod_{j=2}^{i+1} \omega'_j - \sum_{j=1}^{i} \frac{\boldsymbol{q}_j}{\prod_{\ell=1}^{j} g_\ell} \cdot \prod_{\ell=j+2}^{i+1} \omega'_\ell \cdot t_j \\
&= k \cdot \prod_{j=2}^{i} \omega'_j \cdot \omega'_{i+1} - \sum_{j=1}^{i-1} \frac{\boldsymbol{q}_j}{\prod_{\ell=1}^{j} g_\ell} \cdot \prod_{\ell=j+2}^{i} \omega'_\ell \cdot t_j \cdot \omega'_{i+1} - \frac{\boldsymbol{q}_i}{\prod_{\ell=1}^{i} g_\ell} \cdot \prod_{\ell=i+2}^{i+1} \omega'_\ell \cdot t_i \\
&= \left(k \cdot \prod_{j=2}^{i} \omega'_j - \sum_{j=1}^{i-1} \frac{\boldsymbol{q}_j}{\prod_{\ell=1}^{j} g_\ell} \cdot \prod_{\ell=j+2}^{i} \omega'_\ell \cdot t_j \right) \omega'_{i+1} - \frac{\boldsymbol{q}_i}{\prod_{\ell=1}^{i} g_\ell} \cdot t_i \\
&= \omega_i \cdot \omega'_{i+1} - \frac{\boldsymbol{q}_i}{\prod_{\ell=1}^{i} g_\ell} \cdot t_i.
\end{aligned}$$

Por el principio de inducción se sigue que (1.16) satisface (1.15) para todo $i \in \mathbb{N}$. Así, esta fórmula es la forma cerrada de la relación de recurrencia propuesta. □

Por conveniencia, definimos los coeficientes $m_{ij} \in \mathbb{Z}$ con $i > j$ como

$$m_{ij} \coloneqq \frac{\boldsymbol{q}_j}{\prod_{\ell=1}^{j} g_\ell} \cdot \prod_{\ell=j+2}^{i} \omega'_\ell. \tag{1.17}$$

Así pues, juntando esto último con 1.11, obtenemos para $i \in \{1, \ldots, n-2\}$,

$$\begin{aligned}
\boldsymbol{x}_i &= \omega_i \cdot x'_i + g_{i+1} \boldsymbol{t}_i \\
&= k \cdot \prod_{j=2}^{i} \omega'_j \cdot x'_i - \sum_{j=1}^{i-1} m_{ij} x'_i \boldsymbol{t}_j + g_{i+1} \boldsymbol{t}_i.
\end{aligned} \tag{1.18}$$

Similarmente, sustituyendo en 1.13,

$$\boldsymbol{x}_{n-1} = k \cdot \prod_{j=2}^{n-1} \omega'_j \cdot x'_{n-1} - \sum_{j=1}^{n-2} m_{n-1,j} x'_{n-1} \boldsymbol{t}_j + \frac{\boldsymbol{q}_n}{\prod_{j=1}^{n-2} g_j} \boldsymbol{t}_{n-1}, \tag{1.19a}$$

$$\boldsymbol{x}_n = k \cdot \prod_{j=2}^{n-1} \omega'_j \cdot x'_n - \sum_{j=1}^{n-2} m_{n,j} x'_n \boldsymbol{t}_j - \frac{\boldsymbol{q}_{n-1}}{\prod_{j=1}^{n-2} g_j} \boldsymbol{t}_{n-1}. \tag{1.19b}$$

Con este trabajo anterior, ya podemos establecer una relación lineal entre $\boldsymbol{t} \in \mathbb{Z}^{n-1}$ y $\boldsymbol{x} \in \mathbb{Z}^n$. Definimos $\boldsymbol{\omega} \in \mathbb{Z}^n$ como

$$\boldsymbol{\omega}_i \coloneqq x'_i \cdot \prod_{j=2}^{\min\{i,n-1\}} \omega'_j. \tag{1.20}$$

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

$$M_{ij} \coloneqq \begin{cases} -m_{ij}x'_i, & j < i, \\ g_{i+1}, & i = j < n-1, \\ \frac{\boldsymbol{q}_n}{\prod_{k=1}^{n-1} g_k}, & i = j = n-1, \\ -\frac{\boldsymbol{q}_{n-1}}{\prod_{k=1}^{n-1} g_k}, & i = n, j = n-1, \\ 0, & \text{e.o.c.} \end{cases} \tag{1.21}$$

De (1.18) y (1.19) encontramos que

$$\boldsymbol{x} = k\boldsymbol{\omega} + M\boldsymbol{t}. \tag{1.22}$$

En una observación pasada mencionamos que los coeficientes de Bézout ω'_i, x'_i están asociados a términos exclusivamente dependientes de $\boldsymbol{q}$, por lo que no dependen de la elección $\boldsymbol{x} \in \mathbb{Z}$. De esta manera, $\boldsymbol{\omega}$ depende exclusivamente de $\boldsymbol{q}$. El mismo razonamiento aplica para la matriz M. Entonces, como $\boldsymbol{q}$ es fijo, se sigue que $\boldsymbol{\omega}$ y M lo son también.

Lema 1.16. *El vector $\boldsymbol{\omega} \in \mathbb{Z}^n$ satisface $\boldsymbol{q}^T\boldsymbol{\omega} = 1$.*

Demostración. Primero mostramos por inducción hacia atrás que se cumple

$$\sum_{j=i}^{n} \boldsymbol{q}_j\boldsymbol{\omega}_j = \prod_{j=2}^{i} \omega'_j \cdot \prod_{j=1}^{i} g_j, \tag{1.23}$$

para todo $i \in \{1, \ldots, n-1\}$. Empezamos con el caso base $i = n-1$:

$$\boldsymbol{q}_{n-1}\boldsymbol{\omega}_{n-1} + \boldsymbol{q}_n\boldsymbol{\omega}_n = \prod_{j=2}^{n-1} \omega'_j \cdot \left(\boldsymbol{q}_{n-1}x'_{n-1} + \boldsymbol{q}_n x'_n\right). \tag{1.24}$$

Recordemos que x'_{n-1} y x'_n son coeficientes de Bézout asociados a los coeficientes del lado izquierdo de (1.12), los cuales son coprimos. Entonces se cumple

$$\frac{\boldsymbol{q}_{n-1}}{\prod_{j=1}^{n-1} g_j}x'_{n-1} + \frac{\boldsymbol{q}_n}{\prod_{j=1}^{n-1} g_j}x'_n = 1,$$

lo cual implica

$$\boldsymbol{q}_{n-1}x'_{n-1} + \boldsymbol{q}_n x'_n = \prod_{j=1}^{n-1} g_j.$$

Sustituyendo en (1.24), obtenemos

$$\boldsymbol{q}_{n-1}\boldsymbol{\omega}_{n-1} + \boldsymbol{q}_n\boldsymbol{\omega}_n = \prod_{j=2}^{n-1}\omega'_j \cdot \prod_{j=1}^{n-1} g_j.$$

Supongamos inductivamente que (1.23) se satisface para alguna $2 \leq i \leq n-1$. Entonces tenemos

$$\begin{aligned}\sum_{j=i-1}^{n} \boldsymbol{q}_j\boldsymbol{\omega}_j &= \boldsymbol{q}_{i-1}\boldsymbol{\omega}_{i-1} + \sum_{j=i}^{n} \boldsymbol{q}_j\boldsymbol{\omega}_j \\ &= \prod_{j=2}^{i-1}\omega'_j \cdot \boldsymbol{q}_{i-1}x'_{i-1} + \prod_{j=2}^{i}\omega'_j \cdot \prod_{j=1}^{i} g_j \\ &= \prod_{j=2}^{i-1}\omega'_j \cdot \left(\boldsymbol{q}_{i-1}x'_{i-1} + \omega'_i \prod_{j=1}^{i} g_j\right).\end{aligned}$$

Nuevamente, x'_{i-1} y ω'_i son coeficientes de Bézout asociados, respectivamente, a $\frac{\boldsymbol{q}_{i-1}}{\prod_{j=1}^{i-1} g_j}$ y g_i, los cuales son coprimos. De esta manera satisfacen

$$\frac{\boldsymbol{q}_{i-1}}{\prod_{j=1}^{i-1} g_j}x'_{i-1} + g_i\omega'_i = 1,$$

por lo tanto,

$$\boldsymbol{q}_{i-1}x'_{i-1} + \omega'_i \prod_{j=1}^{i} g'_j = \prod_{j=1}^{i-1} g_j.$$

Sustituyendo, obtenemos el resultado (1.23) para $i-1$. Así, por inducción hacía atrás, (1.23) se cumple para todo $i \in \{1, \ldots, n-1\}$. Finalmente, para demostrar el Lema, observamos que

$$\boldsymbol{q}^T\boldsymbol{\omega} = \sum_{j=1}^{n} \boldsymbol{q}_j\boldsymbol{\omega}_j = \prod_{j=2}^{1}\omega'_j \cdot \prod_{j=1}^{1} g_j = g_1 = 1.$$

El primer producto es uno por ser el producto vacío. Recordemos también que g_1 es el máximo común divisor de $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_n$, los cuales son coprimos, y entonces $g_1 = 1$. □

Corolario 1.17. *El vector* $\boldsymbol{q}$ *genera* $\ker\{M^T\}$ *si* $\boldsymbol{q}_n \neq 0$.

Demostración. La matriz M es triangular inferior cuya diagonal principal es distinta de cero. En efecto, para todo $i \in \{1, \ldots, n-2\}$, tenemos

$$M_{ii} = g_{i+1} = \operatorname{mcd}\left\{\frac{\boldsymbol{q}_i}{\prod_{j=1}^{i} g_j}, \ldots, \frac{\boldsymbol{q}_n}{\prod_{j=1}^{i} g_j}\right\}.$$

Pero el máximo común divisor entre cualesquiera enteros siempre es positivo. También tenemos, $M_{n-1,n-1} = \boldsymbol{q}_n \neq 0$. Se sigue que las columnas de M son linealmente independientes,

y entonces su imagen tiene dimensión $n-1$. Por lo tanto, M^T tiene $n-1$ renglones linealmente independientes. Se sigue por el Teorema de la Dimensión que $\dim\ker\{M^T\} = 1$, así que basta mostrar que $\boldsymbol{q} \in \ker\{M^T\}$.

Sea $\boldsymbol{x} \in \mathbb{Z}^n$. Por el Teorema 1.12, existe una capa entera $H_{\boldsymbol{q},k\|\boldsymbol{q}\|^{-2}}$ que contiene a $\boldsymbol{x}$. Así, $\boldsymbol{x}$ satisface la ecuación lineal diofantina $\boldsymbol{q}^T\boldsymbol{x} = k$. Por construcción, existe $\boldsymbol{t} \in \mathbb{Z}^{n-1}$ tal que $\boldsymbol{x} = k\boldsymbol{\omega} + M\boldsymbol{t}$. Luego,

$$k = \boldsymbol{q}^T\boldsymbol{x} = k\boldsymbol{q}^T\boldsymbol{\omega} + \boldsymbol{q}^T M\boldsymbol{t} = k + (\boldsymbol{q}^T M)\boldsymbol{t}.$$

De donde obtenemos $(\boldsymbol{q}^T M)\boldsymbol{t} = 0$. Pero $\boldsymbol{x}$ fue arbitrario, así que también lo fue $\boldsymbol{t}$. Entonces se debe cumplir $\boldsymbol{q}^T M = 0$, lo que implica que $\boldsymbol{q} \in \ker\{M^T\}$. □

Corolario 1.18. *El vector $\boldsymbol{q}$ genera un espacio isomorfo a $\ker\{M^T\}$.*

Demostración. □

Hasta este punto, la gran mayoría de nuestra argumentación para demostrar los resultados ha sido fundamentada a través de las capas enteras $H_{\boldsymbol{q},k\|\boldsymbol{q}\|^{-2}}$, así como por el Teorema 1.12. Sin embargo, estas capas enteras contienen puntos que, en el contexto de programación lineal entera, no son de interés, a saber, contienen puntos no enteros. Nos gustaría concentrarnos exclusivamente en estos puntos enteros, al mismo tiempo que buscamos caracterizarlos por medio de $\boldsymbol{q}$. La siguiente Definición hará que logremos este primer objetivo de enfocarnos exclusivamente en los puntos enteros, mientras que el Teorema 1.21 permitirá que los caractericemos a partir de $\boldsymbol{q}$.

Definición 1.19 ([Sch98])**.** *Decimos que un subconjunto Λ de $\mathbb{R}^n$ es un grupo aditivo si*

1. $0 \in \Lambda$
2. *si $x, y \in \Lambda$, entonces $x + y \in \Lambda$ y $-x \in \Lambda$.*

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 1.20. *No es difícil ver que $\mathbb{Z}^n$ es un grupo aditivo. Si consideramos los vectores canónicos $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$, entonces encontramos que son linealmente independientes, pero también se cumple*

$$\mathbb{Z}^n = \{\lambda_1\boldsymbol{e}_1 + \cdots + \lambda_n\boldsymbol{e}_n : \lambda_i \in \mathbb{Z}\}.$$

De esta, manera $\mathbb{Z}^n$ es una red que tiene como base canónica a los vectores $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$.

Teorema 1.21. *Supongamos que $\boldsymbol{q}_n \neq 0$. Entonces $\boldsymbol{\omega}$ y las columnas de M forman una base de la red $\mathbb{Z}^n$.*

Demostración. En el Lema 1.17 mostramos que las columnas de M son linealmente independientes. Mostremos que $\boldsymbol{\omega}$ es linealmente independiente de las columnas de M. Supongamos que no lo es, por lo que existen escalares $\lambda_1, \ldots, \lambda_{n-1}$ tales que

$$\boldsymbol{\omega} = \lambda_1 \boldsymbol{m}_1 + \cdots + \lambda_{n-1} \boldsymbol{m}_{n-1},$$

donde $\boldsymbol{m}_1, \ldots, \boldsymbol{m}_{n-1}$ son las columnas de M. De los Lemas 1.16 y 1.17 obtenemos

$$1 = \boldsymbol{q}^T \boldsymbol{\omega} = \lambda_1 \boldsymbol{q}^T \boldsymbol{m}_1 + \cdots + \lambda_{n-1} \boldsymbol{q}^T \boldsymbol{m}_{n-1} = 0,$$

lo cual es una contradicción. Se sigue que $\{\boldsymbol{\omega}, \boldsymbol{m}_1, \ldots, \boldsymbol{m}_{n-1}\}$ es un conjunto de vectores linealmente independiente.

Ahora bien, sea $\boldsymbol{x} \in \mathbb{Z}^n$, por lo que se encuentra sobre una capa entera, y entonces satisface la ecuación lineal diofantina $\boldsymbol{q}^T \boldsymbol{x} = k$ para alguna $k \in \mathbb{Z}$. Por construcción, existe un vector $\boldsymbol{t} \in \mathbb{Z}^{n-1}$ tal que

$$\boldsymbol{x} = k\boldsymbol{\omega} + M\boldsymbol{t} = k\boldsymbol{\omega} + \boldsymbol{t}_1 \boldsymbol{m}_1 + \cdots + \boldsymbol{t}_{n-1} \boldsymbol{m}_{n-1}.$$

Como $\boldsymbol{x}$ fue arbitrario, se sigue que

$$\mathbb{Z}^n = \{k\boldsymbol{\omega} + \boldsymbol{t}_1 \boldsymbol{m}_1 + \cdots + \boldsymbol{t}_{n-1} \boldsymbol{m}_{n-1} : k, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_{n-1} \in \mathbb{Z}\}.$$

De esta manera, se cumple que $\{\boldsymbol{\omega}, \boldsymbol{m}_1, \ldots, \boldsymbol{m}_{n-1}\}$ es una base de $\mathbb{Z}^n$. □

Informalmente, a partir de $\boldsymbol{q}$ descomponemos la red $\mathbb{Z}^n$ como una suma de dos subredes isomorfas a $\mathbb{Z}$ y $\mathbb{Z}^{n-1}$, cuyas bases están dadas por $\boldsymbol{\omega}$ y las columnas de M, respectivamente. El vector $\boldsymbol{\omega}$ es una solución particular de la ecuación no homogénea $\boldsymbol{q}^T \boldsymbol{\omega} = 1$, mientras que las columnas de M forman una base del conjunto de soluciones de la ecuación homogénea $\boldsymbol{q}^T \boldsymbol{m} = 0$.

Luego, como $\boldsymbol{q}$ es un vector coprimo arbitrario, tenemos que cualquier vector coprimo y, por extensión cualquier vector esencialmente entero, admite una descomposición de $\mathbb{Z}^n$ en dos subredes. Ciertamente, esta idea de descomponer el espacio completo a partir de soluciones particulares y homogéneas no es novedosa.

1.2.2. Múltiples restricciones

En esta sección hacemos una discusión extensiva sobre la dificultad de agregar más restricciones al problema (1.1). Sea $\boldsymbol{p} \in \mathbb{R}^n$ esencialmente entero y consideremos su múltiplo coprimo $\boldsymbol{q} \in \mathbb{Z}^n$. Sea $A \in \mathbb{Q}^{m \times n}$ una matriz racional con renglones linealmente independientes y sea $\boldsymbol{b} \in \mathbb{Q}^m$ un vector. Consideremos el problema

$$\begin{aligned} \max_{\boldsymbol{x} \in \mathbb{Z}^n} \quad & \boldsymbol{q}^T \boldsymbol{x}, && \text{(1.25a)} \\ \text{s.a.} \quad & \boldsymbol{q}^T \boldsymbol{x} \leq u, && \text{(1.25b)} \\ & A\boldsymbol{q} = \boldsymbol{b}, && \text{(1.25c)} \\ & \boldsymbol{x} \geq \boldsymbol{0}. \end{aligned}$$

Ciertamente, la solución no se encuentra necesariamente en la η-ésima capa entera. Por ejemplo, si dejamos que $A \coloneqq \boldsymbol{q}^T$ y $b \coloneqq u - m$, la solución se encontrará en la ξ-ésima capa entera, donde

$$\xi \coloneqq \left\lfloor \frac{u}{m} - 1 \right\rfloor < \eta.$$

No obstante, si el problema (1.25) es factible, sabemos que la solución se encontrará en alguna capa entera con parámetro $k \in \{\eta, \eta - 1, \ldots\}$, pues todavía contamos con una restricción presupuestaria que se debe satisfacer.

Observación. Recordemos del Teorema 1.14 que, si tenemos solamente la restricción presupuestaria, entonces la utilidad máxima es η si $\boldsymbol{q}_i < 0$ para alguna $i \in \{2, \ldots, n-1\}$. Al igual que en el caso finito, ahora no somos capaces de saber inmediatamente en qué capa entera se encuentra nuestra solución.

Ahora bien, en el contexto del problema (1.25), el parámetro $k \in \mathbb{Z}$ se encarga de maximizar la utilidad (1.25a), así como de respetar el presupuesto (1.25b) a través de $k \leq \eta$. Similarmente, el vector $t \in \mathbb{Z}^{n-1}$ se encarga de respetar las otras restricciones (1.25c).

Teorema 1.22. *El problema (1.25) es equivalente al problema de maximización*

$$\max_{k \in \mathbb{Z}, \boldsymbol{t} \in \mathbb{Z}^{n-1}} k, \tag{1.26a}$$

$$\text{s.a.} \quad k \leq \eta, \tag{1.26b}$$

$$AM\boldsymbol{t} = kA\boldsymbol{\omega} - \boldsymbol{b}, \tag{1.26c}$$

$$M\boldsymbol{t} \geq -k\boldsymbol{\omega}. \tag{1.26d}$$

Demostración. Por el Teorema 1.21, sabemos que la transformación lineal

$$(k, \boldsymbol{t}) \mapsto \boldsymbol{x} \coloneqq k\boldsymbol{\omega} + M\boldsymbol{t}$$

es un isomorfismo entre las redes $\mathbb{Z} + \mathbb{Z}^{n-1}$ y $\mathbb{Z}^n$. Así, tenemos

$$\begin{aligned} A\boldsymbol{x} = \boldsymbol{b} &\iff AM\boldsymbol{t} = \boldsymbol{b} - kA\boldsymbol{\omega}, \\ \boldsymbol{x} \geq \boldsymbol{0} &\iff M\boldsymbol{t} \geq -k\boldsymbol{\omega}, \end{aligned}$$

y por lo tanto basta mostrar que si un vector es factible para un problema, entonces satisface la correspondiente restricción presupuestaria del otro problema. Para ello, es de utilidad recordar que η parametriza la primera capa entera que satisface el presupuesto.

Sea $\boldsymbol{x} \in \mathbb{Z}^n$ un vector factible de (1.25) Como $\boldsymbol{x}$ es entero, entonces se debe cumplir $\boldsymbol{q}^T\boldsymbol{x} \leq \eta$. Ahora bien, existe $(k, \boldsymbol{t}) \in \mathbb{Z}^n$ que satisface $\boldsymbol{x} = k\boldsymbol{\omega} + M\boldsymbol{t}$. Por el Lema 1.16 y el Corolario 1.17 encontramos que

$$k = \boldsymbol{q}^T\boldsymbol{x} \leq \eta,$$

y entonces $(k, \boldsymbol{t})$ es factible. Como $\boldsymbol{x}$ fue arbitrario, se sigue que la solución del problema (1.25) es una cota inferior del problema (1.26). La demostración de que la solución de (1.26) es una cota inferior de (1.25) es análoga.

Finalmente, supongamos que $(k, \boldsymbol{t}) \in \mathbb{Z}^n$ es solución de (1.26). Si existe $\hat{\boldsymbol{x}}$ factible para (1.25) con utilidad $\boldsymbol{q}^T\hat{\boldsymbol{x}} = \hat{k}$ estrictamente mayor, entonces consideramos $(\hat{k}, \hat{\boldsymbol{t}})$ tal que $\hat{\boldsymbol{x}} = \hat{k}\boldsymbol{\omega} + M\hat{\boldsymbol{t}}$. Este vector también es factible con utilidad $k < \hat{k} \leq \eta$, y entonces $(k, \boldsymbol{t})$ no era la solución de (1.26). Obtenemos una contradicción. □

Observación. El vector objetivo todavía es ortogonal a la restricción presupuestaria. No obstante, es más fácil de manejar en caso de usar cortes como en Ramificación y Acotamiento. Si k^* no es entero en la solución al problema relajado, la única manera de ramificar es con el nuevo corte $k \leq \lfloor k^* \rfloor$, pues el otro corte $k \geq \lceil k^* \rceil$ generará un subproblema infactible. Evidentemente, en la sección de análisis de resultados haremos comparaciones de tiempo en los tiempos de terminación entre esta formulación y la original.

La formulación del problema equivalente en el Teorema anterior resulta ser más interesante. Podemos desacoplar esta nueva formulación de manera que obtengamos un problema de maximización y otro de factibilidad. Supongamos, sin pérdida de generalidad, que las entradas de A y $\boldsymbol{b}$ son enteras. Como los renglones de A son linealmente independientes, de [Sch98] sabemos que tiene una única factorización de Hermite. Es decir, existe una matriz $U \in \mathbb{Z}^{n\times n}$ unimodular que satisface $AU = [H, \mathbf{0}]$, donde $H \in \mathbb{Z}^{m\times m}$ es triangular inferior y no singular.

Consideremos el subproblema de maximización

$$\max_{k\in\mathbb{Z}} k, \tag{1.27a}$$

$$\text{s.a.} \quad k \leq \eta, \tag{1.27b}$$

$$A\tilde{\boldsymbol{y}} = kA\boldsymbol{\omega} - \boldsymbol{b}, \tag{1.27c}$$

donde

$$\tilde{\boldsymbol{y}} \coloneqq U \begin{pmatrix} \tilde{\boldsymbol{y}}_m \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = U_m \tilde{\boldsymbol{y}}_m + U_{n-m} \tilde{\boldsymbol{y}}_{n-m} \in \mathbb{Z}^n,$$

con $\tilde{\boldsymbol{y}}_m \in \mathbb{Z}^m$ y $\tilde{\boldsymbol{y}}_{n-m} \in \mathbb{Z}^{n-m}$. Así también, U_m y U_{n-m} denotan las primeras m columnas y últimas $n-m$ columnas de U, respectivamente. Observemos que para toda $k \in \mathbb{Z}$ se cumple

$$AU \begin{pmatrix} H^{-1}\left(kA\boldsymbol{\omega} - \boldsymbol{b}\right) \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = [H, \mathbf{0}] \begin{pmatrix} H^{-1}\left(kA\boldsymbol{\omega} - \boldsymbol{b}\right) \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = kA\boldsymbol{\omega} - \boldsymbol{b}, \tag{1.28}$$

lo cual sugiere definir $\tilde{\boldsymbol{y}}_m \coloneqq H^{-1}(\boldsymbol{b} - kA\boldsymbol{w})$. No obstante, también debemos asegurarnos que este vector sea entero. Observemos que $\tilde{\boldsymbol{y}}_{n-m}$ queda libre, así que en realidad este subproblema tiene dimensión $m+1$. Definimos el conjunto de factibilidad

$$F \coloneqq \{k \in \mathbb{Z} : H^{-1}\left(kA\boldsymbol{\omega} - \boldsymbol{b}\right) \in \mathbb{Z}^m\} \cap \{k \in \mathbb{Z} : k \leq \eta\}. \tag{1.29}$$

Observación. Para que F sea no vacío, debe existir $k \in \mathbb{Z}$ tal que $\det(H) \mid (k\boldsymbol{a}_j^T\boldsymbol{\omega} - \boldsymbol{b}_j)$ para todo $j \in \{1, \ldots, m\}$, donde $\boldsymbol{a}_j$ denota el j-ésimo renglón de A. Es decir, una condición suficiente y necesaria para la no vacuidad de F es

$$\det(H) \mid \operatorname{mcd}\left\{k\boldsymbol{a}_1^T\boldsymbol{\omega} - b_1, \ldots, k\boldsymbol{a}_m^T\boldsymbol{\omega} - b_m\right\}.$$

Ahora bien, H es triangular inferior e invertible, por lo que $\det(H) \neq 0$ es el producto de los elementos $h_1, \ldots, h_m$ en su diagonal. Entonces $h_j \mid \det(H)$ para todo $j \in \{1, \ldots m\}$ y una condición necesaria para la no vacuidad de F es

$$\operatorname{mcm}\{h_1, \ldots, h_m\} \mid \operatorname{mcd}\left\{k\boldsymbol{a}_1^T\boldsymbol{\omega} - b_1, \ldots, k\boldsymbol{a}_m^T\boldsymbol{\omega} - b_m\right\}.$$

Si F es vacío, deducimos que este subproblema es infactible y por lo tanto (1.26) también lo es. Supongamos, pues, que $F \neq \emptyset$. No es difícil observar que F tiene un elemento maximal k^* y que este elemento es la solución al subproblema (1.27). Luego, dada esta solución $k^* \in \mathbb{Z}$, buscamos resolver el subproblema de factibilidad

$$M\boldsymbol{t} = \tilde{\boldsymbol{y}}, \tag{1.30a}$$
$$M\boldsymbol{t} \geq -k^*\boldsymbol{\omega}. \tag{1.30b}$$

Observemos que tenemos un sistema de n ecuaciones lineales con $2n-m-1$ incógnitas, por lo que tendremos que lidiar con $n-m-1$ parámetros libres:

$$M\boldsymbol{t} = \tilde{\boldsymbol{y}} = U_m\tilde{\boldsymbol{y}}_m + U_{n-m}\tilde{\boldsymbol{y}}_{n-m} \iff [M, -U_{n-m}]\begin{pmatrix}\boldsymbol{t}\\ \tilde{\boldsymbol{y}}_{n-m}\end{pmatrix} = U_m\tilde{\boldsymbol{y}}_m. \tag{1.31}$$

Si consideramos ahora la forma normal de Smith de esta matriz por bloques, obtenemos dos matrices unimodulares $S \in \mathbb{Z}^{n\times n}$ y $T \in \mathbb{Z}^{(2n-m-1)\times(2n-m-1)}$ que satisfacen

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

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 (1.31), tenemos

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

Si d_i no divide a $(SU_m\tilde{\boldsymbol{y}}_m)_i$ para alguna $i \in \{1,\dots,n\}$, encontramos que la primera ecuación del subproblema (1.30) no tiene solución en los enteros, lo que implica que la elección de k^* fue la incorrecta para asegurar soluciones enteras a este subproblema. De ser este el caso, redefinimos $F \leftarrow F\setminus\{k^*\}$. Si F ahora es vacío, entonces (1.26) es infactible, de caso contrario escogemos el nuevo elemento de maximal de F y repetimos el proceso.

Supongamos, pues que $d_i \mid (SU_m\tilde{\boldsymbol{y}}_m)_i$ para todo $i \in \{1,\dots,n\}$, por lo que 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 lineal de $\boldsymbol{s}$, es decir, $\boldsymbol{t} = \boldsymbol{t}(\boldsymbol{s})$. Hasta este punto el proceso no ha sido complicado, pues nos hemos encargado de resolver sistemas de ecuaciones lineales diofantinas. En términos del problema original (1.25), hemos encontrado los vectores $\boldsymbol{x}(\boldsymbol{s}) \coloneqq k^*\boldsymbol{\omega} + M\boldsymbol{t}(\boldsymbol{s})$ que maximizan la utilidad y que satisfacen todas las restricciones excepto, posiblemente, las de no negatividad.

La dificultad entra en juego cuando queremos determinar el vector de variables libres $\boldsymbol{s} \in \mathbb{Z}^{n-m-1}$ que hagan que $\boldsymbol{t}(\boldsymbol{s})$ satisfaga la desigualdad en el subproblema (1.30). Debilitando más esta condición, nos gustaría determinar si el conjunto

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

es vacío o no. En esta versión debilitada no nos interesa saber qué elementos contiene o tan siquiera cuántos elementos contiene. Es sabido que los programas enteros tales como

(1.25) o (1.26) son problemas difíciles de resolver, en el sentido de que no es conocido si se pueden resolver en tiempo polinomial. A lo largo de este capítulo, no obstante, hemos resuelto todos los problemas en tiempo polinomial[1]. La única deducción posible, entonces, es que el problema de determinar las variables $\boldsymbol{s}$, o bien de determinar cuántas hay, o bien de determinar su existencia, son todos problemas difíciles de resolver.

A pesar de lo anterior, hay dos casos donde la dificultad se reduce drásticamente. El caso menos interesante es cuando $m = n - 1$, de manera que no hay parámetros libres. Esto se debe a que el politopo factible resultante es un semirrayo o un segmento de línea. Al momento de escoger la k^*-ésima capa entera, estamos agregando la ecuación $k^* = k$, con lo que obtenemos un sistema lineal entero de n ecuaciones con n incógnitas, y entonces la solución es única. Basta entonces verificar que este único vector $\boldsymbol{t}$ satisface la desigualdad en el subproblema (1.30). El caso un poco más interesante se obtiene cuando $m = n - 2$. De esta manera obtenemos un solo parámetro, con lo que podemos determinar rápidamente la existencia o inexistencia de un intervalo de factibilidad.

Ejemplo 1.23. *Consideremos el problema con $n = 2$ variables y $m = 1$ restricciones*

$$\begin{aligned} \text{máx } & x - y, \\ \textit{s.a.} \quad & x - y \leq 12, \\ & 3x + 5y = 25, \\ & x, y \geq 0. \end{aligned}$$

En este caso tenemos $A = (3, 5), \boldsymbol{b} = 25$, y también $\boldsymbol{q} = (1, -1)^T$, al igual que $\eta = 12$. De (1.20) y (1.21) obtenemos

$$\boldsymbol{\omega} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, M = \begin{pmatrix} -1 \\ -1 \end{pmatrix}.$$

De la forma normal de Hermite de A tenemos

$$H = 1, U = \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix},$$

y de la forma normal de Smith de $[M, -U_m]$,

$$S = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, D = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}, T = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}.$$

Como $H = 1$, se sigue que $H^{-1}(\boldsymbol{b} - kA\boldsymbol{\omega}) = 25 - 3k$ es entero para todo $k \in \mathbb{Z}$. Así, el conjunto factible F (c.f. 1.29) está dado por

$$F = \mathbb{Z} \cap \{k \in \mathbb{Z} : k \leq 12\} = \{k \in \mathbb{Z} : k \leq \eta = 12\}.$$

Entonces escogemos $k^* = 12$ por ser el elemento maximal de F. Así, encontramos

$$SU_m \tilde{\boldsymbol{y}}_m = SU_m \left(H^{-1}(\boldsymbol{b} - k^* A\boldsymbol{\omega}) \right) = \begin{pmatrix} 22 \\ 33 \end{pmatrix}$$

[1] En [Sch98] se muestra que calcular el máximo común divisor, resolver ecuaciones lineales diofantinas, y calcular las factorizaciones tanto de Hermite como de Smith son operaciones acotadas por tiempo polinomial.

Observemos que la segunda entrada de $SU_m\tilde{\boldsymbol{y}}_m$ *no es divisible por* $D_{22} = 8$*. Así, el subproblema (1.30) no es factible para la elección de* k^* *previa. Escogemos el segundo elemento de* F *más grande, con lo que tenemos* $k^* \leftarrow 11$*. En este caso obtenemos* $SU_m\tilde{\boldsymbol{y}}_m = (-16, -24)^T$*, por lo que sí hay soluciones enteras. Luego, se debe satisfacer,*

$$T^{-1}\begin{pmatrix} \boldsymbol{t} \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = \begin{pmatrix} 16 \\ 24 \end{pmatrix},$$

de donde se sigue que $(\boldsymbol{t}, \tilde{\boldsymbol{y}}_{n-m}) = (1, 3)$*. Verificamos factibilidad:*

$$M\boldsymbol{t} + k^*\boldsymbol{\omega} = 1\begin{pmatrix} -1 \\ -1 \end{pmatrix} + 11\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 10 \\ -1 \end{pmatrix} \ngeq \mathbf{0}.$$

Ahora la elección de k^* *dio un punto entero pero con una entrada negativa. Seguimos este procedimiento hasta llegar a* $k^* \leftarrow 3$*. En este caso obtenemos* $(\boldsymbol{t}, \tilde{\boldsymbol{y}}_{n-m}) = (-2, -6)^T$*, de donde*

$$M\boldsymbol{t} + k^*\boldsymbol{\omega} = -2\begin{pmatrix} -1 \\ -1 \end{pmatrix} + 3\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \end{pmatrix} \geq \mathbf{0}.$$

Concluimos diciendo que $(k^*, \boldsymbol{t}) \coloneqq (3, -2)$ *es el óptimo del programa (1.26) y entonces* $(x, y) = (5, 2)$ *es el óptimo de (1.25).*

Ejemplo 1.24. *Ahora consideremos el problema con* $n = 3$ *variables y* $m = 1$ *restricciones*

$$\begin{aligned} \text{máx } & x - y + 2z, \\ \textit{s.a.} \quad & x - y + 2z \leq 10 \\ & 3x + 4y - z = 15 \\ & x, y, z \geq 0. \end{aligned}$$

En este caso tenemos $A = (3, 4, -1), \boldsymbol{b} = 15$*, y también* $\boldsymbol{q} = (1, -1, 2)^T$*, al igual que* $\eta = 10$*. De (1.20) y (1.21) obtenemos*

$$\boldsymbol{\omega} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, M = \begin{pmatrix} 1 & 0 \\ -1 & 2 \\ -1 & 1 \end{pmatrix}.$$

De la forma normal de Hermite de A *tenemos*

$$H = 1, U = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 4 & 3 \end{pmatrix},$$

y de la forma normal de Smith de $[M, -U_m]$*,*

$$S = \begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ 3 & 4 & -1 \end{pmatrix}, D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 7 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Nuevamente, observemos que $H = 1$ y por lo tanto $F = \{k \in \mathbb{Z} : k \leq 10\}$. Seguimos exactamente el mismo procedimiento que en el Ejemplo 1.23 hasta llegar a $k^* \leftarrow 5$. Encontramos que se satisface

$$T^{-1}\begin{pmatrix} \boldsymbol{t} \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ s \end{pmatrix} \implies \begin{pmatrix} \boldsymbol{t} \\ \tilde{\boldsymbol{y}}_{n-m} \end{pmatrix} = s\begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix},$$

donde $s \in \mathbb{Z}$ es la única variable libre. En este caso podemos determinar rápidamente un intervalo de existencia: tenemos $M\boldsymbol{t} \geq -k^*\boldsymbol{\omega}$ si y solo si

$$s\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \geq \begin{pmatrix} -5 \\ 0 \\ 0 \end{pmatrix},$$

de donde se sigue inmediatamente que $s \in \{-5, -4, \ldots, 0\}$. Sustituyendo en $\boldsymbol{t}$ y transformando a $\boldsymbol{x}$, encontramos que

$$\left\{ \begin{pmatrix} 0 \\ 5 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \\ 0 \end{pmatrix} \right\}$$

son las seis soluciones del problema. Todas alcanzan un nivel de utilidad $k^* = 5$.

Si el programa (1.25) es factible, entonces el programa (1.26) también lo es. A partir de nuestro procedimiento, eventualmente encontraremos un par $(k^*, \boldsymbol{t}^*)$ que resuelva tanto el subproblema de maximización (1.27) como el de factibilidad (1.30).

Ahora bien, son dos las maneras en las que nuestro problema sea infactible. En primer lugar, puede que nuestro conjunto de factibilidad F sea vacío y por lo tanto el sistema de ecuaciones lineales (1.25c) es inconsistente. O bien, puede ser que F sea no vacío y, a causa del Corolario (1.25) tiene un número infinito de elementos, pero que la desigualdad en el subproblema de factibilidad nunca se satisfaga. La primera situación no supone ningún problema, pero la segunda hará que cualquier algoritmo basado en este modo de proceder nunca termine.

Corolario 1.25. *Si el conjunto de factibilidad F no es vacío, entonces tiene cardinalidad infinita.*

Demostración. Escojamos $k \in F$, entonces

$$\det(H) \mid \operatorname{mcd}\{k\boldsymbol{a}_1^T\boldsymbol{\omega} - b_1, \ldots, k\boldsymbol{a}_m^T\boldsymbol{\omega} - b_m\},$$

de donde se verifica que

$$\det(H) \mid \left(\operatorname{mcd}\{k\boldsymbol{a}_1^T\boldsymbol{\omega} - b_1, \ldots, k\boldsymbol{a}_m^T\boldsymbol{\omega} - b_m\} - n \cdot \det(H)\right)$$

para todo $n \in \mathbb{Z}$. Pero esto implica que

$$\{k - n \cdot \det(H) : n \in \mathbb{Z}\} \cap \{k \in \mathbb{Z} : k \leq \eta\} \subseteq F.$$

El conjunto del lado izquierdo tiene un número infinito de elementos, y entonces F también. □

Capítulo 2

El caso infinito

Corolario 2.1. *Si $\boldsymbol{q}_i < 0$ para algún $i \in \{2, \ldots, n\}$, entonces el valor óptimo del problema (1.1) es $m\eta$. Además, η es el múltiplo de m más grande (en valor absoluto) que satisface $m\eta \leq u$.*

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

Ahora bien, recordemos que $\eta = \lfloor u/m \rfloor$ por el Lema 1.13. Supongamos que $\xi \in \mathbb{Z}$ satisface $m\xi \leq u$ y también $\lfloor u/m \rfloor < \xi$. Si $m > 0$ encontramos que

$$m \left\lfloor \frac{u}{m} \right\rfloor < m\xi \leq u \implies \left\lfloor \frac{u}{m} \right\rfloor < \xi \leq \frac{u}{m},$$

pero esto contradice las propiedades de la función piso. Ahora bien, si $m < 0$, entonces

$$\xi \geq \frac{u}{m} \geq \left\lfloor \frac{u}{m} \right\rfloor \implies m\xi \leq u \leq m \left\lfloor \frac{u}{m} \right\rfloor \leq u,$$

lo que implica que ξ no es el múltiplo más grande de m que satisface $m\xi \leq u$. Independientemente obtenemos una contradicción, por lo que debe ser el caso que, en efecto, η es el múltiplo más grande de m que satisface $m\eta \leq u$. □

Para que ahora se satisfagan las condiciones de no negatividad de $\boldsymbol{x}_{n-1}$ y de $\boldsymbol{x}_n$, encontramos que la variable libre $t_{n-1} \in \mathbb{Z}$ debe cumplir ciertas desigualdades según los signos de $\boldsymbol{q}_{n-1}$ y de $\boldsymbol{q}_n$. Definamos, por conveniencia,

$$b_1 \coloneqq -\frac{\omega_{n-1}x'_{n-1}}{\boldsymbol{q}_n} \cdot \prod_{j=1}^{n-1} g_j, \quad b_2 \coloneqq \frac{\omega_{n-1}x'_n}{\boldsymbol{q}_{n-1}} \cdot \prod_{j=1}^{n-1} g_j. \tag{2.1}$$

Entonces se verifica que

$$t_{n-1} \in \begin{cases} \left[\lceil b_1 \rceil, \lfloor b_2 \rfloor\right] & \text{si } 0 < \boldsymbol{q}_{n-1}, \boldsymbol{q}_n, \\ \left[\lceil b_2 \rceil, \lfloor b_1 \rfloor\right] & \text{si } \boldsymbol{q}_{n-1}, \boldsymbol{q}_n < 0, \\ \left[\lceil \text{máx}\{b_1, b_2\} \rceil, \infty\right) & \text{si } \boldsymbol{q}_{n-1} < 0 < \boldsymbol{q}_n, \\ \left(-\infty, \lfloor \text{mín}\{b_1, b_2\} \rfloor\right] & \text{si } \boldsymbol{q}_n < 0 < \boldsymbol{q}_{n-1}. \end{cases} \tag{2.2}$$

Lema 2.2. *Existe un vector $\boldsymbol{t} \in \mathbb{Z}^{n-1}$ que satisface ambos (1.14) y (2.2).*

Demostración. Tenemos cuatro casos, pero observemos que los dos en donde $\boldsymbol{q}_{n-1}$ y $\boldsymbol{q}_n$ tienen signo distinto no son difíciles: si $\boldsymbol{q}_{n-1} < 0 < \boldsymbol{q}_n$, entonces el vector $\boldsymbol{t} \in \mathbb{Z}^{n-1}$ dado por

$$\boldsymbol{t}_i := \begin{cases} \left\lceil -\frac{\omega_i x_i'}{g_{i+1}} \right\rceil, & i < n-1, \\ \lceil \text{máx}\{b_1, b_2\} \rceil, & i = n-1, \end{cases}$$

satisface ambos (1.14) y (2.2). El caso $\boldsymbol{q}_n < 0 < \boldsymbol{q}_{n-1}$ es completamente similar.

Ahora bien, supongamos que $0 < \boldsymbol{q}_{n-1}, \boldsymbol{q}_n$. Podemos suponer sin pérdida de generalidad que $\boldsymbol{q}_{n-2} < 0$. En efecto, como $\boldsymbol{q}_i < 0$ para alguna $i \in \{2, \ldots, n\}$, somos capaces permutar las entradas i y $n-2$ de $\boldsymbol{q}$ en el problema (1.1). Observemos que

$$\begin{aligned} b_2 - 1 \leq \lfloor b_2 \rfloor \leq b_2, \\ b_1 \leq \lceil b_1 \rceil \leq b_1 + 1. \end{aligned}$$

De donde obtenemos

$$b_2 - b_1 - 2 \leq \lfloor b_2 \rfloor - \lceil b_1 \rceil \leq b_2 - b_1.$$

Así pues, para que el intervalo $[\lceil b_1 \rceil, \lfloor b_2 \rfloor]$ esté bien definido, es suficiente con mostrar que existe un escalar ω_{n-1} que satisfaga $b_2 - b_1 \geq 2$. Tenemos

$$b_2 - b_1 = \omega_{n-1} \prod_{j=1}^{n-1} g_j \cdot \left(\frac{x_{n-1}'}{\boldsymbol{q}_n} + \frac{x_n'}{\boldsymbol{q}_{n-1}} \right) \tag{2.3}$$

Como x_{n-1}' y x_n' son coeficientes de Bézout asociados a los dos coeficientes en (1.12) que son coprimos, se cumple

$$\frac{\boldsymbol{q}_{n-1}}{\prod_{j=1}^{n-1} g_j} x_{n-1}' + \frac{\boldsymbol{q}_n}{\prod_{j=1}^{n-1} g_j} x_n' = 1,$$

lo que implica que

$$\frac{x_{n-1}'}{\boldsymbol{q}_n} + \frac{x_n'}{\boldsymbol{q}_{n-1}} = \frac{\prod_{j=1}^{n-1} g_j}{\boldsymbol{q}_{n-1}\boldsymbol{q}_n}.$$

Sustituyendo en (2.3),

$$b_2 - b_1 = \omega_{n-1} \cdot \frac{\prod_{j=1}^{n-1} g_j^2}{\boldsymbol{q}_{n-1}\boldsymbol{q}_n} \geq 2 \iff \omega_{n-1} \geq 2\frac{\boldsymbol{q}_{n-1}\boldsymbol{q}_n}{\prod_{j=1}^{n-1} g_j^2}. \tag{2.4}$$

De (1.11) sabemos que

$$\omega_{n-1} = \omega_{n-2}\omega_{n-1}' - \frac{\boldsymbol{q}_{n-2}}{\prod_{j=1}^{n-2} g_j} t_{n-2}.$$

Sustituyendo en (2.4), usando el hecho de que $\boldsymbol{q}_{n-2} < 0$ y despejando t_{n-2}, encontramos que $\lceil b_2 \rceil - \lfloor b_1 \rfloor \geq 0$ si

$$t_{n-2} \geq \frac{\omega_{n-2}\omega_{n-1}'}{\boldsymbol{q}_{n-2}} \prod_{j=1}^{n-2} g_j - 2\frac{\boldsymbol{q}_{n-1}\boldsymbol{q}_n}{\boldsymbol{q}_{n-2} g_{n-1}^2} \prod_{j=1}^{n-2} g_j^{-1}$$

Llamemos c al lado derecho de esta desigualdad. Así pues, definimos el vector $\boldsymbol{t} \in \mathbb{Z}^{n-1}$ de manera que

$$\boldsymbol{t}_i \coloneqq \begin{cases} \left\lceil -\frac{\omega_i x_i'}{\boldsymbol{q}_i} \right\rceil, & i < n-2, \\ \left\lceil \max\left\{ -\frac{\omega_i x_i'}{\boldsymbol{q}_i}, c \right\} \right\rceil, & i = n-2, \\ \lceil b_1 \rceil, & i = n-1. \end{cases}$$

Se verifica que $\boldsymbol{t}$ satisface ambos (1.14) y (2.2). Finalmente, el caso $\boldsymbol{q}_{n-1}, \boldsymbol{q}_n < 0$ es completamente similar. □

En síntesis, por el Teorema (1.14) sabemos que la solución se encuentra en la η-ésima capa entera. Por lo tanto, debemos encontrar una solución no negativa a la ecuación lineal diofantina (1.7). Por el Lema 2.2 sabemos que existe un vector $\boldsymbol{t} \in \mathbb{Z}^{n-1}$ que satisface ambos (1.14) y (2.2). Si definimos $\boldsymbol{x}$ como lo indican (1.11) y (1.13) usando $\boldsymbol{t}$, entonces $\boldsymbol{x}$ es una solución entera no negativa. Observemos que podemos construir los vectores $\boldsymbol{t}$ y $\boldsymbol{x}$ simúltaneamente. De esta manera, obtenemos el siguiente Teorema.

Teorema 2.3. *El problema (1.1) se puede resolver a través de encontrar la solución de una ecuación lineal diofantina en n incógnitas.*

2.1. Análisis de resultados

Una consecuencia del Teorema 2.3 es que la complejidad algoritmítica del problema (1.1) es lineal en la dimensión n siempre y cuando $\boldsymbol{q}_i < 0$ para alguna $i \in \{2, \ldots, n\}$. En esta sección describimos un algoritmo cuyo tiempo de terminación es $\mathcal{O}(n)$. A través de los resultados obtenidos previamente, somos capaces de mostrar que nuestro algoritmo es correcto. Finalmente, implementamos nuestro algoritmo en el lenguaje de programación Python y comparamos sus tiempos de terminación con los de la implementación de Ramificación y Acotamiento en la librería PuLP.

Capítulo 3

El caso finito

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

$$\begin{aligned} \max_{\boldsymbol{x}\in\mathbb{Z}^n} \quad & \boldsymbol{u}^T\boldsymbol{x}, && \text{(3.1a)} \\ \text{s.a.} \quad & \boldsymbol{w}^T\boldsymbol{x} \leq c, && \text{(3.1b)} \\ & \boldsymbol{x} \geq \boldsymbol{0}, && \text{(3.1c)} \end{aligned}$$

donde los vectores positivos $\boldsymbol{u}, \boldsymbol{w} \in \mathbb{Z}^n$ son conocidos como vector de útiles y vector de pesos, respectivamente. Puesto que no acotamos $\boldsymbol{x}$, el problema recibe el nombre de Problema de la Mochila no Acotado. Pero también como $\boldsymbol{u} = \boldsymbol{w}$, 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 $k \in \{\eta, \eta-1, \ldots, 0\}$ y terminamos una vez que encontremos un punto no negativo.

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

$$\boldsymbol{q}^T\boldsymbol{x} = q_1x_1 + q_2x_2 + \cdots + q_nx_n = k.$$

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 $\omega_1 \coloneqq k$ 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 (1.11),

$$\left\lceil -\frac{\omega_i x_i'}{g_{i+1}} \right\rceil \leq t_i \leq \left\lfloor \frac{\omega_i \omega_{i+1}'}{q_i} \prod_{j=1}^{i} g_j \right\rfloor. \tag{3.2}$$

para todo $i \in \{1, \ldots, n-2\}$. Después, como $0 < q_{n-1}, q_n$, se sigue de (1.13),

$$\left\lceil -\frac{\omega_{n-1} x_{n-1}'}{q_n} \cdot \prod_{j=1}^{n-2} g_j \right\rceil \leq t_{n-1} \leq \left\lfloor \frac{\omega_{n-1} x_n'}{q_{n-1}} \cdot \prod_{j=1}^{n-2} g_j \right\rfloor. \tag{3.3}$$

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 $i \in \{1, \ldots, n-2\}$, 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 $t_1, \ldots, t_{i-1}$. 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 $t_1, \ldots, t_{n-1} \in \mathbb{Z}$ 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

$$P_k \coloneqq H_{\boldsymbol{q}, k\|\boldsymbol{q}\|^{-2}} \cap \mathbb{Z}^n_{\geq \mathbf{0}} = \{\boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{q}^T \boldsymbol{x} = k, \boldsymbol{x} \geq \mathbf{0}\}, \tag{3.4}$$

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

$$\prod_{i=1}^{\tau_1} \min_{t_1, \ldots, t_{i-1}} \{t_i^{\text{máx}} - t_i^{\text{mín}}\} \leq T(n) \leq \prod_{i=1}^{\tau_2} \max_{t_1, \ldots, t_{i-1}} \{t_i^{\text{máx}} - t_i^{\text{mín}}\}, \tag{3.5}$$

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

[1] Estamos 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 $\ell_{\text{mín}}, \ell_{\text{máx}}$ las longitudes del intervalo de factibilidad más pequeño y del más grande en todos los niveles, respectivamente. Es decir, definimos

$$\ell_{\text{mín}} \coloneqq \min_{1\leq i\leq \tau_1}\left\{\min_{t_1,\ldots,t_{i-1}}\{t_i^{\text{máx}} - t_i^{\text{mín}}\}\right\}, \tag{3.6}$$

$$\ell_{\text{máx}} \coloneqq \max_{1\leq i\leq \tau_2}\left\{\max_{t_1,\ldots,t_{i-1}}\{t_i^{\text{máx}} - t_i^{\text{máx}}\}\right\}. \tag{3.7}$$

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

$$\ell^n_{\text{mín}} \leq T(n) \leq \ell^n_{\text{máx}}. \tag{3.8}$$

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

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

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 $\boldsymbol{p}^T\boldsymbol{x} = u$, 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.