UNIVERSIDAD DE SEVILLA
Facultad de Matemáticas

El problema diofántico de Frobenius

Manuel Jesús Chacón Gómez

Trabajo Fin de Grado

El problema diofántico de Frobenius

Memoria presentada por
Manuel Jesús Chacón Gómez
como Trabajo Fin de Grado
del Grado en Matemáticas
de la Universidad de Sevilla

V^o B^o del Director:

Fdo. José María Tornero Sánchez
Profesor Titular de Universidad
Departamento de Álgebra
Universidad de Sevilla

Sevilla, Diciembre 2016

Índice general

Abstract

In this work, we study the diophantine Frobenius problem. First, in Chapter 1, we briefly present what are numerical semigroups and we see what is the Frobenius number. By the end of this chapter we show that the Frobenius problem is NP-hard. Afterwards, in Chapter 2, we study the Frobenius problem for small n. Finally, in the last chapter, we give some algorithms to solve the general Frobenius problem.

Introducción

En este trabajo, estudiaremos el problema diofántico de Frobenius. Para ello comenzaremos viendo qué es un semigrupo y nos centraremos en un caso especial, los semigrupos numéricos:

$$\langle a_1, \ldots, a_n \rangle = \{a_1 x_1 + \cdots + a_n x_n \mid x_i \in \mathbb{Z}_{\geq 0}\}, \text{ con } \operatorname{mcd}(a_1, \ldots, a_n) = 1.$$

Continuaremos viendo cuáles son los invariantes de un semigrupo, donde introduciremos el número de Frobenius, que es el mayor elemento que no se puede representar como combinación lineal con coeficientes enteros no negativos de $a_1, \ldots, a_n$. Encontrar ese número es el problema de Frobenius, el cual demostraremos que es NP-difícil.

En el capítulo 2, estudiaremos el problema para dimensiones bajas, viendo que para el caso $n = 2$ tenemos una fórmula cerrada, algo que no ocurre cuando aumentamos la dimensión.

Para concluir con el trabajo, estudiaremos algunos algoritmos para resolver el problema de Frobenius en el caso general.

Capítulo 1

Semigrupos y el problema de Frobenius

El estudio de los semigrupos numéricos es equivalente a estudiar la solución entera no negativa de una ecuación lineal no homogénea con coeficientes enteros no negativos. En este estudio tiene especial relevancia un invariante, el número de Frobenius.

1.1. Semigrupos

Definición. *Se llama semigrupo al par $(S, *)$ formado por S un conjunto y una operación binaria interna que verifica la propiedad asociativa, es decir,*

$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$$

Ejemplos.

- $(\mathbb{N}, +)$ *es un semigrupo.*
- $(\mathbb{N}, \cdot)$ *es un semigrupo.*

Nota. *Si un semigrupo $(S, *)$, cumple la propiedad conmutativa, es decir, $a * b = b * a$ $\forall a, b \in S$, diremos que es un semigrupo abeliano.*

Nota. *Normalmente omitiremos la operación binaria $+$ mientras nos referimos a un semigrupo conmutativo y escribiremos S en vez de $(S, +)$.*

Definición. *Un subsemigrupo T del semigrupo S es un subconjunto que es cerrado bajo la operación binaria considerada en S.*

Definición. *Dado A un subconjunto no vacío de S, el subsemigrupo más pequeño de S que contiene a A es la intersección de todos los subsemigrupos de S que contienen a A, notado por $\langle A\rangle$. Es fácil probar que es un semigrupo.*

Definición. *Diremos que S es generado por $A \subseteq S$ si $S = \langle A\rangle$. En este caso, A es un sistema de generadores de S. Si A tiene una cantidad finita de elementos, entonces diremos que S es finitamente generado.*

Ejemplo. *Como hemos visto $S = (\mathbb{N}, +)$ es un semigrupo, el cual es generado por $A = \{1\}$, esto es, $S = \langle A\rangle$ y A es un sistema de generadores finito.*

$S = (\mathbb{N}, \cdot)$ es un semigrupo con infinitos generadores, ya que cualquier conjunto de generadores debe contener a los números primos.

Definición. *Dados dos semigrupos X e Y, la aplicación $f : X \to Y$ es un homomorfismo de semigrupos si $f(a + b) = f(a) + f(b)$ para todo $a, b \in X$.*

Definición. *Un semigrupo numérico es un semigrupo $S \subset \mathbb{Z}_{\geq 0}$ con complementario finito en $\mathbb{Z}_{\geq 0}$ tal que $0 \in S$.*

Ejemplo. *El semigrupo generado por $\{a_1, \ldots, a_n\} \subset \mathbb{Z}_{\geq 0}$, que es el conjunto de combinaciones lineales de estos enteros con coeficientes enteros no negativos:*

$$\langle a_1, \ldots, a_n\rangle = \left\{ \sum_{i=1}^{n} \lambda_i a_i \mid \lambda_i \in \mathbb{Z}_{\geq 0} \right\}$$

Teorema. *[1] Sean enteros no negativos $0 \leq a_1 \leq \cdots \leq a_n$ y supongamos que $\text{mcd}(a_1, \ldots, a_n) = 1$. Consideremos $S = \langle a_1, \ldots, a_n\rangle$. Entonces existe $N \in \mathbb{Z}$ tal que para todo entero $x \geq N$, se tiene que $x \in S$.*

Demostración.

Como el $\text{mcd}(a_1, \ldots, a_n) = 1$, por la identidad de Bezout tenemos

$$m_1 a_1 + \cdots + m_n a_n = 1, \text{ para ciertos } m_i \in \mathbb{Z}.$$

Sean

$$P = \sum_{m_i \geq 0} m_i a_i \geq 0, \quad Q = \sum_{m_i \leq 0} m_i a_i \leq 0$$

P y $-Q$ pertenecen al semigrupo S generado por $\langle a_1, \ldots, a_n\rangle$ y $P + Q = 1$.

Cualquier entero $k \geq 0$ puede escribirse como $k = ha_1 + k'$ con $h \geq 0$ y $0 \leq k' < a_1$ (sería dividir k entre a_1).

Entonces,

$$\begin{aligned}(a_1-1)(-Q)+k &= (a_1-1)(-Q)+ha_1+k' \\ &= ha_1+(a_1-1)(-Q)+(P+Q)k' \\ &= ha_1+(a_1-1-k')(-Q)+k'P \in S,\end{aligned}$$

Porque a_1, P, $-Q \in S$ y todos están multiplicados por enteros no negativos.

Por tanto todo entero $x \geq (a_1-1)Q$ pertenece a S.

□

Nota. *Si* $\text{mcd}(a_1,\ldots,a_n) = d > 1$*, obtendríamos un resultado análogo al anterior trabajando con* $\mathbb{Z}d$ *en vez de* $\mathbb{Z}$*.*

Lema. *[2] Sea* A *un conjunto no vacio de* $\mathbb{N}$*. Entonces* $\langle A\rangle$ *es un semigrupo numérico si y sólo si* $\text{mcd}(A) = 1$*.*

Demostración.

$\boxed{\Longrightarrow}$

Sea $d = \text{mcd}(A)$. Si $s \in \langle A\rangle$, entonces $d|s$. Como $\langle A\rangle$ es un semigrupo numérico, $\mathbb{N}\setminus\langle A\rangle$ es finito, y existe un entero positivo x tal que $d|x$ y $d|(x+1)$. Esto fuerza a que $\text{mcd}(A) = 1$.

$\boxed{\Longleftarrow}$

Esta parte de la demostración es muy similar a la anterior. Es suficiente probar que $\mathbb{N}\setminus\langle A\rangle$ es finito. Como $\text{mcd}(A) = 1$, por la identidad de Bezout tenemos:

$$m_1a_1+\cdots+m_na_n = 1 \text{ con } m_i \in \mathbb{Z} \text{ para } i = 1,\ldots,n$$

y sean

$$P = \sum_{m_i\geq 0} m_ia_i \geq 0, \qquad Q = \sum_{m_i\leq 0} m_ia_i \leq 0.$$

Entonces $P+Q = 1$.

Por el teorema anterior existe $s \in \langle A\rangle$ tal que $s+1 \in \langle A\rangle$. Probemos que si $n \geq (s-1)\,s+(s-1)$, entonces $n \in \langle A\rangle$. Sean q y r los enteros de dividir n entre s tal que $n = qs+r$ con $0 \leq r < s$.

Como $n \geq (s-1)\,s+(s-1)$ deducimos que $q \geq s-1 \geq r$. Entonces $n = (rs+r)+(q-r)\,s = r\,(s+1)+(q-r)\,s \in \langle A\rangle$.

□

Corolario. *Todo semigrupo numérico se puede escribir de la forma* $\langle a_1,\ldots,a_n\rangle$*.*

Demostración.

Sea S un semigrupo numérico, si tomamos elementos $a_1, \ldots, a_n \in S$ tal que $\text{mcd}(a_1, \ldots, a_n) = 1$, tenemos claramente que $\langle a_1, \ldots, a_n \rangle \subset S$ por lo que existe $N \in \mathbb{Z}_{\geq 0}$ como en el teorema, determinado por $\langle a_1, \ldots, a_n \rangle$.

Se obtiene de manera inmediata que

$$\{a_1, \ldots, a_n\} \bigcup \{x \in S \mid x < N\}$$

es un conjunto de generadores de S.

□

Definición. *Algunos de los invariantes asociados a un semigrupo numérico* $S = \langle a_1, \ldots, a_n \rangle$ *son:*

1. *El conjunto de gaps, que es el complementario de* S *en* $\mathbb{Z}_{\geq 0}$*, notado* $G(S)$*.*
2. *El género, que es el cardinal de* $G(S)$*, notado* $g(S)$*.*
3. *El número de Frobenius, que es el máximo entero en* $G(S)$*, notado* $f(S)$*.*
4. *El conductor, que es* $f(s) + 1$ *y se denota por* $c(S)$*.*
5. *El conjunto de elementos esporádicos, que son los elementos de* S *menores que* $f(S)$*, esto es* $S \bigcap [0, f(S)]$*, notado* $N(S)$*.*
6. *El cardinal del conjunto de elementos esporádicos, que se notará* $n(S)$*.*
7. *La multiplicidad, que es el menor elemento no nulo de* S*, notado* $m(S)$*.*
8. *La dimensión, que es el cardinal de un conjunto minimal de generadores, notado* $e(S)$*.*

Ejemplo. *Sea* $S = \langle 5, 7, 11 \rangle$*, vemos todos sus invariantes:*

1. $G(S) = \{1, 2, 3, 4, 6, 8, 9, 13\}$
2. $g(S) = |G(S)| = 8$
3. $f(S) = \max\{G(S)\} = 13$
4. $c(S) = f(S) + 1 = 14$
5. $N(S) = S \bigcap [0, f(S)] = \{5, 7, 10, 11, 12\}$

6. $n(S) = |N(S)| = 5$

7. $m(S) = 5$

8. $e(S) = 3$

1.2. El problema de Frobenius

Sean $a_1, \dots a_n$ enteros positivos con $a_i \geq 2$ para $i = 1, \dots, n$ y de tal manera que $\text{mcd}(a_1, \dots a_n) = 1$. Decimos que x es representable como combinación lineal con coeficientes enteros no negativos de $a_1, \dots a_n$ si existen enteros $\lambda_i \geq 0$ tal que :

$$x = \sum_{i=1}^{n} \lambda_i a_i$$

Frobenius propuso el problema de dar una fórmula para el mayor entero que no es representable como combinación lineal con coeficientes no negativos de un conjunto de enteros positivos con mcd igual 1.

En semigrupos, este problema sería equivalente a dar una fórmula en términos de elementos de un sistema minimal de generadores de un semigrupo numérico S, del mayor entero que no está en S, el número de Frobenius.

La existencia de un entero positivo N tal que cualquier $x \geq N$ es representable como una combinación lineal con coeficientes enteros no negativos de $a_1, \dots, a_n$ es un resultado enunciado anteriormente:

Teorema. *[1] Si el* $\text{mcd}(a_1, \dots a_n) = 1$ *entonces existe un entero* N *tal que cualquier entero* $x \geq N$ *sea representable como combinación lineal con coeficientes enteros no negativos de* $a_1, \dots a_n$.

El problema de Frobenius es también conocido como *money-changing problem* (el problema del cambio del dinero):

> "Dadas n monedas con valores $a_1, \dots, a_n$ con $\text{mcd}(a_1, \dots, a_n) = 1$. ¿Cuál es la cantidad más grande que no podemos devolver con esas monedas?"

A continuación, veremos que el problema de Frobenius es un problema difícil desde el punto de vista del cálculo explícito.

Teorema. *(FNP)[4] El problema de Frobenius es NP-difícil (bajo Turing-reducción).*

Para probar este teorema, mostraremos algunos aspectos relevantes sobre complejidad computacional que necesitamos.

Definición. *Problemas de decisión, son aquellos problemas que solo tienen dos posibles respuestas: sí o no.*

Definición. *Supongamos* Π *y* Π' *son dos problemas, una Turing-reducción en tiempo polinomial de* Π *a* Π' *es un algoritmo A el cual resuelve* Π *usando una subrutina hipotética* A' *para resolver* Π'*, tal que, si* A' *es un algoritmo que resuelve* Π' *tiempo polinomial entonces A podría ser un algoritmo que resuelve* Π *en tiempo polinomial. Diremos que* Π *puede ser Turing-reducido a* Π'*.*

Definición. *Un problema* Π *es NP-difícil si hay un problema de decisión* Π' *NP-completo, tal que* Π' *puede ser Turing-reducido a* Π*.*

Para demostrar el teorema (FNP), tenemos que aplicar la definición anterior, para ello utilizaremos el *problema de la mochila*, el cual es conocido que es NP-completo.[5]

Problema de la mochila: Sean $b_1, \ldots, b_n$ y t enteros positivos. Encontrar, si existen, enteros $x_i \geq 0$ con $1 \leq i \leq n$ tales que $\sum_{i=1}^{n} x_i b_i = t$.

Entonces tenemos que ver que el problema de la mochila puede ser Turing-reducido al problema de Frobenius. Probaremos que usando una subrutina hipotética A que resuelve el problema de Frobenius, podemos crear un algoritmo B para resolver el problema de la mochila:

Sea $\text{mcd}(b_1, \ldots, b_n) = r$. Podemos asumir que $r = 1$, de otro modo consideramos el problema de la mochila con entradas $b_i' = b_i/r$, para cada $i = 1, \ldots, n$, y $t' = t/r$.

Algoritmo B

Encontrar $f(b_1, \ldots, b_n)$

If $t > f(b_1, \ldots, b_n)$ **then**

Existen enteros $x_i \geq 0$ con $1 \leq i \leq n$, tal que $\sum_{i=1}^{n} x_i b_i = t$.

Else

Encuentra $f\left(\overline{b}_1, \ldots, \overline{b}_n, \overline{b}_{n+1}\right)$ donde $\overline{b}_i = 2b_i$ para cada $i = 1, \ldots, n$ y $\overline{b}_{n+1} = 2f(b_1, \ldots, b_n) + 1$ (observemos que $\text{mcd}\left(\overline{b}_1, \ldots, \overline{b}_n, \overline{b}_{n+1}\right) = 1$ y $\overline{b}_{n+1} \equiv 1 \mod 2$).

Encuentra $f\left(\overline{b}_1, \ldots, \overline{b}_n, \overline{b}_{n+1}, \overline{b}_{n+2}\right)$ donde $\overline{b}_{n+2} = f\left(\overline{b}_1, \ldots, \overline{b}_n, \overline{b}_{n+1}\right) - 2t$.

Return

El problema de la mochila tiene respuesta afirmativa si y sólo si $f\left(\overline{b}_1, \ldots, \overline{b}_{n+2}\right) < f\left(\overline{b}_1, \ldots, \overline{b}_{n+1}\right)$.

Antes de probar el teorema (FNP), probaremos la siguiente proposición técnica:

Proposición. *[4] Sean b_i para cada $i = 1, \ldots, n$ y $\overline{b}_i$ para cada $i = 1, \ldots, n+1$ los enteros definidos por el procedimiento B. Entonces,*

$$f\left(\overline{b}_1, \ldots, \overline{b}_{n+1}\right) = 4f\left(b_1, \ldots, b_n\right) + 1.$$

Demostración.

Sea g un entero tal que $g > 4f\left(b_1, \ldots, b_n\right) + 1$. Sea $g' = g - r\overline{b}_{n+1}$, donde $r \equiv g \mod 2$. Si $r = 0$ entonces

$$g' = g > 4f\left(b_1, \ldots, b_n\right) + 1 > 2f\left(b_1, \ldots, b_n\right).$$

Por otro lado, si $r = 1$ entonces

$$g' = g - \overline{b}_{n+1} > 4f\left(b_1, \ldots, b_n\right) + 1 - \left(2f\left(b_1, \ldots, b_n\right) + 1\right) = 2f\left(b_1, \ldots, b_n\right).$$

Por lo tanto, $g' > 2f\left(b_1, \ldots, b_n\right)$ y $g' \equiv 0 \mod 2$ entonces g' es representable como combinación lineal con coeficientes enteros no negativos de $\overline{b}_1, \ldots, \overline{b}_n$. Por lo tanto g es también representable como combinación lineal con coeficientes enteros no negativos de $\overline{b}_1, \ldots, \overline{b}_{n+1}$.

Ahora probaremos por reducción al absurdo que $4f\left(b_1, \ldots, b_n\right) + 1$ no se puede representar como combinación de enteros no negativos de $\overline{b}_1, \ldots, \overline{b}_{n+1}$.

Supongamos que existen enteros $x_i \geq 0$, $1 \leq i \leq n+1$, tal que

$$\sum_{i=1}^{n+1} x_i \overline{b}_i = 4f\left(b_1, \ldots, b_n\right) + 1.$$

Como $4f\left(b_1,\ldots,b_n\right)+1 \not\equiv 0 \mod 2$ entonces $x_{n+1} \geq 1$.

Por otro lado, si $x_{n+1} \geq 2$ entonces $x_{n+1}\overline{b}_{n+1} > 4f\left(b_1,\ldots,b_n\right)+1$ por lo que $x_{n+1} \leq 1$. Por lo tanto $x_{n+1}=1$ luego

$$\sum_{i=1}^{n} x_i\overline{b}_i + \overline{b}_{n+1} = 4f\left(b_1,\ldots,b_n\right)+1$$

y

$$\sum_{i=1}^{n} x_i\overline{b}_i = 2f\left(b_1,\ldots,b_n\right)$$

entonces

$$\sum_{i=1}^{n} x_i b_i = f\left(b_1,\ldots,b_n\right) \text{ lo cual es imposible.}$$

Por lo tanto, $4f\left(b_1,\ldots,b_n\right)+1$, es el mayor número natural que no se puede representar como combinación lineal con coeficientes enteros no negativos de $\overline{b}_1,\ldots,\overline{b}_{n+1}$.

□

Ahora podemos ver que, en efecto el problema de Frobenius es NP-difícil.

Demostración. (FNP)

Sea $t < f\left(b_1,\ldots,b_n\right)$. Veamos que existen enteros $x_i \geq 0$ con $1 \leq i \leq n$, tal que $\sum_{i=1}^{n} x_i b_i = t$ si y sólo si $f\left(\overline{b}_1,\ldots,\overline{b}_{n+2}\right) < f\left(\overline{b}_1,\ldots,\overline{b}_{n+1}\right)$.

$\boxed{\Longrightarrow}$

Supongamos que existen enteros $x_i \geq 0$, $1 \leq i \leq n$, tal que $\sum_{i=1}^{n} x_i b_i = t$. Luego $\sum_{i=1}^{n} x_i\overline{b}_i = 2t$ y como $\overline{b}_{n+2} = f\left(\overline{b}_1,\ldots,\overline{b}_{n+1}\right) - 2t$ entonces

$$f\left(\overline{b}_1,\ldots,\overline{b}_{n+1}\right) = \sum_{i=1}^{n+2} x_i\overline{b}_i.$$

Por lo tanto, $f\left(\overline{b}_1,\ldots,\overline{b}_{n+2}\right) < f\left(\overline{b}_1,\ldots,\overline{b}_{n+1}\right)$.

$\boxed{\Longleftarrow}$

Por otro lado, supongamos que $f\left(\overline{b}_1,\ldots,\overline{b}_{n+2}\right) < f\left(\overline{b}_1,\ldots,\overline{b}_{n+1}\right)$. Por la proposición anterior tenemos que,

$$f\left(\overline{b}_1,\ldots,\overline{b}_{n+1}\right) = 4f\left(b_1,\ldots,b_n\right)+1 = \sum_{i=1}^{n+2} x_i\overline{b}_i$$

para algunos enteros $x_i \geq 0$, con $1 \leq i \leq n+2$.

Como $f\left(\overline{b}_1, \ldots, \overline{b}_{n+1}\right)$ no es representable como combinación lineal con coeficientes enteros no negativos de $\overline{b}_1, \ldots, \overline{b}_{n+1}$ entonces $x_{n+2} \geq 1$.

Por otro lado tenemos

$$x_{n+2}\overline{b}_{n+2} = x_{n+2}\left(f\left(\overline{b}_1, \ldots, \overline{b}_{n+1}\right) - 2t\right)$$

y

$$2t < 2f\left(b_1, \ldots, b_n\right) < \frac{4f\left(b_1, \ldots, b_n\right) + 1}{2}$$

de donde

$$\begin{aligned} x_{n+2}\overline{b}_{n+2} &> x_{n+2}\left(4f\left(b_1, \ldots, b_n\right) + 1 - \left(\frac{4f\left(b_1, \ldots, b_n\right) + 1}{2}\right)\right) \\ &= x_{n+2}\left(\frac{4f\left(b_1, \ldots, b_n\right) + 1}{2}\right). \end{aligned}$$

En consecuencia, si $x_{n+2} \geq 2$ entonces $x_{n+2}\overline{b}_{n+2} > 4f\left(b_1, \ldots, b_n\right)+1$ luego $x_{n+2} \leq 1$. Por lo tanto $x_{n+2} = 1$, así

$$4f\left(b_1, \ldots, b_n\right) + 1 = \sum_{i=1}^{n+1} x_i\overline{b}_i + \overline{b}_{n+2}$$

y

$$4f\left(b_1, \ldots, b_n\right) + 1 = \sum_{i=1}^{n+1} x_i\overline{b}_i + f\left(\overline{b}_1, \ldots, \overline{b}_{n+1}\right) - 2t.$$

Entonces

$$2t = \sum_{i=1}^{n+1} x_i\overline{b}_i.$$

Finalmente, $\overline{b}_{n+1} = 2f\left(b_1, \ldots, b_n\right) + 1 > 2t$ llegamos a que $x_{n+1} = 0$. Por lo tanto,

$$2t = \sum_{i=1}^{n} x_i\overline{b}_i$$

de donde

$$t = \sum_{i=1}^{n} x_i b_i.$$

□

Capítulo 2

Problema de Frobenius para dimensiones bajas ($n \leq 4$)

En este capítulo se demostrarán algunos resultados. Para los que no se demuestren, se dejará indicada la referencia original.

Hasta ahora hemos visto que el cálculo del problema de Frobenius es complejo en general, sin embargo existen algoritmos, que bajo algunas condiciones, pueden resolverlo con mayor o menor eficiencia. El caso caso $n = 2$, es muy particular, ya que tenemos una fórmula explícita para calcularlo.

2.1. Cálculo de $f(a_1, a_2)$

Anteriormente definimos $g(a_1, \ldots, a_n)$ como el género, que es el cardinal de $G(a_1, \ldots, a_n)$, el conjunto de gaps. El estudio de $g(a_1, \ldots, a_n)$ data de principios del 1882 en los artículos de J.J. Sylvester [6], el cual dio una fórmula explícita para calcular $g(a_1, a_2)$.

Teorema. *[6] Sean a_1 y a_2 dos enteros positivos tal que* $\text{mcd}(a_1, a_2) = 1$. *Entonces,*

$$g(a_1, a_2) = \frac{1}{2}(a_1 - 1)(a_2 - 1).$$

Demostración.

Consideramos el producto

$$(1 + x^{a_1} + x^{2a_1} + \cdots + x^{a_1 a_2})(1 + x^{a_2} + x^{2a_2} + \cdots + x^{a_1 a_2}),$$

y analizaremos cómo son los elementos. Cada término entre 1 y $x^{a_1 a_2}$ corresponde a un número menor que $a_1 a_2$, y de la forma $ma_1 + na_2$. Como

$x^{a_1a_2}$ aparece dos veces, tenemos $2x^{a_1a_2}$. Notemos que la primera y última multiplicación sólo aparecen una vez: 1 y $x^{2a_1a_2}$.

Como tenemos dos veces el número de enteros de la forma $ma_1 + na_2$ y menores que a_1a_2, cuando $x = 1$ en el anterior producto, el número de estos enteros es

$$\frac{1}{2}(a_1 + 1)(a_2 + 1) - 2.$$

Entonces, el número de enteros que no se pueden poner de esta forma es

$$a_1a_2 - 1 - \left[\frac{1}{2}(a_1 + 1)(a_2 + 1) - 2\right] = \frac{1}{2}\left[a_1a_2 - a_1 - a_2 + 1\right] = \frac{1}{2}(a_1 - 1)(a_2 - 1).$$

□

A continuación, veremos que podemos calcular $f(a_1, a_2)$ fácilmente.

Teorema. *[7] Sea a_1 y a_2 dos números naturales con* $\mathrm{mcd}(a_1, a_2) = 1$. *Entonces*

$$f(a_1, a_2) = a_1a_2 - a_1 - a_2.$$

Demostración.

Como $\mathrm{mcd}(a_1, a_2) = 1$, entonces cualquier entero N es representable como $N = xa_1 + ya_2$ con $x, y \in \mathbb{Z}$. La representación sería única si pedimos que $0 \leq x < a_2$. En este caso, N se puede representar si $y \geq 0$. Por lo tanto, el mayor valor de N que no podríamos representar es cuando $x = a_2 - 1$ y $y = -1$. Luego,

$$f(a_1, a_2) = (a_2 - 1)a_1 + (-1)a_2 = a_1a_2 - a_1 - a_2.$$

□

Ejemplo. *Calcular el número de Frobenius para el semigrupo $S = \langle 13, 23\rangle$.*

Simplemente aplicamos el teorema anterior:

- $\mathrm{mcd}(13, 23) = 1$
- $f(13, 23) = 13 \cdot 23 - 13 - 23 = 263$

En este caso, también podemos calcular el género fácilmente, aplicando el primer teorema:

- $g(13, 23) = 1/2(13 - 1)(23 - 1) = 132.$

Como podemos comprobar el cálculo del número de Frobenius cuando $n = 2$ es muy simple, algo que no ocurre cuando vamos aumentando n.

2.2. Algoritmos para calcular $f(a_1, a_2, a_3)$

Contrariamente al caso $n = 2$, el cálculo de una fórmula explícita para $f(a_1, a_2, a_3)$ resultó ser muy difícil. Como veremos a continuación existen varios algoritmos para calcular $f(a_1, a_2, a_3)$ en tiempo polinomial, pero no hay esperanza de dar con un algoritmo rápido para resolverlo en el caso general, a no ser que P=NP.

2.2.1. Algoritmo de Rødseth

E.S. Selmer y O. Beyer [8] desarrollaron un algoritmo que era capaz de calcular $f(a_1, a_2, a_3)$. Su método se basaba en muchas manipulaciones de fracciones continuas, algo difícil de implementar, por lo que Ø.J. Rødseth [9] modificó el algoritmo de Selmer-Beyer para simplificarlo, usando "restos negativos" en las divisiones del algoritmo de la fracción continua. Veamos en qué consiste el algoritmo.

Algoritmo de Rødseth:

Sea s_0 el único entero tal que $a_2 s_0 \equiv a_3 \mod a_1$ con $0 \leq s_0 < a_1$.

Aplicamos el algoritmo de la fracción continua con los "restos negativos" para a_1/s_0:

$$a_1 = q_1 s_0 - s_1 \text{ con } 0 \leq s_1 < s_0,$$

$$s_0 = q_2 s_1 - s_2 \text{ con } 0 \leq s_2 < s_1,$$

$$s_1 = q_3 s_2 - s_3 \text{ con } 0 \leq s_3 < s_2,$$

$$\vdots$$

$$s_{m-1} = q_{m+1} s_m,$$

$$s_{m+1} = 0$$

donde $q_i \geq 2$, $s_i \geq 0$ para todo i.

Sean $p_{-1} = 0$, $p_0 = 1$, $p_{i+1} = q_{i+1} p_i - p_{i-1}$ y $r_i = (s_i a_2 - p_i a_3)/a_1$.

Sea v el único número entero tal que $r_{v+1} \leq 0 < r_v$, o equivalentemente, el único entero tal que

$$\frac{s_{v+1}}{p_{v+1}} \leq \frac{a_3}{a_2} < \frac{s_v}{p_v}.$$

Entonces,

$$f(a_1, a_2, a_3) = -a_1 + a_2 (s_v - 1) + a_3 (p_{v+1} - 1) - \min \{a_2 s_{v+1}, a_3 p_v\}.$$

Nota. *El algoritmo de Rødseth tiene una complejidad media de* $O(\log a_2)$ *y en el peor de los casos* $O(a_1 + \log a_2)$ *operaciones, ya que implica la longitud de una fracción continua semi-regular para* a_3/a_2*, la cual puede ser tan larga como* a_2*.*

Ejemplo. *Calcularemos* $f(5, 9, 13)$ *usando el algoritmo de Rødseth.*

- *En primer lugar veremos el valor de* s_0*, recordamos que es el único entero tal que* $a_2 s_0 \equiv a_3 \mod a_1$ *con* $0 \leq s_0 < a_1$*.*

  En nuestro caso $s_0 \in \{0, 1, 2, 3, 4\}$ *y vemos que el único valor que cumple la condición anterior es* $s_0 = 2$*.*

- *Aplicamos el algoritmo de la fracción continua:*

$$5 = q_1 \cdot 2 - s_1 \text{ con } 0 \leq s_1 < 2 \quad \Rightarrow \quad q_1 = 3,\ s_1 = 1$$

$$2 = q_2 \cdot 1 - s_2 \text{ con } 0 \leq s_2 < 1 \quad \Rightarrow \quad q_2 = 2,\ s_2 = 0$$

- *Definimos* $p_{-1} = 0$*,* $p_0 = 1$*,* $p_{i+1} = q_{i+1} p_i - p_{i-1}$*.*

  Tenemos que $p_1 = 3$*,* $p_2 = 5$*.*

- *Sea* v *el único entero tal que* $r_{v+1} \leq 0 < r_v$ *con* $r_i = (s_i a_2 - p_i a_3)/a_1$ *o equivalentemente,*

$$\frac{s_{v+1}}{p_{v+1}} \leq \frac{a_3}{a_2} < \frac{s_v}{p_v}.$$

  En nuestro ejemplo $v = 0$*.*

- *Entonces, aplicando la fórmula del final del algoritmo tenemos:*

$$f(5, 9, 13) = -5 + 9(2 - 1) + 13(3 - 1) - \min\{9, 13\} = 21.$$

2.2.2. Algoritmo de Davison

J.L. Davison [10] modificó el algoritmo de Rødseth y Selmer-Beyer, para conseguir una complejidad de $O(\log a_2)$ para todas las entradas. Veamos algunos conceptos previos en los que se basa el método de Davison.

Definición. *Sea* $b(a_1, \ldots, a_n)$ *el mayor entero no representable como combinación lineal de* $a_1, \ldots, a_n$ *con coeficientes enteros positivos, es decir,*

$$b(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + \sum_{i=1}^{n} a_i.$$

Teorema. *[11] Sean* $d_{12} = \text{mcd}(a_1, a_2)$, $d_{13} = \text{mcd}(a_1, a_3)$ *y* $d_{23} = \text{mcd}(a_2, a_3)$. *Entonces tenemos,*

$$b(a_1, a_2, a_3) = b\left(\frac{a_1}{d_{12}d_{13}}, \frac{a_2}{d_{12}d_{23}}, \frac{a_3}{d_{13}d_{23}}\right) d_{12}d_{13}d_{23}.$$

El algoritmo de Davison en realidad calcula el entero $b\,(a_1, a_2, a_3)$. Para ello utiliza el teorema anterior, que fue demostrado por Johnson, y la definición de $b\,(a_1, a_2, a_3)$. Veamos cómo funciona:

Algoritmo de Davison:
Sean $1 < a < b < c$ enteros positivos, primos relativos por parejas.

1. Resolver $bs \equiv c \mod a$ con $0 < s < a$

   If $bs < c$ **Then** c es dependiente de a y b y

   $f\,(a, b, c) = b\,(a, b, c) - a - b - c = ab + c - a - b - c = ab - a - b$ y **STOP**.

2. Usando el algoritmo de división euclídea para s y a:

$$a = a_1 s + r_1 \text{ con } 0 \leq r_1 < s,$$

$$s = a_2 r_1 + r_2 \text{ con } 0 \leq r_2 < r_1$$

$$r_1 = a_3 r_2 + r_3 \text{ con } 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{m-2} = a_m r_{m-1} + r_m \text{ con } 0 \leq r_m < r_{m-1}$$

   donde $s = r_0 > r_1 > r_2 > \ldots > r_{m-1} = 1 > r_m = 0$.

3. Sea $q_{i+1} = a_{i+1}q_i + q_{i-1}$ para $i = 1, \ldots, m-1$ con $q_0 = 1$ y $q_1 = a_1$, encontrar k tal que

$$\frac{r_{2k}}{q_{2k}} < \frac{c}{b} < \frac{r_{2k-2}}{q_{2k-2}}$$

   (notar que $k \geq 1$ ya que $bs > c$).

4. Sea

$$\Phi(t) = \frac{r_{2k-2} - tr_{2k-1}}{q_{2k-2} + tq_{2k-1}}$$

   usando una búsqueda binaria para encontrar el valor t^* el cual satisface:

$$\Phi(t^*) < \frac{c}{b} < \Phi(t^* - 1), \text{ donde } 1 \leq t^* \leq a_{2k}.$$

   (esto es posible ya que la función Φ es estrictamente decreciente en el intervalo $[0, a_{2k}]$).

5. Fijando

$$x' = r_{2k-2} - (t^* - 1)r_{2k-1}, \quad y' = q_{2k-2} + (t^* - 1)q_{2k-1}$$

y

$$x'' = r_{2k-2} - t^* r_{2k-1}, \quad y'' = q_{2k-2} + t^* q_{2k-1}.$$

Entonces,

$$\begin{aligned} f(a,b,c) &= b(a,b,c) - a - b - c \\ &= \max\{bx' + cq_{2k-1}, cy'' + br_{2k-1}\} - a - b - c \end{aligned}$$

y **STOP**.

Nota. *La complejidad en los pasos 1, 2, 3 y 4 es* $O(\log a)$*, el último paso no tendría peso en el cálculo de la complejidad (*$O(1)$*). También notar que la complejidad, suponiendo que* a*,* b *y* c *sean coprimos dos a dos, es* $O(\log b)$*.*

Ejemplo. *Calcularemos* $f(5,9,13)$ *mediante el algoritmo anterior.*

- *Previamente comprobamos que* $1 < a < b < c$ *y que son primos relativos por parejas, para poder aplicar el algoritmo.*

1. *Resolvemos* $bs \equiv c \mod a$ *con* $0 < s < a$*, como en el ejemplo anterior* $s = 2$

2. *Aplicamos el algoritmo de la división euclidea:*

$$5 = a_1 \cdot 2 + r_1 \text{ con } 0 \le r_1 < 2 \quad \Rightarrow \quad a_1 = 2 \text{ y } r_1 = 1$$

$$2 = a_2 \cdot 1 + r_2 \text{ con } 0 \le r_2 < 1 \quad \Rightarrow \quad a_2 = 2 \text{ y } r_1 = 0$$

cumple que $s = r_0 = 2 > r_1 = 1 > r_2 = 0$*.*

3. *Definimos* $q_{i+1} = a_{i+1}q_i + q_{i-1}$ *para* $i = 1$*,* $q_0 = 1$*,* $q_1 = a_1 = 2$*,* $q_2 = 5$*. Buscamos* k *tal que*

$$\frac{r_{2k}}{q_{2k}} < \frac{c}{b} < \frac{r_{2k-2}}{q_{2k-2}}, \text{ entonces } k = 1.$$

4. *Sea*

$$\Phi(t) = \frac{r_{2k-2} - tr_{2k-1}}{q_{2k-2} + tq_{2k-1}},$$

buscamos t^* *tal que*

$$\Phi(t^*) < \frac{c}{b} < \Phi(t^* - 1) \text{ con } 1 \le t^* \le a_{2k},$$

como $k = 1$ *entonces* $t^* = 1$ *ó* 2*.*

Comprobamos que el único valor de t^* *que cumple la desigualdad es* $t^* = 1$*.*

5. *Recordar* $K = 1$ *y* $t^* = 1$. *Definimos:*

$$\begin{array}{rclcl} x' & = & r_{2k-2} - (t^* - 1)r_{2k-1} & = & 2 \\ x'' & = & r_{2k-2} - t^* r_{2k-1} & = & 1 \\ y' & = & q_{2k-2} + (t^* - 1)q_{2k-1} & = & 1 \\ y'' & = & q_{2k-2} + t^* q_{2k-1} & = & 3 \end{array}$$

Entonces aplicando el último paso del algoritmo,

$$\begin{aligned} f(5,9,13) &= b(5,9,13) - 5 - 9 - 13 \\ &= \max\{9 \cdot 2 + 13 \cdot 2, 13 \cdot 3 + 9 \cdot 1\} - 5 - 9 - 13 \\ &= \max\{44, 48\} - 27 = 21. \end{aligned}$$

2.2.3. Método de Killingbergtrø

H.G. Killingbergtrø [12] dio un nuevo enfoque al estudiar del problema de Frobenius cuando $n = 4$. Desarrolló un método que se basaba en construir "figuras-cubo" de las que se puede sacar información para resolver el problema de Frobenius. Killingbergtrø presentó un método para una elección de casos arbitrarios (ejemplificado para $a_1 = 103$, $a_2 = 133$, $a_3 = 165$ y $a_4 = 228$) y argumentó que podía ser aplicado para cualquier $n \geq 3$.

Consideremos el método de Killingbergtrø para tres enteros arbitrarios a_1, a_2 y a_3. La idea principal es construir una figura con cuadrados unidad en el primer cuadrante.

Algoritmo de Killingbergtrø:
Sea L_1 (resp. L_2 y L_3) el menor entero tal que $L_1 a_1$ (resp. $L_2 a_2$ y $L_3 a_3$) es representable como combinación lineal con coeficientes enteros no negativos de $\{a_2, a_3\}$ (resp. representable por $\{a_1, a_3\}$ y por $\{a_1, a_2\}$).

Suponemos que, $a_1 L_1 = (a_2, a_3) \cdot (p_1, p_2)$, para algunos enteros positivos p_1, p_2 y denotamos por $(x, y) - \textit{cuadrado}$ el cuadrado unidad con vértices $\{x, x+1, y, y+1\}$.

Sean

$$\begin{aligned} C &= \{\text{Todos los cuadrados unidad del primer cuadrante}\} \\ C_1 &= \{(x,y)\text{-cuadrados con } x > p_1 \text{ y } y > p_2\} \\ C_2 &= \{(x,y)\text{-cuadrados con } x > L_2\} \\ C_3 &= \{(x,y)\text{-cuadrados con } y > L_3\}. \end{aligned}$$

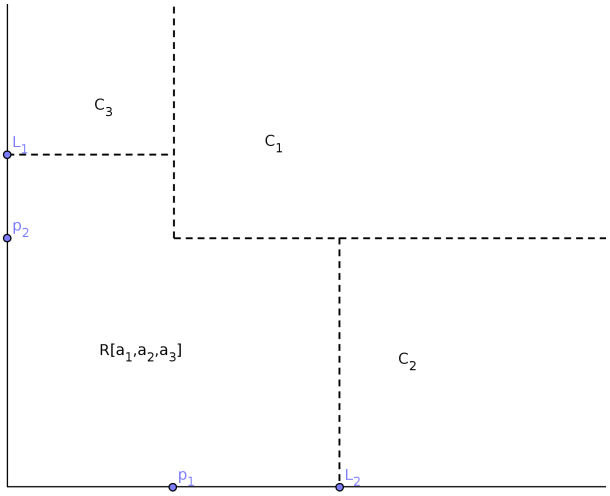


Figura 2.1: $R\left[a_1, a_2, a_3\right]$.

Definimos $R\left[a_1, a_2, a_3\right] := C \backslash \{C_1 \cup C_2 \cup C_3\}$, (ver Figura 2.1) $R\left[a_1, a_2, a_3\right]$ lo denominaremos como figura cúbica.

Sea BLC el conjunto de todos los puntos enteros $c = (c_1, c_2)$ tal que c es la esquina inferior izquierda de los cuadrados que pertenecen a $R\left[a_1, a_2, a_3\right]$. Entonces,

$$f(a_1, a_2, a_3) = \max\left\{c_1 a_2 + c_2 a_3 \mid (c_1, c_2) \in BLC\right\} - a_1.$$

Ejemplo. *Calcularemos $f(5, 9, 13)$ aplicando el algoritmo de Killingbergtrø.*

- *En primer lugar calcularemos L_i con $i = 1, 2, 3$. Para L_1 tenemos que buscar el menor entero tal que $a_1 L_1$ sea combinación lineal con coeficientes enteros no negativos de a_1 y a_2 (análogo para L_2 y L_3).*

$$\begin{aligned} a_1 L_1 = (a_2, a_3) \cdot (p_1, p_2) \quad &\Rightarrow \quad (p_1, p_2) = (1, 2),\ L_1 = 7 \\ a_2 L_2 = (a_1, a_3) \cdot (p_1', p_2') \quad &\Rightarrow \quad (p_1', p_2') = (1, 1),\ L_2 = 2 \\ a_3 L_3 = (a_1, a_2) \cdot (p_1'', p_2'') \quad &\Rightarrow \quad (p_1'', p_2'') = (6, 1),\ L_3 = 3 \end{aligned}$$

- *Veamos quienes son C_1, C_2 y C_3:*

$$\begin{aligned} C_1 &= \{(x, y)\text{-cuadrados con } x > 1 \text{ y } y > 2\} \\ C_2 &= \{(x, y)\text{-cuadrados con } x > 2\} \\ C_3 &= \{(x, y)\text{-cuadrados con } y > 3\} \end{aligned}$$

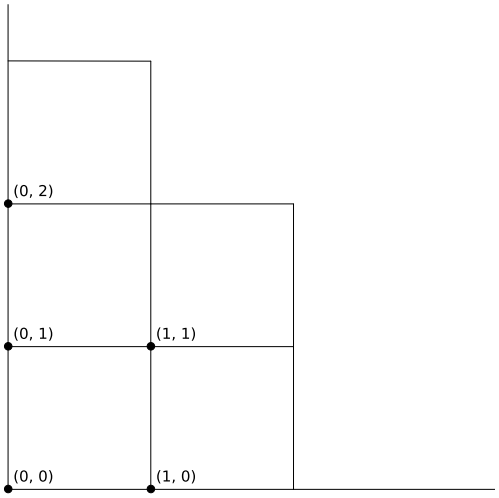


Figura 2.2: $R\,[5, 9, 13]$ con los puntos BLC.

- $R\,[5, 9, 13] = C \setminus \{C_1 \cup C_2 \cup C_3\}$ *(ver Figura 2.2)*
- *Observando la Figura 2.2, el conjunto*

$$BLC = \{(0, 0), (1, 0), (0, 1), (1, 1), (0, 2)\}\,.$$

- *Entonces,*

$$f(5, 9, 13) = \max\{9 \cdot c_1 + 13 \cdot c_2 \mid (c_1, c_2) \in BLC\} - a_1 = 26 - 5 = 21$$

Nota. *La complejidad del método de Killingbergtrø depende de lo eficiente que seamos a la hora de encontrar los enteros L_i.*

2.3. Una fórmula para $f(a_1, a_2, a_3)$

Hasta ahora hemos visto algunos algoritmos para calcular $f(a_1, a_2, a_3)$, pero no tenemos una fórmula explícita para calcularlo. F. Curtis [13], demostró que para el caso $n = 3$, y en consecuencia cuando $n \geq 3$, no existe una fórmula explícita que pueda calcular el número de Frobenius.

Teorema. *(TFC) [13] Sea*

$$A = \left\{(a_1, a_2, a_3) \in \mathbb{N}^3 \mid a_1 < a_2 < a_3, a_1 \text{ y } a_2 \text{ son primos, } a_1 \nmid a_3 \text{ y } a_2 \nmid a_3\right\}.$$

Entonces no existe un polinomio no nulo $H \in \mathbf{C}\,[X_1, X_2, X_3, Y]$ tal que $H(a_1, a_2, a_3, f(a_1, a_2, a_3)) = 0$ para todo $(a_1, a_2, a_3) \in A$.

Para demostrar el teorema (TFC) necesitaremos de los siguientes lemas técnicos:

Lema. *[13] Sean $\alpha \in \mathbb{R}^+$ y $\epsilon > 0$ dados. Sea p un primo y $i,\ j \in \mathbb{N}$ con $\mathrm{mcd}(p,i) = \mathrm{mcd}(p,j) = 1$. Entonces existe $x,\ y \in \mathbb{N}$ tal que x es primo, $x \equiv i \mod p$, $y \equiv j \mod p$, $\mathrm{mcd}(x,y) = 1$, y $|\alpha - y/x| < \epsilon$.*

Lema. *[13] Sea $S = \langle a_1, a_2, a_3 \rangle$ un semigrupo, donde $2 < a_1 < a_2 < a_3$. Sea $2 \leq k \leq a_1 - 1/2 + 1$, y suponemos que $a_1 - k < a_3/a_2 < a_1 - k + 1$ con $a_2 \equiv 1 \mod a_1$ y $a_3 \equiv a_1 - k + 1 \mod a_1$. Entonces,*

$$f(a_1, a_2, a_3) = (k-2)a_2 + a_3 - a_1.$$

Demostración. (TFC)

Razonaremos por reducción al absurdo, supongamos que existe un polinomio H en las condiciones del teorema.

Fijamos un primo $p \neq 2$ y sea $2 \leq k \leq \dfrac{p-1}{2+1}$.

Sea $J(X_2, X_3) = H(p, X_2, X_3, (k-2)X_2 + X_3 - p)$.

Sea $\alpha \in (p-k, p-k+1)$ un irracional. Para $n = 1, 2, 3, \ldots$, por el primer lema elegimos, $x_n \equiv 1 \mod p$, $y_n \equiv p - k + 1 \mod p$, con x_n primo, $\mathrm{mcd}(x_n, y_n) = 1$ y $|\alpha - y_n/x_n| < 1/n$.

Entonces $(p, x_n, y_n) \in A$ y por el segundo lema, $J(x_n, y_n) = 0$. Sea $J^*(X_2, X_3, Z)$ la homogeneización de J con respecto a Z en $\mathbb{C}[X_2, X_3, Z]$.

Entonces $J^*(x_n, y_n, 1) = 0$, lo cual implica $J^*(1, y_n/x_n, 1/x_n) = 0$, luego por continuidad $J^*(1, \alpha, 0) = 0$ para cualquier α. Asi la curva proyectiva $\gamma(J^*)$ contiene infinitos puntos $(1 : \alpha : 0)$, en consecuencia $\gamma(J^*)$ contiene a $\gamma(Z)$. Se sigue que $Z | J^*$, luego $J(X_2, X_3) = 0$.

Fijamos ahora un primo $p > 2$, $P(X_2, X_3, Y) = H(p, X_2, X_3, Y)$, y como antes, sea $P^*(X_2, X_3, Y, Z)$ la homogeneización de P con respecto a Z en $\mathbb{C}[X_2, X_3, Y, Z]$.

Entonces P^* se anula en el hiperplano $\gamma((k-2)X_2 + X_3 - Y - pZ)$ para $k = 2, \ldots, p - 1/2 + 1$, luego $\deg P = \deg P^* \geq p - 1/2$. Así, tiene que cumplir

$$\deg H \geq \frac{p-1}{2}$$

para todo primo $p > 2$, y entonces no existe H.

□

El siguiente corolario nos muestra que $f(a_1, a_2, a_3)$ no puede ser determinado por ningún conjunto de fórmulas explícitas las cuales podrían ser

reducidas a un conjunto finito de polinomios cuando están restringidas al conjunto A.

Corolario. *[13] No existe un conjunto finito de polinomios* $\{h_1, \ldots, h_n\}$, *tal que para cada terna* (a_1, a_2, a_3) *exista algún* h_i *tal que* $h_i(a_1, a_2, a_3) = f(a_1, a_2, a_3)$.

Demostración.

$H = \prod_{i=1}^{n} (h_i(X_1, X_2, X_3) - Y)$ se anularía en A.

□

Los intentos de dar una fórmula general para $f(a_1, a_2, a_3)$, pasan por usar L_1, L_2 y L_3 que, como ya vimos en el algoritmo de Killingbergtrø, son los menores enteros positivos tal que existen enteros $x_{ij} \geq 0$, $1 \leq i, j \leq 3$, $i \neq j$ con

$$L_1 a_1 = x_{12} a_2 + x_{13} a_3,$$

$$L_2 a_2 = x_{21} a_1 + x_{23} a_3,$$

$$L_3 a_3 = x_{31} a_1 + x_{32} a_2.$$

Teorema. *[1] Sean* a_1, a_2 *y* a_3 *coprimos dos a dos y* $\{i, j, k\} = \{1, 2, 3\}$. *Entonces,*

$$f(a_1, a_2, a_3) = \begin{cases} \max\{L_i a_i + x_{jk} a_k, L_j a_j + x_{ik} a_k\} - \sum_{n=1}^{3} a_n & \text{si } x_{ij} > 0 \quad \forall i, j \\ L_j a_j + L_i a_i - \sum_{n=1}^{3} a_n & \text{si } x_{ij} = 0 \end{cases}$$

La siguiente fórmula fue dada por S.M. Johnson [11].

Teorema. *[11] Sean* a_1, a_2 *y* a_3 *coprimos dos a dos,* $L_i > 1$ *para* $i = 1, 2, 3$ *y* $x_{i,j} > 0$ *para todo* $i \neq j$, *entonces*

$$f(a_1, a_2, a_3) = L_i a_i + \max_{j,k \neq i} \{x_{jk} a_k, x_{kj} a_j\} - \sum_{n=1}^{3} a_n.$$

Observemos, que por las hipótesis del teorema anterior no podemos obtener el número de Frobenius con seguridad cuando $n = 3$ (por ejemplo, $f(4, 9, 25)$ ya que $x_{13} = x_{23} = 0$ y $L_3 = 1$).

La fórmula del primer teorema no tiene esas limitaciones y es válida para cualquier terna (a_1, a_2, a_3), el problema que tiene es calcular los L_i de manera eficiente.

La siguiente fórmula, que tiene relación con las anteriores, fue obtenida en 2004 por L.G Fel [14].

$$f(a_1,a_2,a_3)=\frac{1}{2}\left(W+\sqrt{W^2-4\left(w_1w_2+w_1w_3+w_2w_3+a_1a_2a_3\right)}\right)-(a_1+a_2+a_3)$$

donde $w_i=L_ia_i$ para $i=1,2,3$ y $W=w_1+w_2+w_3$.

2.4. Algunos casos particulares de $f(a_1,a_2,a_3)$

A continuación, en esta sección veremos algunos casos particulares para calcular $f(a_1,a_2,a_3)$ y algunos resultados que nos pueden ayudar a simplificar el problema. Por ejemplo S.M. Johnson [11] demostró que si $\mathrm{mcd}(a_1,a_2)=d$ puede ser eliminado con el fin de calcular $f(a_1,a_2,a_3)$.

Teorema. *[11] Si a_1, a_2 y a_3 son primos relativos y $\mathrm{mcd}(a_1,a_2)=d$ entonces*

$$f(a_1,a_2,a_3)=df\left(\frac{a_1}{d},\frac{a_2}{d},a_3\right)+(d-1)a_3.$$

Demostración.

Sea $\mathrm{mcd}(a_1,a_2)=d$ y $\mathrm{mcd}(a_1,a_3)=\mathrm{mcd}(a_2,a_3)=1$, entonces por un teorema anterior (ver sección 2.2.2) tenemos que:

$$b(a_1,a_2,a_3)=b\left(\frac{a_1}{d},\frac{a_2}{d},a_3\right)d.$$

Aplicando la definición de $b(a_1,a_2,a_3)$ en ambos lados de la igualdad:

$$f(a_1,a_2,a_3)+\sum_{i=1}^{3}a_i=d\left(f\left(\frac{a_1}{d},\frac{a_2}{d},a_3\right)+\frac{a_1}{d}+\frac{a_2}{d}+a_3\right).$$

Entonces, operando obtenemos:

$$\begin{aligned}f(a_1,a_2,a_3)\ &=df\left(\frac{a_1}{d},\frac{a_2}{d},a_3\right)+a_1+a_2+da_3-\sum_{i=1}^{3}a_i=\\&=df\left(\frac{a_1}{d},\frac{a_2}{d},a_3\right)+(d-1)a_3.\end{aligned}$$

□

Del teorema anterior, podemos obtener el siguiente corolario:

Corolario. *En las condiciones anteriores, si además $a_3\geq f\left(\frac{a_1}{d},\frac{a_2}{d}\right)$, entonces*

$$f(a_1,a_2,a_3)=d(a_1a_2-a_1-a_2)+(d-1)a_3.$$

Z. Oiu y C.Niu [15] generalizaron el resultado anterior de la siguiente manera.

Teorema. *[15] Sea* $\text{mcd}(a_1, a_3) = d$, $a_1 = a_1'd$ *y* $a_2 = a_2'd$ *tal que existen enteros* $x_1, x_2 \geq 0$ *con* $a_3 = x_1a_1' + x_2a_2'$. *Entonces,*

$$f(a_1, a_2, a_3) = \frac{a_1a_2}{d} - a_1 - a_2 + (d-1)a_3.$$

Brauer y Shockley [16] generalizaron el resultado de Johnson para $n \geq 1$ en el siguiente lema:

Lema. *[16] Sea* $d = \text{mcd}(a_1, \ldots, a_{n-1})$. *Entonces*

$$f(a_1, \ldots, a_n) = df\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) + (d-1)a_n.$$

Demostración.

Probaremos que

$$f(a_1, \ldots, a_n) = df\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) + (d-1)a_n$$

si y sólo si

$$b(a_1, \ldots, a_n) - \sum_{i=1}^{n} a_i = db\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) - d\sum_{i=1}^{n-1}\frac{a_i}{d} - da_n + (d-1)a_n$$

o equivalentemente, si y sólo si

$$\begin{aligned} b(a_1, \ldots, a_n) &= db\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) + a_n - da_n + (d-1)a_n \\ &= db\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right). \end{aligned}$$

Notar que $b(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_ix_i$ con $x_i > 0$. Luego podemos escribir $a_n + b(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_ix_i + a_nx_n$ con $x_i > 0$ y así

$$b(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_ix_i + a_n(x_n - 1).$$

Por definición de b, se tiene que cumplir que $x_n = 1$.

Sea $a_i = da'_i$, $i = 1, \ldots, n-1$. Entonces,

$$b(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_i x_i = d \sum_{i=1}^{n-1} a'_i x_i \tag{2.1}$$

y b es divisible por d, es decir $b = db'$.

Claramente b' no puede ser expresado como combinación lineal con coeficientes enteros positivos de $a'_1, \ldots, a'_n$.

Si $h > b'$ entonces h puede expresarse como combinación lineal con coeficientes enteros positivos de $a'_1, \ldots, a'_{n-1}, a_n$. Como $hd > b'd = b$ entonces

$$hd = \sum_{i=1}^{n} a_i z_i = z_n a_n + d \sum_{i=1}^{n-1} a'_i z_i \text{ con } z_i > 0.$$

Luego, d tiene que dividir a z_n, es decir $z_i = dz'_i$ con $i = 1, \ldots, n$, y

$$h = z'_n a_n + \sum_{i=1}^{n-1} a'_i z_i.$$

Finalmente, $b' = b(a'_1, \ldots, a'_{n-1}, a_n)$ y la ecuación (2.1) tenemos que

$$b(a_1, \ldots, a_n) = db\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right).$$

□

A continuación, veremos otro lema importante de Brauer y Shockley.

Lema. *[16]*

$$f(a_1, \ldots, a_n) = \max_{l \in \{1,2,\ldots,a_n - 1\}} \{t_l\} - a_n$$

donde t_l es el menor entero positivo congruente con l módulo a_n, que es expresado como combinación lineal con coeficientes enteros no negativos de $a_1, \ldots, a_{n-1}$.

Demostración.

Sea L un entero positivo. Si $L \equiv 0 \mod a_n$ entonces L es una combinación lineal con coeficientes enteros no negativos de a_n.

Si $L \equiv l \mod a_n$ entonces L es una combinación lineal con coeficientes enteros no negativos de $a_1, \ldots, a_n$ si y sólo si $L \geq t_l$.

□

Los métodos obtenidos por Brauer y Shockley pueden dar el valor exacto para algunos casos especiales de $n = 3$, por ejemplo, si a_1, a_2, a_3 son primos relativos y $a_1|(a_2 + a_3)$ entonces

$$f(a_1, a_2, a_3) = -a_1 + \max\left\{a_2 \left\lfloor \frac{a_1 a_3}{a_2 + a_3} \right\rfloor, a_3 \left\lfloor \frac{a_1 a_2}{a_2 + a_3} \right\rfloor\right\}.$$

Otro resultado particular que puede ser interesante fue dado por J.B. Roberts [17]. Previamente veremos el siguiente lema el cual utilizaremos en la demostración.

Lema. *[17]*

$$\max_{n \in K} (x_n + y_n) \leq b - 2 + \left\lfloor \frac{m}{b} \right\rfloor$$

donde K es el conjunto de los n tales que $P \leq n \leq P + m - 1$, $m \geq 1$.

Teorema. *[17] (a) Si* $\text{mcd}(a_3 - a_1, a_2 - a_1) = 1$ *entonces*

$$\begin{aligned} f(a_1, a_2, a_3) \ \leq \ & a_1 \left(a_3 - a_2 - 2 + \left\lfloor \frac{a_1}{a_3 - a_1} \right\rfloor\right) \\ & + (a_2 - a_1 - 1)(a_3 - a_1 - 1) + a_1 + a_2 + a_3. \end{aligned}$$

(b) Si $a, j > 2$ son enteros entonces

1. *Si* $a \equiv -1 \mod j$ *y* $a \geq j^2 - 5j + 3$, *entonces*

$$f(a, a + 1, a + j) = \left\lfloor \frac{a + 1}{j} \right\rfloor a + (j - 3)a.$$

2. *Si* $a \equiv -1 \mod j$ *y* $a \geq j^2 - 4j + 2$, *entonces*

$$f(a, a + 1, a + j) = \left\lfloor \frac{a + 1}{j} \right\rfloor (a + j) + (j - 3)a.$$

(c) Sean $0 < a < b$ y m enteros tal que $\text{mcd}(a, b) = 1$, $m \geq 2$ *entonces*

$$f(m, m + a, m + b) \leq m \left(b - 2 + \left\lfloor \frac{m}{b} \right\rfloor\right) + (a - 1)(b - 1).$$

Demostración.

Solamente demostraremos el apartado (c), ya que los otros apartados se obtienen de este.

(c) Sea $P = (a - 1)(b - 1)$, x_n e y_n las soluciones no negativas de $ax + by = n$ con x lo más pequeño posible y $n \geq P$. Sea K el conjunto de n tal que $P \leq n \leq P + m - 1$ con $m \geq 1$.

Definimos $Q = \max_{n \in K} (x_n + y_n)$.

A continuación, definimos $\bar{x}_j$, $\bar{y}_j$ y $\bar{z}_j$ para $j \geq P$ de la siguiente manera:

$$\bar{x}_j = x_i, \quad \bar{y}_j = y_i \text{ para } j \equiv i \mod m, \quad P \leq i \leq P + m - 1,$$
$$\bar{z}_j = Q + \frac{j - P}{m} - \bar{x}_j - \bar{y}_j.$$

Entonces,

$$\begin{aligned} m\bar{z}_j + (m+a)\bar{x}_j + (m+b)\bar{y}_j &= m(\bar{z}_j + \bar{x}_j + \bar{y}_j) + a\bar{x}_j + b\bar{y}_j \\ &= mQ + m\frac{j-P}{m} + a\bar{x}_j + b\bar{y}_j. \end{aligned}$$

Como j tiene la forma

$$P + sm,\ P + sm + 1, \ldots,\ P + sm + m - 1$$

para $s \geq 0$, el lado derecho de la ecuación tiene la forma,

$$mQ + ms + P,\ mQ + ms + P + 1, \ldots,\ mQ + ms + P + m - 1.$$

Por lo tanto, como $j \geq P$ y $s \geq 0$, el lado de la izquierda de la ecuación es mayor o igual que $P + mQ$. Reemplazando Q por la cota superior del lema anterior obtenemos el resultado. □

E.L. Goldberg [18], también estudió $f(a_1, a_2, a_3)$ para algunos casos especiales.

Teorema. *[18] Sean $1 < a < b$ enteros con $\text{mcd}(a, b) = d$ y $\text{mcd}(d, m) = 1$ con $md^2 > b(b - a - 2d)$ y $dm = ax_0 + by_0$ con $0 \leq x_0 < b/d$ y $0 \leq y_0$ Entonces,*

1. $f(m, m+a, m+b) = \left(\frac{a}{d} + x_0 + y_0 + d - 3\right) m + b\left(\frac{a}{d} - 1\right) - a$, *cuando* $dx_0 \geq b - a$,
2. $f(m, m+a, m+b) = \left(\frac{b}{d} + y_0 + d - 3\right) m + b\left(\frac{a}{d} - 1\right) - a(x_0 + 1)$ *en otro caso.*

Este resultado resuelve el problema de Frobenius para primos relativos $1 < a_1 < a_2 < a_3$ si estos números no son muy diferentes, es decir, a_1 es suficientemente grande en comparación con $a_3 - a_1$.

El siguiente resultado lo dio J.S. Byrnes [19]. Su método puede ser aplicado en algunos casos cuando $n = 3$.

Teorema. *[19] Sea $a_1 < a_2 < a_3$, con $a_2 \equiv 1 \mod a_1$. Entonces,*

- *Si $a_3 \leq ja_2$, entonces*

$$f(a_1, a_2, a_3) = a_1a_2 - (a_1 + a_2).$$

- *Si $(j-m)a_2 < a_3 \leq ja_2$, entonces*

$$f(a_1, a_2, a_3) = a_3\left(\frac{a_1 - m}{j}\right) + (m-1)a_2 - a_1.$$

- *Si $a_2\left(\dfrac{j}{a_1 - m + j}\right)(j-m) \leq a_3 < (j-m)a_2$, entonces*

$$f(a_1, a_2, a_3) = a_3\left(\frac{a_1 - m - j}{j}\right) + (j-1)a_2 - a_1.$$

donde j y m son tales que $a_3 \equiv j \mod a_1$ con $0 \leq j < a_1$ y (si $j \neq 0$) $a_1 \equiv m \mod j$ con $1 \leq m \leq j$.

Definición. *Se dice que $a_1, \ldots, a_n$ es una secuencia independiente si ninguno de los a_i con $i = 1, \ldots, n$ puede ser representado por los otros.*

Selmer [20] encontró una cota y a partir de ella una fórmula general cuando a_1, a_2 y a_3 son independientes.

Teorema. *[20] Si a_1, a_2 y a_3 son independientes y coprimos dos a dos, entonces*

$$f(a_1, a_2, a_3) \leq \max\{(s-1)a_2 + (q-1)a_3, (r-1)a_2 + qa_3\} - a_1$$

donde s es determinado por $a_3 \equiv sa_2 \mod a_1$, $1 < s < a_1$ y q y r están determinados por $a_1 = qs + r$ con $0 < r < s$. Además, si $a_2 \geq t(q+1)$ donde $a_3 = sa_2 - ta_1$ con $t > 0$ entonces

$$f(a_1, a_2, a_3) = \max\{(s-1)a_2 + (q-1)a_3, (r-1)a_2 + qa_3\} - a_1.$$

Kan, Stechkin y Sharkov [21] obtuvieron una relación entre $f(a_1, a_2, a_3)$ y $f(s, s+1, s+p)$ siendo p y s números enteros que ellos definieron. Veamos en qué consiste.

Teorema. *[21] Sean $a_1 < a_2 < a_3$ enteros positivos y sea $d = \mathrm{mcd}(a_1, a_2)$. Entonces,*

$$f(a_1, a_2, a_3) = \frac{a_1a_2\left(f(s, s+1, s+p) + 2s + 1\right)}{ds(s+1)} + (d-1)a_3 - (a_1 + a_2)$$

donde $s = \dfrac{a_2}{d}v - 1$, $\quad p = s\left(\dfrac{a_3dv}{a_1} - 1\right)$ y $v \in \mathbb{N}$ verificando la condición $a_2v \equiv d \mod a_1$ con $vd < a_1$.

2.5. Cotas para $n = 3$

En esta sección estudiaremos algunas cotas para $f(a_1, a_2, a_3)$ y veremos cómo algunas de ellas pueden darnos su valor exacto.

Para comenzar veremos cómo Kannan [1] dio un enfoque totalmente distinto al problema de Frobenius, usando el radio de cobertura. Además encontró dos cotas superiores que estaban relacionadas con la cota que obtuvo Selmer en su teorema.

Teorema. *[1] Sean $0 < w_1 < a_3$ y $0 < w_2 < a_3$ los únicos enteros tales que $a_1 w_1 \equiv a_2 \mod a_3$ y $a_2 w_2 \equiv -a_1 \mod a_3$ respectivamente y sean r_1 y r_2 los mayores enteros positivos tales que $-a_3 + r_1 w_1 < 0$ y $a_3 - w_2 r_2 > 0$ respectivamente.*

$$\begin{aligned} \text{(a) } f(a_1, a_2, a_3) \;\leq\; & \max\{a_1(a_3 - r_1 w_1) + a_2(r_1 + 1), a_1 w_1 + a_2 r_1\} \\ & - a_1 - a_2 - a_3. \end{aligned}$$

$$\begin{aligned} \text{(b) } f(a_1, a_2, a_3) \;\leq\; & \max\{a_1 + a_2(a_3 + (1 - r_2)w_2), a_1 r_2 + a_2 w_2\} \\ & - a_1 - a_2 - a_3. \end{aligned}$$

Las cotas proporcionadas en el teorema anterior no tienen que estar cerca la una de la otra, obviamente nos interesa la cota más pequeña. También, puede darse el caso en que una de ellas o las dos, nos proporcionen el valor exacto de $f(a_1, a_2, a_3)$. Veamos esto en algunos ejemplos:

Ejemplo. *Sean $a_1 = 4$, $a_2 = 7$ y $a_3 = 9$. Por el teorema tenemos que:*

$$\begin{aligned} 0 < w_1 < 9 \text{ tal que } 4w_1 \equiv 7 \mod 9 \quad &\Rightarrow \quad w_1 = 4, \\ 0 < w_2 < 9 \text{ tal que } 7w_2 \equiv -4 \mod 9 \quad &\Rightarrow \quad w_2 = 2, \end{aligned}$$

y r_1, r_2 los mayores enteros que cumplan:

$$\begin{aligned} -9 + 4r_1 \;< 0 \quad &\Rightarrow \quad r_1 = 2, \\ 9 - 2r_2 \;> 0 \quad &\Rightarrow \quad r_2 = 4. \end{aligned}$$

Aplicando los dos apartados del teorema obtenemos el mismo resultado:

$$f(4, 7, 9) \leq \max\{25, 30\} - 20 = 10 = f(4, 7, 9).$$

Ejemplo. *Sean $a_1 = 5$, $a_2 = 9$, $a_3 = 13$. Como en el ejemplo anterior tenemos $w_1 = 7$, $w_2 = 11$, $r_1 = 1$ y $r_2 = 1$ que hemos calculado mediante el mismo método. Aplicando el teorema tenemos:*

$$\begin{aligned} &\text{(a) } f(5, 9, 13) \leq \max\{48, 44\} - 27 = 21 = f(5, 9, 13). \\ &\text{(b) } f(5, 9, 13) \leq \max\{122, 104\} - 27 = 95. \end{aligned}$$

M. Beck, R. Diaz y S. Robin [22] usaron otras técnicas para obtener la siguiente cota superior.

Teorema. *[22] Sea* $\text{mcd}(a_1, a_2, a_3) = 1$. *Entonces,*

$$f(a_1, a_2, a_3) \leq a_1 a_2 a_3 \sqrt{\frac{1}{4}\left(\frac{1}{a_1 a_2} + \frac{1}{a_2 a_3} + \frac{1}{a_1 a_3}\right)} - \frac{1}{2}(a_1 - a_2 - a_3).$$

La última cota que daremos, fue gracias a Y. Vitek [23].

Teorema. *[23] Si* $a_1 < a_2 < a_3$ *son independientes (i.e., ninguno de los* a_i *es representable por los otros dos) entonces*

$$f(a_1, a_2, a_3) \leq a_1 \left\lfloor \frac{a_3}{2} - 1 \right\rfloor.$$

2.6. El caso $n = 4$

Si calcular una fórmula para $f(a_1, a_2, a_3)$ resulta difícil, si aumentamos a $n \geq 4$ dicha dificultad aumenta. Para el caso concreto de $n = 4$ tenemos pocos resultados ya que la mayoría de los mismos entrarían en el estudio del caso general.

Un ejemplo de ello, es el estudio de Dulmage y Mendelson [24]. Mediante su método, para el cual utilizaron la teoría de grafos, consiguieron obtener el siguiente resultado particular para calcular $f(a_1, a_2, a_3, a_4)$.

Teorema. *[24] Sea a un entero no negativo. Entonces,*

1. $f(a, a+1, a+2, a+4) = (a+1)\left\lfloor \frac{a}{4} \right\rfloor + \left\lfloor \frac{a+1}{4} \right\rfloor + 2\left\lfloor \frac{a+2}{4} \right\rfloor - 1.$
2. $f(a, a+1, a+2, a+5) = a\left\lfloor \frac{a+1}{5} \right\rfloor + \left\lfloor \frac{a}{5} \right\rfloor + \left\lfloor \frac{a+1}{5} \right\rfloor + \left\lfloor \frac{a+2}{5} \right\rfloor + 2\left\lfloor \frac{a+3}{5} \right\rfloor - 1.$
3. $f(a, a+1, a+2, a+6) = a\left\lfloor \frac{a}{6} \right\rfloor + 2\left\lfloor \frac{a}{6} \right\rfloor + 2\left\lfloor \frac{a+1}{6} \right\rfloor + 5\left\lfloor \frac{a+2}{6} \right\rfloor + \left\lfloor \frac{a+3}{6} \right\rfloor + \left\lfloor \frac{a+4}{6} \right\rfloor + \left\lfloor \frac{a+5}{6} \right\rfloor - 1.$

Vitek [23] que, como ya vimos dio una cota cuando $n = 3$, también proporcionó una cota en este caso:

$$f(a_1, a_2, a_3, a_4) \leq \left\lfloor \frac{(a_4 - 2)(a_3 - 3)}{3} \right\rfloor - 1.$$

Para terminar, daremos la fórmula propuesta por I. D. Kan [25], que al igual que antes, fue un resultado particular del estudio del caso general.

Teorema. *[25] Sea* $\{\alpha\}$ *la parte fraccionaria de* $\alpha \in \mathbb{R}$*, que es* $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$*. Sean* a *y* b *dos enteros positivos tal que* $a > b \geq 2$*.*

Si $2a + 3 \geq (2b - 3)\lfloor a/b \rfloor$ *entonces,*

$$f(a, a+1, 2a+3, a+b) = (a+b)\left\lfloor \frac{a-1}{b} \right\rfloor + ab - 2a - 1 - \\ - \min\left\{ -b + (ab+b)\left\{ -\frac{a}{b} \right\} + a\left\lfloor \frac{b\{(a-1)/b\}}{3} \right\rfloor, a\left\lfloor \frac{b+2}{3} \right\rfloor \right\}.$$

Capítulo 3

El caso general

En este capítulo, presentaremos algunos algoritmos para resolver el problema de Frobenius cuando $n \geq 4$.

3.1. El método de Scarf y Shallcross

H.E. Scarf y D.F. Shallcross [26] relacionaron el problema de Frobenius con el área de conjuntos cerrados maximales que no contienen puntos del retículo.

Definición. *Sea $\{x \ : \ Ax \leq b\}$ un convexo donde A es una matriz. Diremos que es un convexo maximal libre de puntos del retículo, si no tiene puntos del retículo en su interior y, si quitamos alguna de las desigualdades, contiene al menos un punto del retículo en su interior.*

Scarf y Shallcross demostraron que si pueden maximizar una función lineal sobre el conjunto de b's que producen un convexo maximal libres de puntos del retículo para la matriz A de dimensión $n \times (n-1)$, entonces pueden resolver el problema de Frobenius.

Algoritmo de Scarf y Shallcross:

Sea $a = (a_1, \ldots, a_n)$ y sea A una matriz $n \times (n-1)$, donde sus columnas generan un retículo con dimensión $(n-1)$, h tal que $a \cdot h = 0$ (el conjunto de soluciones h constituyen un hiperplano).

Observemos que en este caso los convexos $\{x \ : \ Ax \leq b\}$ serán símplices no vacíos si $a \cdot b \geq 0$.

Entonces si b es entero y $\{x \ : \ Ax \leq b\}$ no contiene puntos del retículo,

$$f(a_1, \ldots, a_n) = \max \{a \cdot b\},$$

Veamos la exactitud del método:

Observemos que si b es un vector entero tal que $\{x \ : \ Ax \leq b\}$ no contiene puntos del retículo, entonces $f = a \cdot b$ no puede ser escrito como $a \cdot h$ con h un vector no negativo.

Si se cumpliera lo anterior llegaríamos a una contradicción, porque $0 = a \cdot (b - h)$ así que $b - h$ es un retículo $(n-1)-$dimensional generado por las columnas de A. Luego, $b - h = A\alpha$ para algún entero α y de esta forma, el conjunto $\{x \ : \ Ax \leq b\}$ contiene un punto del retículo.

Por otro lado, si b es un vector entero tal que $\{x \ : \ Ax \leq b\}$ contiene un punto del retículo α, entonces $f = a \cdot b = a \cdot (b - A\alpha)$ con $b - A\alpha$ un vector entero no negativo.

Finalmente, ya que $\text{mcd}(a_1, \ldots, a_n) = 1$, todo entero f puede ser escrito como $a \cdot b$ para algún b entero. Entonces, $f(a_1, \ldots, a_n)$ es el valor máximo de $a \cdot b$ para aquellos enteros b tal que $\{x \ : \ Ax \leq b\}$ está libre de puntos del retículo.

Ejemplo. *Calcularemos $f(13, 23)$ con el método anterior.*

Observemos que $\text{mcd}(13, 23) = 1$*, el conjunto de vectores $h = (h_1, h_2)$ que satisfacen $(13, 23) \cdot (h_1, h_2) = 0$ dado por $(\pm 23r, \mp 13r)$ donde $r = 0, 1, 2, \ldots$. El retículo $1-$dimensional generado por h (figura 3.1).*

Una columna de la matriz $A = \begin{pmatrix} -23 \\ 13 \end{pmatrix}$ *que genera los puntos del retículo h.*

Queremos encontrar los enteros $b = (b_1, b_2)$ tales que

$$\begin{pmatrix} -23 \\ 13 \end{pmatrix} x \leq \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

no esta en los puntos del retículo y $(13, 23) \cdot (b_1, b_2)$ es maximal.

Tenemos que $\dfrac{-b_1}{23} \leq x \leq \dfrac{b_2}{13}$ *con $0 > b_1 > -23$ y $0 < b_2 < 13$ puntos que no pertenecen al retículo.*

Finalmente, con las condiciones anteriores, $(b_1, b_2) = (-1, 12)$ y

$$f(13, 23) = (13, 23) \cdot (-1, 12) = 263.$$

Scarf y Shallcross usaron el algoritmo anterior para calcular $f(a_1, a_2, a_3)$ en tiempo lineal, pero los a_i tenían que estar próximos. Para ello usaban una transformación particular de la matriz A, que identificaba los convexos maximales libres de puntos del retículo que tenía asociado.

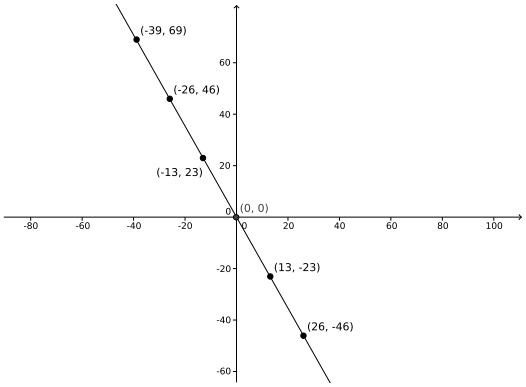


Figura 3.1: Retículo generado por el conjunto de soluciones de $(13, 23) \cdot (h_1, h_2) = 0$

3.2. Método de Heap y Lynn

Definición. *Una matriz $B = (b_{ij})$, $1 \leq i, j \leq m$ se llama no negativa (resp. positiva) si $b_{ij} \geq 0$ (resp. si $b_{ij} > 0$). A la matriz positiva B la denotaremos por $B > 0$.*

Definición. *Diremos que B una matriz $(n \times n)$ es reducible si existe una matriz $(n \times n)$ de permutación P tal que*

$$PBP^T = \begin{bmatrix} B_{1,1} & B_{1,2} \\ 0 & B_{2,2} \end{bmatrix}$$

donde $B_{1,1}$ es una submatriz $(r \times r)$ y $B_{2,2}$ es una submatriz $(n-r) \times (n-r)$. Si no existe tal matriz, entonces diremos que B es irreducible.

Definición. *Sea B una matriz no negativa e irreducible, diremos que es primitiva si $B^p > 0$ para algún entero $p \geq 1$.*

Definición. *Se llamara índice de primacidad de B y lo notaremos $\gamma(B)$, al menor entero tal que $B^{\gamma(B)} > 0$.*

El método de Heap y Lynn [27] se basa en técnicas de teoría de grafos para demostrar que el problema de Frobenius es equivalente a calcular el índice de primacidad de una matriz B de orden $a_n + a_{n-1} + 1$.

Definición. *Sea $B = (b_{ij})$ una matriz real $(m \times m)$. Definimos el grafo dirigido $G(B)$ de B, como el grafo con vértices $\{1, \ldots, m\}$ y aristas dirigidas de i a j si y solo si $b_{ij} \neq 0$.*

Definición. *Llamaremos circuito a un camino el cual el primer y último vértice son el mismo. Diremos que un circuito es elemental si solo aparece cada vértice una vez.*

Heap y Lynn, se dieron cuenta de que había una fuerte conexión entre $G(B)$ y $\gamma(B)$ que usaron para establecer los siguientes lemas.

Lema. *[27] Si B es primitiva entonces $\gamma(B)$ es el menor entero tal que para todo $m \geq \gamma(B)$ hay un camino de longitud m conectando dos vértices arbitrarios (no necesariamente distintos) de $G(B)$.*

Lema. *[27] Sea B una matriz primitiva y sean $0 < a_1 < \ldots < a_n$ las distintas longitudes de todos los circuitos elementales de $G(B)$. Entonces, $\mathrm{mcd}(a_1, \ldots, a_n) = 1$ y la longitud L, cualquier circuito de $G(B)$ puede ser expresado de la forma*

$$L = \sum_{i=1}^{n} x_i a_i \text{ con } x_i \geq 0 \text{ para todo } i.$$

Lema. *[27] Sea B una matriz primitiva $a_1 < \ldots < a_n$ las distintas longitudes de los circuitos elementales de $G(B)$. Entonces,*

$$f(a_1, \ldots, a_n) \leq \gamma(B) - 1.$$

Demostración.

Como los elementos diagonales de $B^{\gamma(B)+m}$ son positivos para todo $m \geq 0$. Por el primer lema, sabemos que hay circuitos en $G(B)$ de longitud $\gamma(B)+m$. Usando el lema anterior y por la definición de $f(a_1, \ldots, a_n)$ obtenemos:

$$f(a_1, \ldots, a_n) \leq \gamma(B) - 1.$$

□

Definición. *Dados enteros $1 \leq a_1 < \ldots < a_n$, se define el grafo de Frobenius, notado por $G(B) = G(a_1, \ldots, a_n)$, obtenido de la matriz $B = b_{ij}$, $1 \leq i, j \leq s = a_n + a_{n-1} - 1$, donde*

$$b_{ij} = \begin{cases} 1 \text{ si } j = i+1 \text{ con } i = 1, \ldots, s-1 \text{ y } i \neq a_{n-1}, \\ 1 \text{ si } j = 1 \text{ con } i = s \text{ ó } a_t,\ t = 1, \ldots, n-1, \\ 1 \text{ si } i = 1 \text{ y } j = a_{n-1} + 1, \\ 0 \text{ en otro caso.} \end{cases}$$

Nota. *Los circuito elementales de $G(a_1, \ldots, a_n)$ tienen longitudes $a_1, \ldots, a_n$.*

Usando la misma técnica del lema anterior y analizando el grafo de Frobenius, Heap y Lynn obtuvieron el siguiente resultado:

Teorema. *[27] Sea B la matriz definida anteriormente. Entonces,*

$$f(a_1, \ldots, a_n) = \gamma(B) - 2a_n + 1.$$

Usando el teorema anterior, se obtiene un método para encontrar el número de Frobenius. La complejidad del mismo, depende de la eficiencia al calcular el índice de primacidad de la matriz B.

Ejemplo. *Sea $a_1 = 3$ y $a_2 = 7$, calcularemos $f(3, 7)$ utilizando el resultado anterior.*

En primer lugar calculemos $\gamma(B)$:

$$B = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Elevando la matriz obtenemos su índice de primacidad:

$$B^{23} = \begin{pmatrix} 10 & 6 & 2 & 6 & 2 & 6 & 5 & 1 & 3 \\ 2 & 6 & 5 & 6 & 5 & 1 & 3 & 4 & 1 \\ 6 & 2 & 6 & 2 & 6 & 5 & 1 & 3 & 4 \\ 3 & 4 & 1 & 4 & 1 & 1 & 3 & 1 & 0 \\ 1 & 3 & 4 & 3 & 4 & 1 & 1 & 3 & 1 \\ 5 & 1 & 3 & 1 & 3 & 4 & 1 & 1 & 3 \\ 6 & 5 & 1 & 5 & 1 & 3 & 4 & 1 & 1 \\ 2 & 6 & 5 & 6 & 5 & 1 & 3 & 4 & 1 \\ 6 & 2 & 6 & 2 & 6 & 5 & 1 & 3 & 4 \end{pmatrix} \quad B^{24} = \begin{pmatrix} 5 & 10 & 6 & 10 & 6 & 2 & 6 & 5 & 1 \\ 6 & 2 & 6 & 2 & 6 & 5 & 1 & 3 & 4 \\ 10 & 6 & 2 & 6 & 2 & 6 & 5 & 1 & 3 \\ 1 & 3 & 4 & 3 & 4 & 1 & 1 & 3 & 1 \\ 5 & 1 & 3 & 1 & 3 & 4 & 1 & 1 & 3 \\ 6 & 5 & 1 & 5 & 1 & 3 & 4 & 1 & 1 \\ 2 & 6 & 5 & 6 & 5 & 1 & 3 & 4 & 1 \\ 6 & 2 & 6 & 2 & 6 & 5 & 1 & 3 & 4 \\ 10 & 6 & 2 & 6 & 2 & 6 & 5 & 1 & 3 \end{pmatrix}$$

Luego $\gamma(B) = 24$ y aplicando el teorema $f(3, 7) = 24 - (2)7 + 1 = 11$.

Nota. *$G(B^k)$ es el grafo dirigido considerando todos los caminos de $G(B)$ de longitud $k > 1$. Así, $\gamma(B)$ es el menor entero tal que hay una arista dirigida por cada par de vértices en $G(B^{\gamma(B)})$. Luego, $G(B^{\gamma(B)})$ es el digrafo donde todo par de vértices que se unen por dos aristas (una en cada dirección).*

Para reducir el tiempo de cálculo en su método, Heap y Lynn [28] definieron otro grafo dirigido llamado grafo mínimo de Frobenius.

Definición. *Sean $1 \leq a_1 < \ldots < a_n$ enteros,se define el grafo mínimo de Frobenius, notado por $G(\bar{B})$, obtenido a partir de la matriz $\bar{B} = (\bar{b}_{ij})$ (la cual es de orden a_n) definida:*

$$\bar{b}_{ij} = \begin{cases} 1 \text{ si } j = i+1 \text{ con } i = 1, \ldots, a_n - 1, \\ 1 \text{ si } i - j = a_s - 1 \text{ para algún } 1 \leq s \leq n, \\ 0 \text{ en otro caso.} \end{cases}$$

Ejemplo. *Sea $a_1 = 3$, $a_2 = 5$ y $a_3 = 7$. Entonces, la matriz $\bar{B}$ tiene la forma:*

$$\bar{B} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Teorema. *(THL) [28] Sea $\bar{B}$ la matriz definida anteriormente. Entonces,*

$$f(a_1, \ldots, a_n) = \gamma(\bar{B}) - a_n.$$

Para la demostración del teorema nos basaremos en el siguiente resultado.

Lema. *[28]*

(a) Existe un único camino del vértice i al j, $i < j$ en $G(\bar{B})$.

(b) Hay sólo un circuito elemental de longitud a_i en $G(\bar{B})$.

(c) Cada vértice en $G(\bar{B})$ se encuentra en un circuito elemental de longitud a_i con $i = 1, \ldots, n$.

Corolario. *[28] $\bar{B}$ es primitiva.*

Demostración.

Como $G(\bar{B})$ está fuertemente conectada (hay un circuito elemental de longitud a_i), entonces $\bar{B}$ es irreducible. □

Demostración. (THL)

En primer lugar demostraremos que

$$f(a_1, \ldots, a_n) + a_n \leq \gamma(\bar{B}).$$

Notar que cualquier camino del vértice 1 al vértice a_n debe consistir en un camino elemental de longitud $a_n - 1$, aplicando el apartado (a) del lema anterior, la suma de un número de circuitos, es necesariamente de la forma:

$$L = a_n - 1 + \sum_{i=1}^{n} x_i a_i \text{ donde } x_i \geq 0.$$

Por lo tanto, no existe un camino del vértice 1 al vértice a_n de longitud $f(a_1, \ldots, a_n) + a_n - 1$. Obtenemos la desigualdad por un lema anterior de esta sección.

Ahora, demostraremos

$$f(a_1, \ldots, a_n) + a_n \geq \gamma(\bar{B}).$$

Para ello, nos damos cuenta que cualesquiera dos vértices i y j de $G(\bar{B})$ pueden ser conectados por un camino de longitud $a_n - 1$ como máximo, ya que existe un circuito elemental de longitud a_n el cual contiene a todos los vértices del grafo. Como el vértice i se encuentra en los circuitos elementales de longitudes a_s, $1 \leq s \leq n$, hay un camino que conecta el vértice i con el vértice j de longitud

$$a_n - 1 - \delta + \sum_{i=1}^{n} x_i a_i$$

para todo $a_i \geq 0$ y algún $\delta \geq 0$. Dado $\mu \geq 0$ podemos elegir los $\{a_i\}$ tales que

$$\sum_{i=1}^{n} x_i a_i = f(a_1, \ldots, a_n) + 1 + \delta + \mu,$$

por lo tanto, existe un camino que conecta un vértice aleatorio i con otro vértice aleatorio j de longitud

$$a_n + f(a_1, \ldots, a_n) + \mu$$

para todo $\mu \geq 0$. Finalmente, obtenemos la desigualdad del primer lema de la sección tomando $\mu = 0$. □

3.3. Algoritmo de Greenberg

H. Greenberg [29] uso ideas de programación matemática para obtener un algoritmo con el cual calcular $f(a_1, \ldots, a_n)$. Este algoritmo esta basado en el siguiente resultado.

Teorema. *[29] Sea $a_1, \ldots, a_n$ y L enteros positivos y sea*

$$E(L) = \min\left\{\sum_{j=1}^{n} x_j a_j \mid \sum_{j=2}^{n} x_j a_j \equiv L \mod a_1,\ x_j \geq 0\right\}.$$

Entonces, existen enteros $x_j \geq 0$ tal que $\sum_{j=1}^{n} x_j a_j = L$ si y sólo si $L \geq E(L)$. Además, no existen enteros no negativos x_i tal que

$$\sum_{j=1}^{n} x_j a_j = E(L) - s a_1$$

para cada $s \in \{1, 2, \ldots, (E(L) - L)/a_1\}$ y cualquier $L \in \{1, \ldots, a_1 - 1\}$ y esta es la única ecuación de la forma $\sum_{j=1}^{n} x_j a_j = L$ sin soluciones con x_i enteros no negativos, para cada $L \in \{1, \ldots, a_1 - 1\}$.

Nota. *$E(L) = E(L')$ si L y L' son de la misma clase módulo a_1. El cálculo de $E(L)$ sólo tenemos que hacerlo para $L = 1, 2, \ldots, a_1 - 1$.*

Observemos que $E(L)$ y L son de la misma clase módulo a_1. Además, si $E(L)$ es conocido, con solución $x_1 = 0$, $x_j = x'_j$ para $j \geq 2$ y $L \geq E(L)$, entonces una solución de $L = \sum_{j=1}^{n} x_j a_j$ es:

$$x_1 = \frac{E(L) - L}{a_1}$$

con $x_j = x'_j$ para $j \geq 2$.

Con el teorema anterior, completamos la caracterización de todas las soluciones y no soluciones de $L = \sum_{j=1}^{n} x_j a_j$ obtenida a partir de la función $E(L)$.

Corolario. *[29]*

$$f(a_1, \ldots, a_n) = max\,\{E(L) \mid L = 1, \ldots, a_1 - 1\} - a_1.$$

Ejemplo. *Calcularemos $f(5, 9, 13)$ usando el algoritmo de Greenberg.*

En primer lugar calculamos,

$$E(j) = \min\{5x_1 + 9x_2 + 13x_3 \mid 9x_2 + 13x_3 \equiv j \mod 5, x_1, x_2, x_3 \geq 0\}$$

con $j = 1, \ldots, 4$. *Luego,*

$$E(1) = 26, \ \textit{con } x_1 = x_2 = 0, x_3 = 2.$$
$$E(2) = 22, \ \textit{con } x_1 = 0, x_2 = x_3 = 1.$$
$$E(3) = 13, \ \textit{con } x_1 = x_2 = 0, x_3 = 1.$$
$$E(4) = 9, \quad \textit{con } x_1 = x_3 = 0, x_2 = 1.$$

Entonces, $f(5, 9, 13) = \max\{26, 22, 13, 9\} - 5 = 21$.

3.4. Algoritmo de Nijenhuis

A. Nijenhuis [30] dio un algoritmo para calcular $f(a_1, \ldots, a_n)$. Para ello utilizó un grafo ponderado con aristas dirigidas, y construyó un camino de peso mínimo de un vértice a todos los demás.

Algoritmo de Nijenhuis:
Sea D un grafo dirigido, con vértices $\{v_0, \ldots, v_{a_1-1}\}$ y para cada $0 \leq p \leq a_1 - 1$ existe una arista dirigida del vértice v_p al $v_{p'}$ donde $p' \equiv p + a_i \mod a_1$ para todo $1 \leq i \leq n$, y el peso de la arista es a_i.

Sea w_p el camino de peso mínimo que va desde el vértice v_0 al v_p (el peso de un camino dirigido es la suma de todos los pesos de las aristas implicadas). Entonces,

$$f(a_1, \ldots, a_n) = \max_{1 \leq p \leq a_1 - 1} \{w_p\} - a_1.$$

Observemos que w_p es el elemento más pequeño del conjunto de enteros representables como combinación lineal con coeficientes enteros no negativos de $a_1, \ldots, a_n$ congruentes con p módulo a_1. Este algoritmo tiene una complejidad de $O(na_1 \log a_1)$ asumiendo $a_1 < a_2 < \ldots < a_n$.

Ejemplo. *Calcularemos* $f(5, 9, 13)$ *usando el algoritmo anterior.*
Construimos el grafo de vértices $\{v_0, \ldots, v_4\}$. *Figura 3.1.*

A continuación, calculamos los w_i *que serían el camino con menor peso desde* v_0 *a* v_i *con* $i = 0, 1, 2, 3, 4$. *Luego,* $w_0 = 5$, $w_1 = 26$, $w_2 = 22$, $w_3 = 13$ *y* $w_4 = 9$.

Entonces, $f(5, 9, 13) = \max\{5, 26, 22, 13, 9\} - 5 = 21$.

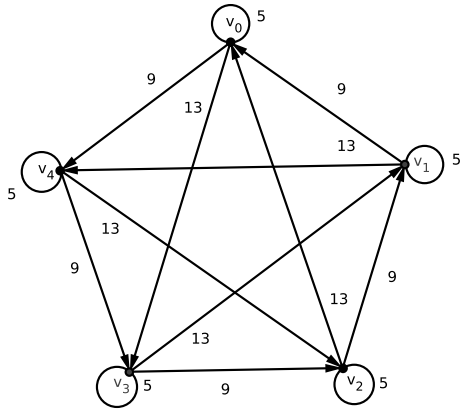


Figura 3.2: Grafo dirigido de Nijenhuis cuando $a_1 = 5, a_2 = 9, a_3 = 13$

3.5. Algoritmo de Wilf

H.S. Wilf [31] obtuvo un algoritmo para calcular $f(a_1, \ldots, a_n)$ con una complejidad del orden de $O(na_n^2)$.

Algoritmo de Wilf:
Formamos un círculo con a_n puntos, etiquetados por $l_0, l_1, \ldots, l_{a_n-1}$ estos puntos pueden estar encendidos o apagados (al principio el punto l_0 está encendido y el resto apagados).

Comenzamos en l_0, y avanzamos en sentido horario. Nos iremos encontrando con cada luz que la encenderemos si alguna de las n luces que están situadas a distancia $a_1, \ldots, a_n$ en sentido antihorario está encendida, si no la dejamos apagada. Si la luz en la que no encontramos ya está encendida, pasamos a la siguiente. El proceso se detiene tan pronto como tengamos a_1 luces consecutivas encendidas.

Sea $s(l_{a_i})$ el número de veces que la luz l_{a_i} es visitada durante el proceso y sea l_r la última luz apagada visitada antes de que termine el proceso. Entonces,

$$f(a_1, \ldots, a_n) = r + (s(l_r) - 1)a_n.$$

Ejemplo. *Calcularemos* $f(5, 9, 13)$ *utilizando el método de Wilf. En la figura 3.3 representamos el proceso donde la flecha va en sentido de las agujas del*

reloj y los círculos negros(resp. blancos) representan las luces apagadas(resp. encendidas).

En nuestro proceso vemos que l_8 es la última luz visitada antes de que termine el proceso, pasando dos veces por ella, entonces

$$f(5, 9, 13) = 8 + (s(l_8) - 1)13 = 8 + (2 - 1)13 = 21.$$

3.6. El enfoque de Kannan

R. Kannan [32] proporcionó un algoritmo para resolver el problema de Frobenius en tiempo polinomial para cualquier n fijado. Kannan hizo esto probando, en primer lugar, una relación exacta entre el problema de Frobenius y un concepto geométrico llamado radio de cobertura.

Definición. *Sea P un conjunto convexo, cerrado y acotado de volumen no nulo en $\mathbb{R}^n$ y L un retículo de dimensión n perteneciente a $\mathbb{R}^n$. El menor $t \in \mathbb{R}^+$ para que $tP + L$ sea igual $\mathbb{R}^n$ es llamado radio de cobertura de P con respecto a L, denotado $\mu(P, L)$.*

Nota. *El radio de cobertura de un politopo P con respecto al retículo L es la cantidad más pequeña t, con la cual podemos ampliar P y poner una copia de P en cada punto del retículo de tal manera que cubra todo el espacio.*

Teorema. *[32] Sean*

$$L = \left\{ (x_1, \ldots, x_{n-1}) \mid x_i \in \mathbb{Z} \ y \ \sum_{i=1}^{n-1} a_i x_i \equiv 0 \mod a_n \right\}$$

$$S = \left\{ (x_1, \ldots, x_{n-1}) \mid x_i \geq 0, x_i \in \mathbb{R} \ y \ \sum_{i=1}^{n-1} a_i x_i \leq 1 \right\}.$$

Entonces,

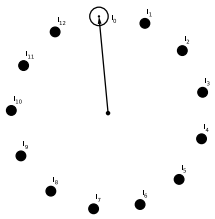
$$\mu(S, L) = f(a_1, \ldots, a_n) + \sum_{i=1}^{n} a_i,$$

donde $\mu(S, L)$ es el radio de cobertura de S con respecto a L.

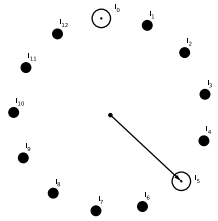
Demostración.

En primer lugar, demostraremos que

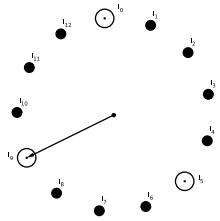
$$\mu(S, L) \leq f(a_1, \ldots, a_n) + \sum_{i=1}^{n} a_i.$$



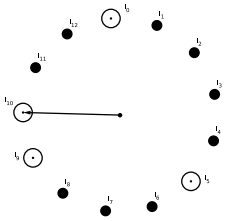
(a) Comenzamos en sentido de las agujas del reloj.



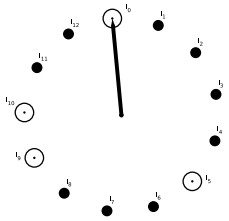
(b) La encendemos, ya que contando 5 hacia atrás, esta encendida.



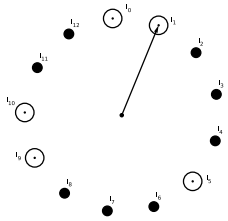
(c) La encendemos,ya que l_0 esta encendida, 9 atrás.



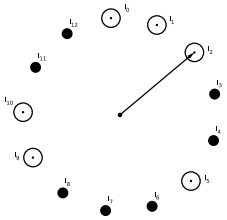
(d) l_5 encendida, 5 atrás.



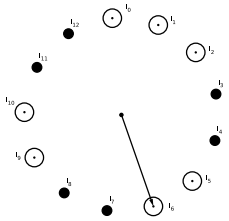
(e) Ya hemos dado una vuelta, a partir de aquí $s(l_r) = 2$.



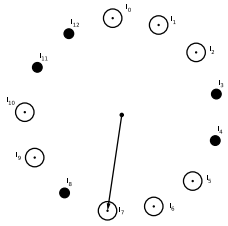
(f) l_9 encendida, 5 atrás.



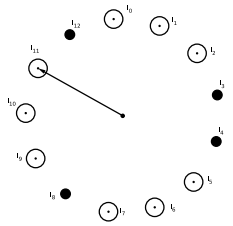
(g) l_{10} encendida, 5 atrás.



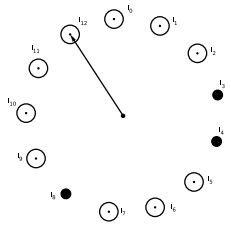
(h) l_1 encendida, 5 atrás.



(i) l_2 encendida, 5 atrás.



(j) l_6 encendida, 5 atrás.



(k) l_7 encendida, 5 atrás, el proceso termina ya que tenemos $a_1 = 5$ luces encendidas consecutivamente.

Figura 3.3: Método de Wilf.

Supongamos que $y \in \mathbb{Z}^{n-1}$ y $\sum_{i=1}^{n-1} a_i y_i \equiv l \mod a_n$. Sea t_l el menor entero positivo congruente con l módulo a_n, que es representable como combinación lineal con coeficientes enteros no negativos de $a_1, \ldots, a_{n-1}$. Luego, existen enteros $x_1, \ldots, x_n \geq 0$ tales que

$$\sum_{i=1}^{n-1} a_i x_i = t_l = l + a_n x_n, \text{ con } x' = (x_1, \ldots, x_{n-1}),$$

tenemos que $(y - x') \in L$ y $(y - x') + t_l S$ está contenido en $y - x' + x' = y$. Como esto es cierto para cualquier $y \in \mathbb{Z}^{n-1}$ y $t_l \leq f(a_1, \ldots, a_n) + a_n$ entonces

$$\mathbb{Z}^{n-1} \subseteq (f(a_1, \ldots, a_n) + a_n)S + L,$$

y claramente

$$\mathbb{R}^{n-1} \subseteq \mathbb{Z}^{n-1} + (a_1 + \cdots + a_n)S.$$

Observemos que para $z \in \mathbb{R}^{n-1}$, tenemos $\lfloor z \rfloor = (\lfloor z_1 \rfloor, \ldots, \lfloor z_{n-1} \rfloor) \in \mathbb{Z}^{n-1}$ y $(z - \lfloor z \rfloor) \in (a_1 + \cdots + a_{n-1})S$. Por lo tanto,

$$\mathbb{R}^{n-1} \subseteq \mathbb{Z}^{n-1} + (a_1 + \cdots + a_{n-1})S \subseteq (f(a_1, \ldots, a_n) + a_1 + \cdots + a_{n-1})S + L.$$

A continuación, demostraremos que $\mu(S, L) \geq f(a_1, \ldots, a_n) + \sum_{i=1}^{n} a_i$.

Veamos por reducción al absurdo que $f(a_1, \ldots, a_n) + a_n$ es el menor real positivo t tal que $tS + L$ está contenido en $\mathbb{Z}^{n-1}$.

Suponemos que no es así. Entonces para algún $t' < f(a_1, \ldots, a_n) + a_n$, $t'S + L$ esta contenido en $\mathbb{Z}^{n-1}$. Para cualquier $l \in \{1, \ldots a_n - 1\}$ escogemos $y \in \mathbb{Z}^{n-1}$ tal que $\sum_{i=1}^{n-1} a_i y_i \equiv l \mod a_n$. Por lo tanto, y está en $t'S + x$ para algún $x \in L$, ya que $(y - x)$ está en $t'S$. Pero $\sum_{i=1}^{n-1} a_i(y_i - x_i) \equiv l \mod a_n$ y $y_i - x_i \geq 0$ para todo i lo que implica que $t_l \leq t'$. Ya que es cierto para cualquier l entonces, por un lema anterior, tenemos que $f(a_1, \ldots, a_n) \leq t' - a_n$ pero $t' - a_n < f(a_1, \ldots, a_n)$ llegando a una contradicción. De este modo,

$$f(a_1, \ldots, a_n) + a_n = \min\left\{t \mid t > 0, \text{ real y } \mathbb{Z}^{n-1} \subseteq tS + L\right\}.$$

Para la ecuación anterior, veamos que existe $y \in \mathbb{Z}^{n-1}$ tal que para cualquier $x \in L$ con $y_i - x_i \geq 0$ para todo i tenemos que

$$\sum_{i=1}^{n-1} a_i(y_i - x_i) \geq f(a_1, \ldots, a_n) + a_n.$$

Sea $\epsilon \in \mathbb{R}$ con $0 < \epsilon < 1$ y consideramos el punto $p = (p_1, \ldots, p_{n-1})$ definido por $p_i = y_i + (1 - \epsilon)$ para todo i. Supongamos que q es cualquier punto de L tal que $p_i \geq q_i$ para todo i. Entonces los q_i son todos enteros, ya que deberíamos tener $q_i \leq y_i$ para todo i. Por lo tanto,

$$\sum_{i=1}^{n-1} a_i(p_i - q_i) = (1-\epsilon)\sum_{i=1}^{n-1} a_i + \sum_{i=1}^{n-1} a_i(y_i - q_i) \geq (1-\epsilon)\sum_{i=1}^{n-1} a_i + f(a_1, \ldots, a_n) + a_n.$$

Dado que este argumento es válido para cualquier $\epsilon \in (0, 1)$, tenemos $\mu \geq f(a_1, \ldots, a_n) + \sum_{i=1}^{n-1} a_i$. □

Kannan desarrolló un algoritmo en tiempo polinomial para encontrar el radio de cobertura de cualquier politopo, fijando la dimensión. Con el teorema anterior vemos que encuentra un algoritmo en tiempo polinomial para calcular $f(a_1, \ldots, a_n)$ para cualquier n fijado. Desafortunadamente, el algoritmo de Kannan es doblemente exponencial en n y no es muy usado en la práctica.

Investigando la relación de Kannan encontramos una fórmula para el mínimo y máximo de $\mu(S, L)$. Explicamos este enfoque, ya que puede llevar a una demostración más constructiva del teorema anterior, que el procedimiento para calcular $f(a_1, \ldots, a_n)$.

Definición. *Escribimos $\mu(x) = \mu S(x)$ para denotar una copia $\mu-$dilatada de S colocada en el punto $x = (x_1, \ldots, x_{n-1}) \in L$.*

Definición. *Decimos que $\mu(x)$ absorbe el punto x' si x' se encuentra en $\mu(x)$ donde $x_i < x'_i$ para todo i. En otras palabras, el punto x' es absorbido por $\mu(x)$ si x' se encuentra en el interior o en una de las caras del simplex $\mu(x)$.*

Proposición. *[1] El espacio $(n-1)-$dimensional es cubierto por una copia $\mu-$dilatada de S colocada en cada punto de L si y sólo si cada punto $x \in \mathbb{Z}^{n-1}$ es absorbido por $\mu(x')$ para algún $x' \in L$ con $x'_i < x_i$, $1 \leq i \leq n-1$.*

Demostración.

$\boxed{\Longrightarrow}$

Asumimos que $\mathbb{R}^{n-1}$ es cubierto por una copia $\mu-$dilatada de S y suponemos que hay un punto $x \in \mathbb{Z}^{n-1}$, x no es absorbido por ninguna $\mu(x')$ con $x'_i < x_i$ para $1 \leq i \leq n-1$. Entonces, podemos encontrar $0 < \epsilon < 1$ tal que $(x_1 - \epsilon, \ldots, x_n - \epsilon)$ no esta cubierto por ninguna de las copias $\mu-$dilatadas de S lo cual es una contradicción ya que el espacio esta cubierto.

$\boxed{\Longleftarrow}$

En sentido contrario, sea $x \in \mathbb{R}^{n-1}$. Debemos demostrar que x es absorbido por $\mu(x')$ para algún $x' \in L$ con $x'_i < x_i$, $1 \leq i \leq n-1$. Esto es cierto si $x \in \mathbb{Z}^{n-1}$ por hipótesis, ya que asumimos que $x_k \notin \mathbb{Z}$ para algún $1 \leq k \leq n-1$. Sean x'_i los enteros más pequeños tales que $x_i \leq x'_i$ para cada $i = 1, \ldots, n-1$. Ya que $x' \in \mathbb{Z}^{n-1}$ entonces es absorbido por algún $\mu(\bar{x})$ con $\bar{x}_i < x'_i$, para $1 \leq i \leq n-1$. Pero, por construcción de x' y la definición de absorción tenemos que $\bar{x}_i < x_i$. Luego, x es también absorbido por $\mu(\bar{x})$.

□

Corolario. *[1] Sea μ^*_x el menor entero positivo tal que el punto $x \in \mathbb{Z}^{n-1}$ es absorbido por $\mu^*_x(x')$ para algún $x' \in L$ con $x'_i < x_i$, $1 \leq i \leq n-1$. Entonces,*

$$\mu(S, L) = \max_{x \in \mathbb{Z}^{n-1}} \{\mu^*_x\}.$$

Ejemplo. *Veamos que podemos deducir la formula de Sylvester usando el resultado anterior. Sean a y b enteros positivos tales que $\mathrm{mcd}(a, b) = 1$. Entonces $L = \{rb \mid r \in \mathbb{Z}_{\geq 0}\}$ y S el segmento $[0, 1/a]$. Claramente el menor entero t tal que tS cubre todo el intervalo $[0, b]$ es ab. Luego,*

$$F(a, b) = \mu(S, L) - a - b = ab - a - b.$$

Ejemplo. *Calcularemos $f(5, 9, 13)$ usando los resultados de Kannan. Representamos en retículo L y el conjunto S en la figura 3.4. Ya conocemos que $f(5, 9, 13) = 21$, por tanto $\mu(L, S) = 48$. En la figura 3.5 vemos como $(48)S$ cubre todo el plano mientras $(47)S$ no, deja pequeños triángulos sin cubrir.*

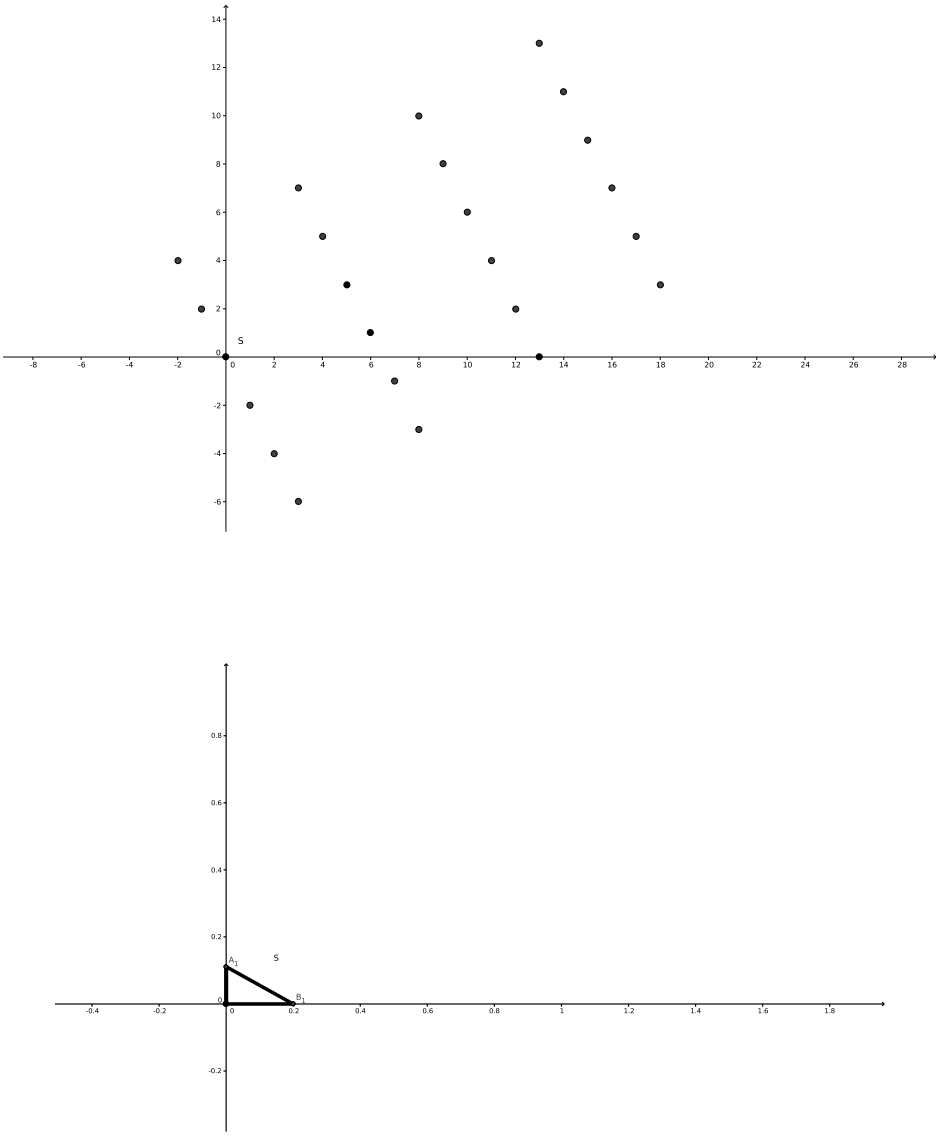
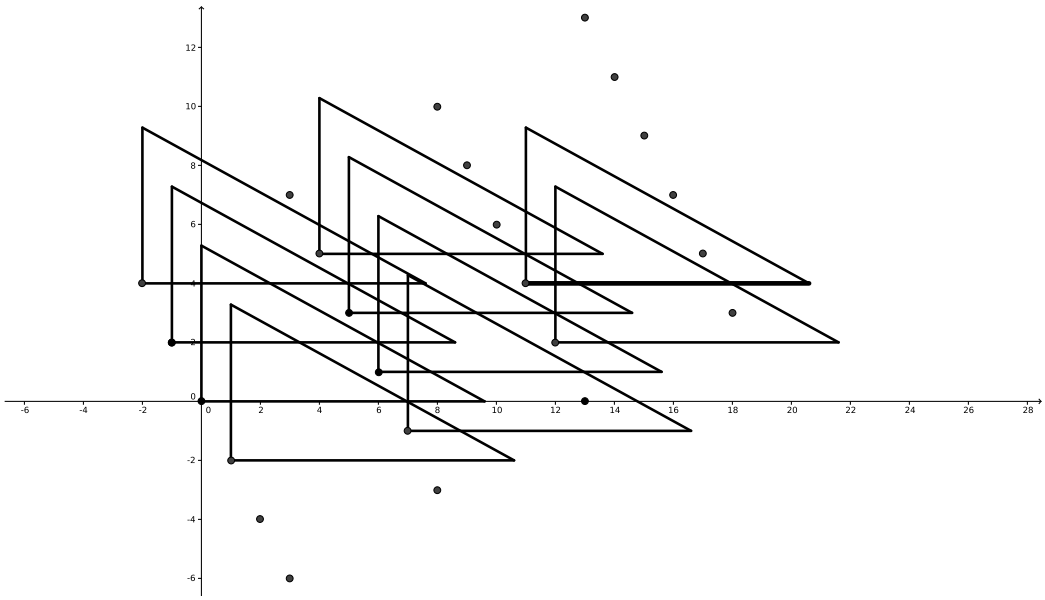
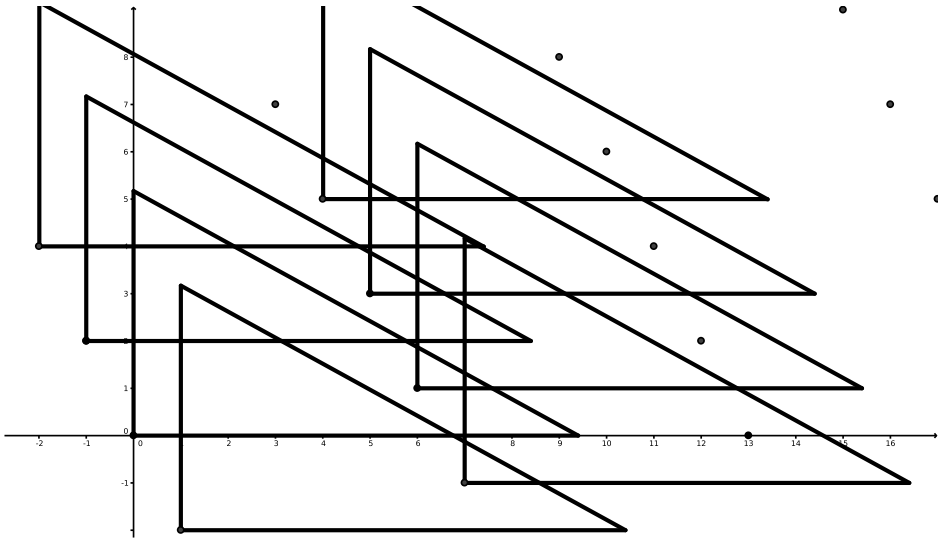


Figura 3.4: El retículo L y el conjunto S.



(a) (48)S cubre todo el plano.



(b) (47)S deja pequeños huecos sin cubrir.

Figura 3.5: (a) (48)S y (b) (47)S.

Bibliografía

[1] J. L. Ramírez Alfonsín, *The diophantine Frobenius problem (Vol. 30)*, Oxford University Press (2005).

[2] J. C. Rosales, P. A. García-Sánchez, *Numerical semigroups (Vol. 20)*, Springer (2009).

[3] G. Márquez Campos, *Calculo de invariante combinatorios de semigrupos numéricos y aplicaciones*, Universidad de Sevilla. Tesis doctoral (2014).

[4] J. L. Ramírez Alfonsín, *Complexity of the Frobenius problem*, Combinatorica 16(1) (1996), 143-147.

[5] R. M. Karp, *Reducibility among combinatorial problems. In Complexity of computer computations*, Springer (1972), 85-103.

[6] J. J.Sylvester, *Mathematical Questions, with their solutions,from the Educational Times*, Vol. 41 (1884), p. 21.

[7] M. Nijenhuis and H.S. Wilf, *Representation of integers by linear forms in nonnegative integers*, J. Number Theory 4 (1972), 98-106.

[8] E S. Selmer, O. Beyer, *On the linear diophantine problem of Frobenius in three variables*, Journal für die Reine und Angewandte Mathematik 301 (1978), 161-170.

[9] Ø. J. Rødseth, *On a linear diophantine of Frobenius*, Journal für die Reine und Angewandte Mathematik 301 (1978), 171-178.

[10] J. L. Davison, *On the linear diophantine of Frobenius*, J. Number Theory 48 (1994), 353-363.

[11] S. M. Johnson, *A linear diophantine problem*, Can. J. Math. 12 (1960), 390-398.

[12] H. G. Killingbergtrø, *Using figures in Frobenius' problem*, Normat 2 (2000), 75-82.

[13] F. Curtis, *On formulas for the Frobenius number of a numerical semigroup*, Math. Scand. 67 (1990), 190-192.

[14] L. G. Fel, *Frobenius problem for semigroups* $S(d_1, d_2, d_3)$, manuscript (2004), 43 pages.

[15] C. Niu, Z.Oiu, *On a problem Frobenius*, J. Shandong Univ. Nat. Sci. Ed. 21(1) (1986), 1-6.

[16] A. Brauer, J. E. Shockley, *On a problem of Frobenius*, Journal für die Reine und Angewandte Mathematik 211 (1962), 215-220.

[17] J. B. Roberts, *On a diophantine problem*, Canadian Journal of Mathematics 9 (1957), 219-222.

[18] E. L. Goldberg, *On a linear diophantine equation*, Acta Arithmetica 31 (1976), 239-246.

[19] J. S. Byrnes, *On a partition problem of Frobenius*, Journal of Combinatorial Theory Ser. A 17 (1974), 162-166.

[20] E. S. Selmer, *On a linear diophantine Problem of Frobenius*, Journal für die Reine und Angewandte Mathematik 293/294(1) (1977), 1-17.

[21] I. D. Kan, B. S. Stechkin, I. V. Sharkov, *On the Frobenius problem for thee arguments*, Mat. Zametki, 62(4) (1997), 626-629.

[22] M. Beck, R. Diaz, S. Robins, *The Frobenius problem, rational polytopes, and Frobenius Dedekind sums*, J. Number Theory, 96(1) (2002), 1-21.

[23] Y. Vitek, *Bounds for a diophantine problem of Frobenius II*, Can. J. Math. 28(6) (1976), 1280-1288.

[24] A. L. Dulmage, N. S. Mendelshon, *Gaps in the esponent set of primitive matrices*, Illinois J. Math. 8 (1964), 642-656.

[25] I. D. Kan, *Representation of numbers by linear forms*, Mat. Zametki, 68(4) (2000), 210-216.

[26] H. E. Scarf, D. F. Shallcross, *The Frobenius problem and maximal lattice free bodies*, Mathematics of Operations Research 18 (1993), 511-515.

[27] B. R. Heap, M. S. Lynn, *A graph-algorithm for the solution of a linear diophantine problem of Frobenius*, Numerische Mathematik 6 (1964), 346-354.

[28] B. R. Heap and M. S. Lynn, *On a linear diophantine problem of Frobenius: an improved algorithm*, Numerische Mathematik 7 (1965), 226-231.

[29] H. Greenberg, *An algorithm for a linear diophantine equation and a problem of Frobenius*, Numerische mathematik 34(4) (1980), 349-352.

[30] M. Nijenhuis, *A minimal-path algorithm for the "money changing problem"*, Amer. Math. Monthly 86(4) (1979), 832-838. Corregido en ibid., 87 (1980), 377.

[31] H. S. Wilf, *A circle-of-lights algorithm for the "money changing problem"*, Amer. Math. Monthly 85 (1978), 562-565.

[32] R. Kannan, *Lattice translates of a polytope and the Frobenius problem*, Combinatorica 12 (1992), 161-177.