Ecuaciones lineales diofantinas aplicadas a programas lineales enteros

Iñaki Sebastián Liendo Infante

11 de junio de 2025

Índice general

Capítulo 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 las siguientes secciones. En particular, va se destaca la importancia de las ecuaciones lineales diofantinas para la construcción de nuestro algoritmo. En este capítulo consideramos pertinente no incluir demostraciones, pues los enunciados son mostrados en cualquier clase de álgebra superior o de programación lineal, por ejemplo. La referencia principal para la sección de teoría de números es [Lav14]. Finalmente, a lo largo de este capítulo tanto como de esta tesis excluimos al cero del conjunto de los números naturales.

1.1. Teoría de Números

1.1.1. 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 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 $\operatorname{mcd}\{a_1, \ldots, a_n\} = 1$, 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 $1, 3, 3$ son coprimos pero evidentemente $3, 3$ 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 $d = \text{mcd}\{a_1, \ldots, a_n\}$ si y solo si d es la mínima combinación lineal entera positiva de $a_1, \ldots, a_n$.*

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

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, entoncees $M(a) = \{0\}$. En caso contrario encontramos que $M(a)$ es un conjunto infinito. Ánalogamente a la Definición 1.1, definimos al 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 $m = \text{mcm}\{a_1, \ldots, a_n\}$. 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 no es vacía.

1.1.2. 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

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

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. Los siguientes resultados 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 $d \coloneqq \text{mcd}\{a, b\}$ 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 $d \coloneqq \text{mcd}\{a, b\}$ 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. Entonces

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

por lo que $c' \cdot x', c' \cdot y'$ es una ecuación particular a 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*

$$\begin{cases} x = x_0 + \frac{b}{d}t, \\ y = y_0 - \frac{a}{d}t, \end{cases} \tag{1.1}$$

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

1.2. Programación lineal

Capítulo 2

El algoritmo

En este capítulo desarrollamos el algoritmo para resolver prácticamente cualquier tipo de problemas de programación lineal entera; se divide en tres subsecciones que construyen el algoritmo de forma incremental. En primer lugar, consideramos el caso cuando las únicas dos restricciones son de no negatividad ($\boldsymbol{x} \geq \mathbf{0}$) y una presupuestaria ($\boldsymbol{c}^T\boldsymbol{x} \leq u$ para algún escalar u). A partir de ello, generamos una sucesión de ecuaciones lineales enteras cuya solución provee candidatos para el óptimo del problema.

En segundo lugar, agregamos m restricciones de desigualdad además de la presupuestaria. Este es el parteaguas donde el algoritmo toma relevancia, pero donde también aumenta en complejidad y supone ciertas dificultades con los tiempos de terminación. Discutiremos ampliamente posibles direcciones que puedan mejorar de manera significativa la rapidez de nuestro algoritmo.

En tercer lugar, eliminamos la restricción presupuestaria y, por lo tanto, nuestro algoritmo será capaz de resolver problemas lineales enteros en su forma general. Ciertamente esta subsección es la más corta, pues lo único que hacemos es agregar implícitamente una restricción presupuestaria válida resolviendo el problema lineal relajado. Es de esta manera que podremos hacer uso de los resultados obtenidos en la segunda fase.

En cuarto lugar, agregamos consideraciones que facilitan la implementación del algoritmo. En particular, consideramos el caso donde hay una o más restricciones de igualdad, así como el caso donde las variables de decisión son binarias. Finalmente, discutiremos brevemente una extensión a este algoritmo para que sea capaz de resolver problemas lineales mixtos.

Definición 2.1 ([BH09])**.** *Decimos que un vector $\boldsymbol{v} \in \mathbb{R}^n \setminus \{0\}$ es esencialmente entero*[1] *si existen $\boldsymbol{w} \in \mathbb{Z}^n$, $k \in \mathbb{R}$ 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. 1.1) y si su primera entrada es no negativa.*

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

Ejemplo 2.2. *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.*

[1] El artículo los nombra *projectively rational vectors*, mas el autor de esta tesis no encontró una traducción al español establecida, por lo que decidió nombrarlos de la forma que lo hizo. Por la misma razón, el autor decidió traducir *c-layer* como "capa entera" en la Definición 2.3.

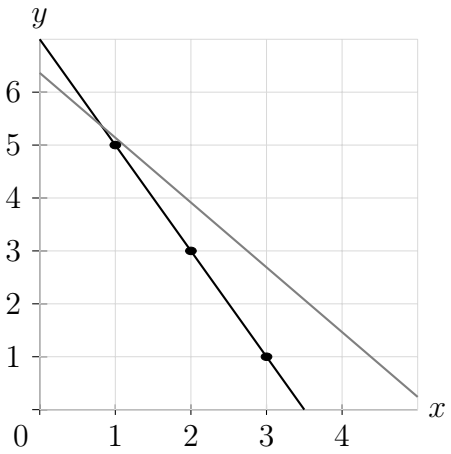

Figura 2.1: Representación de una capa entera (en negro) junto a un hiperplano afino que no es capa entera (en gris). La capa entera tiene como parámetros $\boldsymbol{v} = (2,1)^T$ y $t = 1{,}4$, mientras que los del hiperplano afino son $\boldsymbol{v} = (\sqrt{3}, \sqrt{2})^T$ y $t = 1{,}4$.

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 el punto de vista puramente teórico, esta condición reduce drásticamente el tipo de programas lineales que podemos resolver. No obstante, 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 2.3 ([BH09])**.** *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*

$$H_{\boldsymbol{v},t} \coloneqq \ker\{x \mapsto \boldsymbol{v}^T x\} + t\boldsymbol{v} \tag{2.1}$$

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

Cualquier vector coprimo induce una familia de capas enteras y, sorprendentemente, esa familia contiene a todos los puntos enteros en el espacio, como lo indica el siguiente teorema.

Lema 2.4 ([BH09]). *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 2.5 ([BH09]). *Sea $\boldsymbol{v} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{w}$ su múltiplo coprimo. Entonces la familir de capas enteras $\left\{H_{\boldsymbol{w},k\|\boldsymbol{w}\|^{-2}} : k \in \mathbb{Z}\right\}$ cubre a $\mathbb{Z}^n$.*

Demostración. □

2.1. Fase 1: una restricción presupuestaria

Sea $\boldsymbol{p} \in \mathbb{R}^n$ un vector esencialmente entero y sea $\boldsymbol{q} \in \mathbb{Z}^n$ su múltiplo coprimo. Consideremos el programa lineal

$$\begin{aligned} \max_{\boldsymbol{x}\in\mathbb{R}^n} \quad & \boldsymbol{p}^T\boldsymbol{x}, && \text{(2.2a)} \\ \text{s.a.} \quad & \boldsymbol{p}^T\boldsymbol{x} \geq u, && \text{(2.2b)} \\ & \boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}. \end{aligned}$$

2.2. Fase 2: múltiples restricciones junto con la presupuestaria

2.2.1. Estrategias alternativas para el problema de factibilidad

2.3. Fase 3: múltiples restricciones

2.4. Consideraciones y extensiones del algoritmo

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.