Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

EL NOMBRE DE FROBENIUS

Autor: Pau Maristany Sala

Director: Dr. Santiago Zarzuela
Realitzat a: Departament d'Àlgebra i Geometria

Barcelona, 27 de juny de 2018

Abstract

Let $a_1, \ldots, a_n$ be positive integers, find the largest natural number that is not representable as a non-negative combination of $a_1, \ldots, a_n$. This problem is called **Frobenius Problem**. The project consists on a exposition of some of the most important results about this problem. We will study it using numerical semigroups and Hilbert series. We will prove that Frobenius Problem is $\mathcal{NP}$-hard and also that there is no polynomial formula for the general case.

Resum

Siguin $a_1, \ldots, a_n$ nombres naturals, trobar el nombre més gran que no pot ser expressat com a suma positiva o nul·la d'aquests. Aquest problema s'anomena **problema de Frobenius**. Aquest projecte és un recull d'alguns dels resultats més importants que hi ha sobre aquest. Estudiarem aquest problema usant semigrups numèrics i les sèries de Hilbert. També donarem una demostració que és un problema $\mathcal{NP}$-hard i que no existeix cap fórmula polinòmica pel cas general.

Agraïments

A totes les persones que m'han escoltat i han deixat que les escolti. A totes les persones que han après algo de mi i a les que han deixat que aprengui alguna cosa d'elles. D'aquesta llarga llista, em veig amb la necessitat de remarcar la feina que han fet les següents persones:

Agraïments al meu avi i a la meva àvia per haver-me aguantat tants anys.

Agraïments al meu pare, a la meva mare i a mon germà per tot el que m'han donat al llarg de la vida.

Agraïments a la meva cosina per ajudar-me sempre que ho necessitava, i quan no, també. Agraïments al meu cosí per tots els moments inoblidables que hem passat junts.

Agraïments a l'Ignasi, al You, a l'Àngel, per haver-me aguantat tots els cinc anys de carrera. Així com també a l'Àlex, Jesús, Gerard i Laia, per l'últim tram d'aquesta.

Agraïments a l'Oriol i a la Mar pel grup fonamental.

I agraïments a totes les amistats que he tingut al llarg de la vida, la llista dels quals és massa extensa per escriure-la sencera.

Índex

1 Introducció

El matemàtic Ferdinand Georg Frobenius (1849-1917) durant unes conferències va descriure el problema següent:

Donats n nombres naturals $a_1, \ldots, a_n$, trobar el nombre més gran que no pot ser expressat com a suma d'aquests.

Aquests han estat anomenats, respectivament, **problema de Frobenius** i **nombre de Frobenius**, per Alfred Brauer [4].

Considerats $a_1, \ldots, a_n$ nombres naturals, d'ara en endavant, ens referirem al nombre de Frobenius d'aquests com $F(a_1, \ldots, a_n)$. Donat un nombre natural n_0, ens referirem al nombre de Frobenius en el cas $n = n_0$ quan tractem amb $F(a_1, \ldots, a_{n_0})$.

El nombre de Frobenius, simple a primera vista, es pot complicar de maneres molt diferents. El seu estudi engloba àmbits molt diversos de les matemàtiques. Al llarg d'aquest treball s'intentarà tractar aquest problema de diferentes maneres, veient les virtuds i mancances de cada una.

El projecte

Aquest projecte intenta assolir dos objectius. El primer objectiu d'aquest treball és analitzar alguns dels resultats més importants que hi ha sobre el nombre de Frobenius, així com establir unes eines bàsiques que ens ajudin al seu càlcul. Els resultats recullits engloben des de la impossibilitat de donar una fórmula polinòmica general pel nombre de Frobenius amb tres generadors o més (tema 5) fins a donar-ne una (que no és polinòmica) pel cas de $F(a_1, a_2, a_3)$, a partir de dues maneres diferents: amb els semigrups numèrics (tema 4) i amb sèries de Hilbert (tema 6).

El segon objectiu d'aquest projecte és escriure de forma entenedora, clara, precisa i ordenada les demostracions d'aquests resultats, per tal que estiguin a l'abast del màxim nombre de lectors possible. Així, s'ha intentat que aquesta memòria sigui el màxim autocontiguda possible. De fet, hi haurà una demostració per a la majoria dels resultats presentats.

A través d'aquesta memòria veurem com un resultat que a priori sembla innocent engloba molts aspectes diferents de la matemàtica; no només a l'hora de tractar aquest problema des de punts de vista molt diversos, sinó que en la mateixa demostració d'un resultat apareixen eines que van des d'anàlisi de successions a varietats algebraiques, passant pels semigrups numèrics i la successió de Farey.

Estructura de la memòria

Aquest projecte és un recull d'alguns dels resultats més significatius del nombre de Frobenius. Per aquest motiu la memòria s'estructura en capítols en els quals s'analitzen aquests resultats de forma separada.

El segon capítol és una introducció al nombre de Frobenius usant un símil, seguit

d'un petit resum de la història que hi ha darrera aquest i acabant amb dos resultats que asseguren l'existència d'aquest si i només si $\gcd(a_1, \ldots, a_n) = 1$.

En el tercer capítol s'analitzen resultats que determinen directament el nombre de Frobenius i en quins casos són aplicables, proporcionant dues demostracions diferents pel cas $F(a_1, a_2)$. També es presenten dos teoremes en el cas $n = 3$. El primer impossibilita el fet que hi hagi una fórmula polinòmica a partir de $n \geq 3$. El segon, presenta una mena de fórmula pel cas $n = 3$ que serà demostrada més endavant de dues maneres diferents.

El quart és un estudi bastant exhaustiu dels semigrups numèrics, una estructura algebraica de subconjunts dels naturals, per treballar diferents resultats, incloent-hi la demostració del teorema la fórmula de $F(a_1, a_2, a_3)$, el teorema 3.5. Cal remarcar la importància del subconjunt d'*Apèry*, a partir del qual s'obtenen resultats molt importants, com ara una caracterització del conjunt dels pseudo-nombres de Frobenius.

El cinquè es basa totalment en la demostració del teorema 3.3, que demostra la impossibilitat de proporcionar una fórmula polinòmica general per a $F(a_1, \ldots, a_n)$. Crida l'atenció tot el ventall d'àrees de matemàtiques que engloba.

El sisè és un estudi del nombre de Frobenius usant eines d'àlgebra homològica com les sèries de Hilbert. Es veurà la seva relació amb el denumerant de Sylvester, i s'acabarà treballant usant successions exactes de mòduls finitament generats. Per acabar, es mostrarà una segona demostració del teorema 3.5 usant les eines introduïdes en aquest capítol.

El setè capítol s' orienta a la part algorítmica que hi ha al darrera del nombre de Frobenius, donant un algoritme i acabant amb la demostració que estem davant d'un problema $\mathcal{NP}$-hard en termes de Turing.

Finalment, l'Annex conté dues demostracions.

Cal remarcar la impòrtancia que han tingut en aquest projecte dues fonts bibliogràfiques en concret. La primera [18], de Ramírez Alfonsín, i la segona [21], de Rosales, J. C. i García-Sánchez, P. A. Malgrat això, hem volgut consultar les fonts originals de la majoria dels resultats aquí presentats, i així es presenten les referències de forma detallada.

2 El problema de les monedes

El símil de les monedes és una forma molt visual de mostrar l'explicació del nombre de Frobenius: *en un país, les úniques monedes que hi ha són les d'*$a_1, \ldots, a_n$ *valors. Quines quantitats es poden pagar? Sota quines hipòtesis el nombre de valors que no es poden pagar són finits?*

Seguint amb el símil, en aquest capítol veurem que si $\gcd(a_1, \ldots, a_n) = 1$, aleshores existeix una quantitat N tal que qualsevol més gran o igual a aquesta es pot pagar. De fet, per la identitat de *Bèzout*, es poden pagar totes les quantitats si admetem que es pot donar canvi, és a dir, que es pot restar.

En aquest projecte s'estudiarà el cas en què no es pot donar canvi, és a dir, quins valors es poden donar només sumant, i és que és aquí on apareix el nombre de Frobenius.

Resulta curiós que aquest símil és usat molt més en el món de la computació, mentre que el nom de nombre de Frobenius acostuma a acompanyar estudis des d'un punt de vista algebraic.

Aquest problema també s'ha divulgat amb el nom de *McNugget Problem*, on un nombre és *McNugget* si i només si es poden aconseguir aquesta quantitat de *McNuggets* al famós restaurant nord-americà *McDonald's* amb caixes de 6, 9, o 20 unitats. És a dir, és un estudi del cas concret $F(6, 9, 20)$.

2.1 Una mirada cap enrere

Encara que sembli un problema relativament simple, un dels primers autors en tractar amb aquest fou Alfred Brauer al 1942 en [4]. En aquest document descriu com Ferdinand Georg Frobenius el mencionava en unes conferències. És per aquesta raó que se li dona l'autoria a ell, si bé mai el posà per escrit. No va ser fins uns anys més tard que es començarien a donar resultats en aquesta línia d'investigació.

La demostració de la fórmula del nombre de Frobenius quan $n = 2$ va ser donada pel propi Frobenius, però no va ser capaç de trobar la del cas $n = 3$. Qui va poder donar el teorema pel cas $n = 3$ fou Herzog [11], al 1969. Observem com va passar bastant temps des de l'ultim avenç.

En aquella època, Wilf i Nijenhuis [14] [24] també l'estaven estudiant, però des d'un punt de vista computacional.

També va ser en aquella dècada que van observar la seva relació amb la sèrie de Hilbert, i a partir de llavors aquest problema va agafar més renom i més coneixement entre els matemàtics.

En aquest projecte es tractaran resultats novells, com ara la impossibilitat de donar una fórmula polinòmica pel cas general, que data del 1990 [8], o bé que és un problema $\mathcal{NP}$-hard en termes de Turing, que data del 1996 [19].

2.2 Existència

De forma natural el primer que un es qüestiona quan sent a parlar del nombre de Frobenius és sobre la seva existència. En aquesta secció veurem que si $\gcd(a_1, \ldots, a_n) = 1$, aleshores existeix, i també que aquesta hipòtesi no només és suficient sinó que és necessària.

Per a veure l'existència donarem un altre nombre N tal que per a tot enter s més gran o igual que N llavors s es pot representar com a suma no negativa de $a_1, \ldots, a_n$.

Teorema 2.1. *Siguin $a_1, \ldots, a_n$ enters tals que $\gcd(a_1, \ldots, a_n) = 1$, llavors existeix $N \in \mathbb{N}$ tal que per a tot enter $s \geq N$, s es pot expressar com a suma d'una combinació no negativa de $a_1, \ldots, a_n$.*

Demostració. Pel Teorema de Bezout, existeixen $m_1, \ldots, m_n \in \mathbb{Z}$ tal que $a_1 m_1 + \ldots + a_n m_n = 1$. Siguin P la suma de tots els termes $a_i m_i$ positius i Q el valor absolut de la suma de tots els termes $a_i m_i$ negatius, per tant $P - Q = 1$. Veurem que $(a_1 - 1)Q = N$.
Sigui $l \geq (a_1 - 1)Q$, anomenem $k = l - (a_1 - 1)Q$, i si fem la divisió entera de k entre a_1, obtenim que existeixen dos enters $h \geq 0$ i $0 \leq k' < a_1$ tal que $k = ha_1 + k'$. Per tant, $l = (a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$, que pot ser expressat com a suma positiva de a_i's, ja que Q i P ho són i $a_1 - k' - 1 \geq 0$ per la divisió entera. □

Aquesta cota superior de $F(a_1, \ldots, a_n)$ està lluny de ser una bona cota, ja que actualment se n'han trobat molt més bones. Per exemple, en el cas $a_1 = 2.014$ i $a_2 = 4.021$ calculant la identitat de Bezout obtenim que:

$$4.021 \cdot 863 - 2.014 \cdot 1.723 = 1,$$

per tant la cota que hem vist seria $(2.014 - 1)2.014 \cdot 1.723 = 6.985.355.586$, lluny de la cota superior donada pel teorema 7.1, que seria $4.021^2 = 16.168.441$. De fet, pel teorema 4.22 obtenim que $F(2.014, 4.021) = 8.092.259$.

Veiem ara que la hipòtesi no només és suficient, sinó que és necessària:

Corol·lari 2.2. *Siguin $a_1, \ldots, a_n$ nombres naturals tals que $gcd(a_1, \ldots, a_n) = d > 1$, aleshores la quantitat de nombres naturals no expressables com a suma positiva de $a_1, \ldots, a_n$ és infinita.*

Demostració. Si el $\gcd(a_1, \ldots, a_n) = d > 1$, aleshores d divideix a qualsevol suma que es podria fer amb $a_1 \ldots, a_n$, així, la quantitat de nombres naturals que no poden ser expressats és infinita. □

Obtenim així que $F(a_1 \ldots, a_n)$ existeix si i només si $\gcd(a_1 \ldots, a_n) = 1$. En cap dels dos resultats acabats de veure es parla de nombre de Frobenius directament, això està fet expressament perquè siguin aplicables sense que hi hagi la necessitat de modificar-los més endavant al tema 4.

3 Nombre de Frobenius en alguns casos

En aquest capítol s'estudiarà el nombre de Frobenius quan $n = 2$, donant el Teorema 3.1, que en dona una fórmula polinòmica. D'aquest teorema se'n veuran dues demostracions. N'apareix una tercera en el capítol 4, però cal dir n'hi ha moltes més. També es veurà per sobre el cas quan $n = 3$, donant uns resultats que seran demostrats més endavant.

Els resultats d'aquest capítol i les demostracions mostrades aquí són totes extretes de [18].

3.1 Nombre de Frobenius quan $n = 2$

Aquest apartat es basa en donar dues demostracions del següent teorema:

Teorema 3.1. *Siguin a i b dos nombres naturals tals que* $\gcd(a, b) = 1$*, aleshores*

$$F(a, b) = ab - a - b.$$

La primera demostració, que és més simple, està basada en el càlcul de les solucions de l'equació diofàntica:

$$ax + by = m. \tag{3.1}$$

La segona, és un argument geomètric que usa el Teorema de Pick.

Demostració 1. Com que $\gcd(a, b) = 1$, per a tot m existeixen x, y tals que $m = ax + by$.
Les solucions de 3.1 són de la forma:

$$x = rm + tb$$
$$y = sm - ta$$

per a tot m, on r i s són enters tals que $ra + sb = 1$ i amb t enter arbitrari.
Per tant, podem afirmar que per a tota m si $0 \leq x < b$, llavors existeix una única solució (x, y) de l'equació 3.1.
Sigui S el conjunt de nombres naturals format per sumes positives o nules de a i b, és a dir, s pertany a S si i només si existeixen x i $y \geq 0$ tals que $s = ax + by$.
Veiem ara que si $m \in S$, amb $m = ax + by$, amb $0 \leq x < b$ llavors $y \geq 0$:
Suposem que $m = ax + by = ax' + by'$, amb $x', y' \geq 0$.
Llavors, $a(x' - x) = b(y - y')$ i com que $0 \leq x < b$, obtenim dos casos:

$x = x'$ en aquest cas $y = y' \geq 0$.

$x < x'$ en aquest cas $y > y' \geq 0$.

Per tant, podem afirmar que per a tots els elements de S, que són de la forma $ax + by$, al restringir la x en $0 \leq x < b$, la y pren valors positius o iguals a 0.

Per aquesta raó, l'enter m més gran que no pertany a S és aquell on $x = b - 1$ i $y = -1$, donant així la fórmula

$$F(a, b) = a(b - 1) - b = ab - a - b$$

i demostrant el teorema. □

Aquí hem definit S com el conjunt de nombres naturals formats per sumes positives o nul·les d'a i de b. Amb aquestes condicions S és una estructura algebraica que s'anomena semigrup numèric. D'aquesta estructura algebraica se'n farà un estudi més exhaustiu al capítol 4.

La segona demostració consisteix en considerar les rectes de la forma $ax+by = m$, i veure quines tenen solucions enteres al primer quadrant, és a dir positives o iguals a 0, i arribar a la conclusió que qualsevol recta de la forma $ax + by = m$ amb $m > ab - a - b$ té solució entera no negativa.

Fixem-nos en la figura 3.1, on estan marcats tots els punts amb coordenades enteres positives o iguals a 0 i les rectes equivalen a:

$$5x + 4y = 11$$
$$5x + 4y = 20$$
$$5x + 4y = 34$$

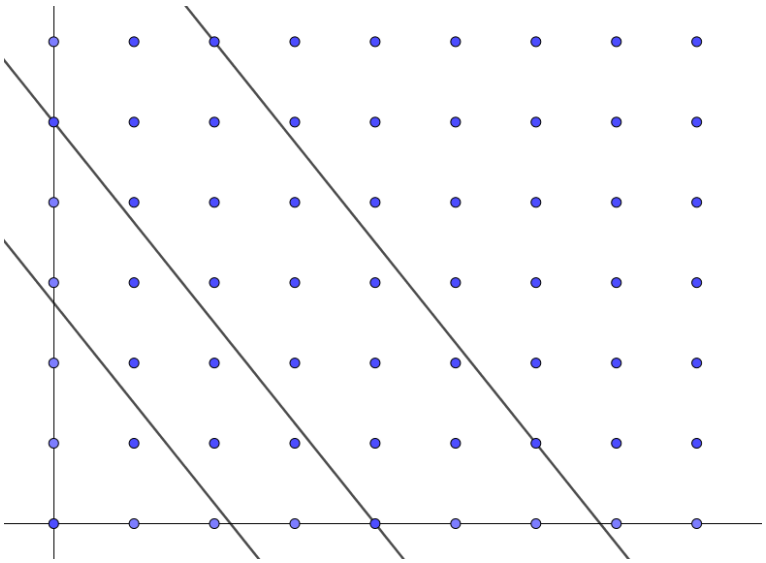

Figura 1: Exemple de rectes amb coordenades als enters, la primera recta és $5x+4y = 11$, la segona és $5x + 4y = 20$ i la tercera és $5x + 4y = 34$.

La primera recta no talla a cap punt, de fet, qualsevol recta de la forma $5x+4y = m$ amb $m > 11$ sí que talla a algun punt amb coordenades enteres positives. Això fa que 11 sigui el nombre de Frobenius de 4 i 5 ($4 \cdot 5 - 4 - 5 = 11$).

La segona recta, en canvi, talla els punts $(4,0)$ i $(0,5)$, ja que $5 \cdot 4 + 4 \cdot 0 = 20$ i $5 \cdot 0 + 4 \cdot 5 = 20$. I la tercera en els punts $(6,1)$ i $(3,6)$.

La primera recta ($ax+by = ab-a-b$) i la segona recta ($ax+by = ab$) apareixeran a la segona demostració, conformant un paral·lelogram a partir de l'estudi del qual es basa tota aquesta.

Per la segona demostració, usarem el Teorema de Pick:

Teorema 3.2 (Teorema de Pick)**.** *Sigui S un polígon al pla amb els vèrtexs amb coordenades als enters, llavors:*

$$A(S) = I(S) + \frac{B(S)}{2} - 1$$

on $A(S)$ és l'àrea de S, $I(S)$ és la quantitat de punts amb coordenades als enters a l'interior de S i $B(S)$ és la quantitat de punts amb coordenades als enters pertanyen als costats del polígon S.

La demostració d'aquest teorema no es donarà, per la falta d'espai i la senzillesa però llargada d'aquesta. El lector la pot trobar a [7]. Aquesta es basa en reduir qualsevol polígon en unió de triangles i usant inducció en aquests.

Demostració 2. Considerem el polígon P de vèrtexs $A = (b,0)$, $B = (b-1,-1)$, $C = (0,a)$ i $D = (-1,a-1)$, que està representat a la figura 2.
Primerament estudiarem la seva àrea. Després veurem quins són els punts de la frontera i, pel teorema de Pick, obtindrem la quantitat de punts que hi ha a l'interior d'aquest polígon. Més tard veurem que a cada recta de la forma $ax + by = j$, amb $ab - a - b < j < ab$ només passa per un punt en coordenades enteres positives. Finalment veurem que tota recta de la forma $ax + by = m$ amb $m > ab$ té una solució amb coordenades enteres positives, demostrant així el teorema.
Sigui r la recta que va del $(b-1,-1)$ al $(-1,a-1)$, que té com a equació:

$$ax + by = ab - a - b$$

ja que $a(b-1) + b(-1) = ab - b - a$ i $a(-1) + b(a-1) = -a + ab - b$.
Sigui s la recta que va del $(b,0)$ al $(0,a)$, que té com a equació $ax + by = ab$.
L'objectiu d'aquesta demostració és veure que la recta r no té cap solució amb coordenades als enters al primer quadrant, i que tota altra recta de la forma

$$ax + by = m$$

amb $m > ab - a - b$ sí que en té.
Calculem l'àrea de P de manera traddicional, i, comparant-la amb la fórmula de Pick, ens donarà la quantitat de punts que hi ha a P. Com que el vector $\overrightarrow{BA} = \overrightarrow{(1,1)}$ és paral·lel al vector $\overrightarrow{DC}$ i de la mateixa manera el vector $\overrightarrow{BD} = \overrightarrow{(-b,a)}$ és paral·lel al vector $\overrightarrow{AC}$, obtenim que P és un paral·lelogram, i per tant l'àrea de P és:

$$\text{Àrea } P = \det\left(\overrightarrow{BA}, \overrightarrow{BD}\right) = \begin{vmatrix} 1 & 1 \\ -b & a \end{vmatrix} = a + b$$

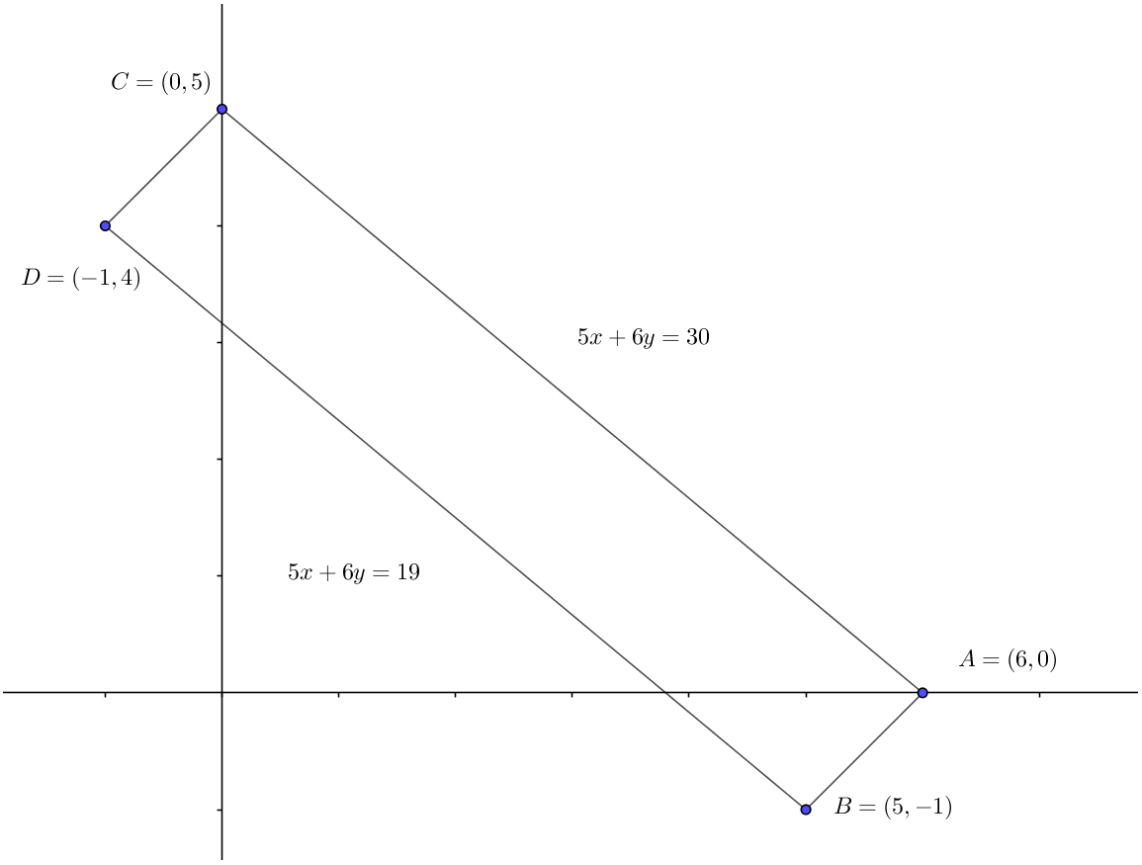

Figura 2: Exemple de polígon P en el cas $a = 5$ i $b = 6$.

Veiem ara quins punts hi ha a la frontera de P.
Si ens fixem en l'equació $ax + by = ab$ i la veiem mod a, obtenim que:

$$by \equiv 0 \mod a,$$

i com que $\gcd(a, b) = 1$ l'equació només tindrà solucions quan $y \equiv 0 \mod a$, és a dir, quan y sigui múltiple de a, en cap cas en l'interval $(0, a)$.
Per veure el resultat equivalent amb el segment de B a D, veiem que només té solucions enteres quan $(y + 1)$ és multiple de a, que no passa en cap cas quan $y \in (-1, a - 1)$.
I del segment que va punt A al B o el segment que va del punt D al C, aquest no té cap solució entera, doncs el segment mesura $\sqrt{2}$ i va d'un punt enter a un altre.
Si ho comparem amb la fórmula del Teorema de Pick obtenim que el nombre de punts amb coordenades als enters a l'interior de P és

$$a + b = I(P) + \frac{4}{2} - 1 = I(P) + 1$$

Veiem ara que cada segment de la forma

$$ax + by = ab - a - b + i$$

conté exactament un punt amb coordenades enteres a l'interior de P per a cada $i = 1, \ldots, a+b-1$. Suposem que existeix $1 \leq j \leq a+b-1$ tal que el segment $ax + by = ab - a - b + j$ conté dos punts de $I(P)$: (x_1, y_1) i (x_2, y_2). És a dir:

$$ax_1 + by_1 = ax_2 + by_2 = ab - a - b + j,$$

per tant,

$$a(x_1 - x_2) = b(y_2 - y_1),$$

i com que $\gcd(a, b) = 1$, $(x_1 - x_2) = sb \geq b$, per tant estarien fora del polígon S.
Si una recta de la forma $ax + by = ab - a - b + j$ no tingués cap punt enter en $I(P)$, aleshores, alguna recta de la forma $ax + by = ab - a - b + j$ en tindria dos, contradient el que hem acabat de veure.
Per tant, cada recta de la forma $ax + by = ab - a - b + j$ amb $1 \leq j \leq a + b$ conté solucions enteres positives.
Fàcilment es veu que $ax + by = m \geq ab$ també.
Si $m \geq ab$, considerem $t_0 = \min\{t \in \mathbb{Z} \mid m - t(a+b) \leq ab\}$ i $w = m - t_0(a+b)$.
Observem que $ab - a - b < w \leq ab$, per tant existeixen x_0 i y_0 enters positius tals que $ax_0 + by_0 = w$. Així, agafant $x_1 = x_0 + t_0$ i $y_1 = y_0 + t_0$, obtenim dos nombres naturals tals que

$$ax_1 + by_1 = a(x_0 + t_0) + b(y_0 + t_0) = ax_0 + by_0 + t_0(a+b) = m$$

demostrant el teorema. □

3.2 Nombre de Frobenius quan $n = 3$

A diferència del cas $n = 2$, el cas $n = 3$ ha resultat ser molt més complicat. Abans de fer un estudi d'aquest, cal observar un resultat molt important al que arribà Frank Curtis en [8]. El tema 5 es basa completament en la demostració d'aquest teorema.

Teorema 3.3. *Sigui* $A = \{(s_1, s_2, s_3) \in \mathbb{N}^3 \mid s_1 < s_2 < s_3,\ s_1$ *i* s_2 *són primers, i* $s_i \nmid s_3$ *per* $i = 1, 2\}$. *Llavors, no existeix cap polinomi diferent de zero* $f \in \mathbb{C}[X_1, X_2, X_3, Y]$ *tal que* $g(s_1, s_2, s_3, F(s_1, s_2, s_3)) = 0$ *per a tot* $(s_1, s_2, s_3) \in A$.

El corol·lari següent mostra que $F(s_1, s_2, s_3)$ no pot ser determinat per cap conjunt finit de fórmules polinòmiques.

Corol·lari 3.4. *No hi ha cap conjunt finit de polinomis* $\{f_1, ..., f_n\}$ *tal que per a tot trio* (s_1, s_2, s_3) *hi ha alguna* i *tal que* $f_i(s_1, s_2, s_3) = F(s_1, s_2, s_3)$.

Demostració. $g = \prod_{i=1}^{n} (f_i(X_1, X_2, X_3) - Y)$ s'anul·laria a A. □

Tot i així, hi ha una fórmula que dona el $F(a_1, a_2, a_3)$ donats tres nombres naturals a_1, a_2, a_3 relativament primers dos a dos:

Teorema 3.5. *Siguin* $\{a_1, a_2, a_3\}$ *tres nombres relativament primers dos a dos,* c_1, c_2 *i* c_3 *els enters més petits tals que existeixen enters* $r_{ij} \geq 0$, $1 \leq i, j \leq 3, i \neq j$ *amb:*

$$c_1 a_1 = r_{12} a_2 + r_{13} a_3,$$
$$c_2 a_2 = r_{21} a_1 + r_{23} a_3,$$
$$c_3 a_3 = r_{31} a_1 + r_{32} a_2.$$

Llavors,

$$F(a_1, a_2, a_3) = \begin{cases} \max\{c_j a_j + r_{ik} a_k, c_k a_k + r_{ji} a_j\} - \sum_{s=1}^{3} a_s & si \quad r_{ij} > 0 \\ & \text{per a tot } i, j, \\ c_j a_j + c_i a_i - \sum_{s=1}^{3} a_s & si \quad x_{ij} = 0 \end{cases}$$

Si bé pot semblar que la hipòtesi que a_1, a_2, a_3 han de ser coprimers dos a dos sigui molt forta, més endavant es veurà que no.

Es veuran dues demostracions d'aquest teorema, la primera en el quart capítol i la segona en el sisè.

Seguidament, s'introduirà una fórmula que dona el nombre de Frobenius de 3 naturals, basada en el nombre de Frobenius en el cas $n = 2$ i en un resultat que es veurà més endavant.

Proposició 3.6. *Siguin* a_1, a_2, a_3 *enters tals que* $\gcd(a_1, a_2) = d$, $a_1 = a_1' d$, $a_2 = a_2' d$ *tal que existeixen enters* x_1, $x_2 \geq 0$ *amb* $a_3 = x_1 a_1' + x_2 a_2'$, *aleshores:*

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

Demostració. Per la proposició 4.23 obtenim que

$$F(a_1, a_2, a_3) = dF(a_1', a_2', a_3) + (d-1)a_3 = d(a_1' a_2' - a_1' - a_2') + (d-1)a_3$$
$$= \frac{a_1 a_2}{d} - a_1 - a_2 + (d-1)a_3$$

doncs $F(a_1', a_2', a_3) = F(a_1', a_2')$. □

Aquest resultat presenta com, a partir d'una hipòtesi molt restrictiva, es pot trobar el nombre de Frobenius d'una forma quasi immediata, en comparació amb el teorema 3.5 que quasi no demana cap hipòtesi addicional.

3.3 Nombre de Frobenius d'algunes sèries numèriques

Per acabar aquest capítol s'introduiran dos resultats que permeten trobar el nombre de Frobenius de conjunts de nombres naturals que segueixen un patró bastant definit.

Teorema 3.7. *Siguin a, d i s enters positius amb* $\gcd(a,d)=1$. *Aleshores,*

$$F(a, a+d, \ldots, a+sd) = \Big(\Big[\frac{a-2}{s}\Big]+1\Big)a + (d-1)(a-1) - 1.$$

Teorema 3.8. *[16] Siguin m, n, k enters positius tals que* $\gcd(m,n)=1$. *Aleshores,*

$$F(m^k, m^{k-1}n, m^{k-2}n^2, \ldots, n^k) = n^{k-1}(mn-m-n) + \frac{(n-1)m^2(m^{k-1}-n^{k-1})}{(m-n)}.$$

Les demostracions d'aquests dos teoremes es troben a l'Annex (doncs ambdues estan basades en càlculs de sumes).

En aquest capítol hem vist com es complica passar del cas $n=2$ al cas $n=3$. De fet, en el cas $n=4$ no es té cap mena de fórmula i s'han trobat molts pocs resultats més enllà del valor de $F(a, a+1, a+2, a+4)$, $F(a, a+1, a+2, a+5)$ i $F(a, a+1, a+2, a+6)$, obtinguts a partir de la teoria de grafs en [10].

4 Semigrups numèrics

En aquest capítol s'estudiarà l'estructura algebraica de semigrup numèric, es treballarà el nombre de Frobenius usant eines d'aquesta, es donarà una demostració del teorema 3.5 i s'acabarà amb alguns resultats que se'n deriven. Tots els resultats que hi ha en aquest capítol, i dels que n'hi ha, la seva demostració, estan extrets de [21]; exceptuant els dos que hi ha a l'últim apartat.

4.1 Semigrups numèrics i conjunt d'Apéry

Aquest apartat és una introducció i un estudi dels semigrups numèrics i del conjunt d'Apèry.

Definició 4.1. *Una parella formada per un conjunt S amb una operació binària $+$, $(S,+)$, és un semigrup si la operació té la propietat associativa.*

Per raons de notació, quan parlem d'un semigrup S en general, estarem donant per entendre que és una parella $(S,+)$, encara que no es mencioni l'operació binària.

Exemple 4.2. Tot grup és un semigrup.

Exemple 4.3. Si considerem $\mathbb{Z}$ amb la multiplicació.

Tots els semigrups que es tractaran en aquest treball tindran la propietat commutativa, per aquesta raó ja no es repetirà l'adjectiu commutatiu a partir d'aquest punt i es donarà per certa.

Definició 4.4. *Sigui $(S,+)$ un semigrup, un subconjunt T de S és un subsemigrup de S si T és tancat per la operació $+$.*

Observem que clarament la intersecció de subsemigrups és un altre subsemigrup.

Sigui A un subconjunt de S, el subsemigrup més petit (amb la relació d'ordre $\subseteq$) que conté A és la intersecció de tots els subsemigrups de S que el contenen. Aquest s'anomena subsemigrup generat per A, es denota per $\langle A\rangle$ i els elements de A generadors de $\langle A\rangle$.

Sigui $a \in A$ i $\lambda \in \mathbb{N}$, anomenarem λa a la suma de λ vegades a amb ella mateixa:

$$\lambda a = \underbrace{a + \ldots + a}_{\lambda}.$$

És senzill veure que:

$$\langle A\rangle = \{\lambda_1 a_1 + ... + \lambda_n a_n \mid n \in \mathbb{N}\setminus\{0\}, \lambda_1, ..., \lambda_n \in \mathbb{N}\setminus\{0\}, a_1, ..., a_n \in A\}.$$

Diem que S està generat per $A \subseteq S$ si $S = \langle A\rangle$.

Definició 4.5. *Un semigrup M és un monoid si conté l'element neutre, és a dir, un element 0 tal que $a + 0 = a$.*

Definició 4.6. *Sigui M un monoid i N un subsemigrup de M, diem que N és un submonoid de M si conté l'element neutre.*

Podem traslladar la definició de subsemigrup generat per A als submonoids. Sigui M un monoid i A un subconjunt de M, llavors el submonoid més petit de M que conté A és:

$$\langle A\rangle = \{\lambda_1 a_1 + ... + \lambda_n a_n \mid n \in \mathbb{N}, \lambda_1, ..., \lambda_n \in \mathbb{N}, a_1, ..., a_n \in A\}.$$

Observem que $\langle\emptyset\rangle = \{0\}$.

Exemple 4.7. Si considerem el monoid de $\mathbb{N}$ amb la multiplicació, i sigui P el conjunt de nombres naturals primers, llavors pel Teorema Fonamental de l'Aritmètica, $\langle P\rangle = \mathbb{N} \setminus \{0\}$.

Exemple 4.8. Els nombres naturals amb la suma formen un monoid.

A partir d'aquest últim exemple, definirem els semigrups numèrics de la següent manera:

Definició 4.9. *Un submonoid de $\mathbb{N}$ és un semigrup numèric si el seu complement és finit.*

Si A i B són dos subconjunts dels nombres enters, llavors definim $A+B = \{a+b \mid a \in A, b \in B\}$.

Sigui S un submonoid. Escrivim $S^* = S \setminus 0$. Per tant obtenim que $S^* + S^*$ correspon al conjunt de S format pels elements que venen donats per la suma de dos elements diferents del zero que pertanyen a S.

Proposició 4.10. *Sigui A un subconjunt finit de $\mathbb{N}$. Llavors $\langle A\rangle$ és semigrup numèric si i només si $gcd(A) = 1$.*

Aquest resultat s'obté directament del teorema 2.1 i del corol·lari 2.2.

La següent proposició no només diu que tot monoid (i per tant tot semigrup numèric) conté un sistema de generadors, sinó que dona un candidat. En aquesta secció veurem que aquest sistema de generadors és finit i donarem una caracterització d'aquests.

Proposició 4.11. *Sigui S un submonoid de $\mathbb{N}$, llavors $S^* \setminus (S^* + S^*)$ és un sistema de generadors de S. A més, tot sistema de generadors de S conté $S^* \setminus (S^* + S^*)$.*

Demostració. Sigui $s \in S^*$. Si $s \notin S^* \setminus (S^* + S^*) \Rightarrow \exists x, y \in S^*$ tal que $s = x + y$, amb $x, y < s$. Repetim aquest procediment per x i per y, i després d'un nombre finit de passos obtenim que $\exists s_1, \ldots, s_n \in S^* \setminus (S^* + S^*)$ tal que $s = s_1 + \ldots + s_n$. Per tant, $S^* \setminus (S^* + S^*)$ és un sistema de generadors.
Veiem ara que tot sistema de generadors conté $S^* \setminus (S^* + S^*)$.
Sigui $A = (a_1, \ldots, a_n)$ un sistema de generadors de S. Si $x \in S^* \setminus (S^* + S^*) \Rightarrow x = \lambda_1 a_1 + \ldots + \lambda_n a_n$, però $x \notin S^* + S^* \Rightarrow x = a_i$ per a un cert $i \in \{1, \ldots, n\}$. □

Per tal de veure que tot semigrup numèric està finitament generat, hem de definir el conjunt de Apéry, anomenat així en honor a Roger Apéry (1916-1994).

Definició 4.12. *Siguin S un semigrup numèric i $n \in S^*$. El conjunt d'Apéry de n en S és:*

$$\mathrm{Ap}(S,n) = \{s \in S \mid s - n \notin S\}.$$

Un sistema minimal de generadors A d'un semigrup numèric S és minimal si tot subconjunt T no igual de A no genera S.

Fixem-nos que, a partir de la definició del conjunt d'Apéry, si $S = \langle a_1, \ldots, a_n \rangle$ amb $a_1, \ldots, a_n$ un sistema minimal de generadors, llavors tots els elements de $\mathrm{Ap}(S, a_i)$ són de la forma $\alpha_1 a_1 + \ldots + \alpha_{i-1} a_{i-1} + \alpha_{i+1} a_{i+1} + \ldots + \alpha_n a_n$.

Exemple 4.13.

$$\mathrm{Ap}(\langle 4, 7 \rangle, 15) = \{0, 4, 7, 8, 11, 12, 14, 16, 18, 20, 21, 24, 25, 28, 32\},$$

$$\mathrm{Ap}(\langle 6, 7, 8 \rangle, 12) = \{0, 6, 7, 8, 14, 15, 16, 21, 22, 23, 29\}.$$

Fixem-nos que en ambdós casos el nombre d'elements de $\mathrm{Ap}(S, n)$ és n.

Proposició 4.14. *Siguin S un semigrup numèric i n un element de S. Llavors*

$$\mathrm{Ap}(S,n) = \{w(0) = 0, w(1), w(2), ..., w(n-1)\}$$

on $w(i)$ és el més petit de tots els elements de S congruents amb i mod n, per tot $i \in \{0, ..., n-1\}$.

Demostració. Primer, com que el complementari de S és finit obtenim que $\forall i \in \{0, ..., n-1\}$ existeix $k \in \mathbb{N}$ tal que $kn + i \in S$.
Sigui $X_i = \{s \in S \mid s \equiv i \mod n\}$. Pel resultat que just hem vist, cap dels X_i és buit.
Aleshores $\mathrm{Ap}(S,n) = \{\min X_i \mid i \in \{0, \ldots, n-1\}\}$, que és un resultat trivial. □

Corol·lari 4.15. *El nombre d'elements de $\mathrm{Ap}(S,n)$ és n.*

Teorema 4.16. *Tot semigrup numèric admet un sistema de generadors minimal finit.*

Per a veure la demostració d'aquest teorema, veurem un lema que és conseqüència directe de la proposició 4.14:

Lema 4.17. *Siguin S un semigrup numèric i $n \in S^*$. Aleshores per a tot $s \in S$, existeix una única parella $(k, w) \in \mathbb{N} \times \mathrm{Ap}(S,n)$ tal que:*

$$s = kn + w$$

I usant aquest lema es pot demostrar el teorema 4.16 fàcilment.

Demostració del Teorema 4.16. Pel lema 4.17, observem que $\langle \mathrm{Ap}(S,n) \cup \{n\} \rangle = S$, que és un sistema de generadors finit.
Com que $\mathrm{Ap}(S,n) \cup \{n\}$ conté $S^* \setminus (S^* + S^*)$, $S^* \setminus (S^* + S^*)$ és finit.
I finalment observem que $S^* \setminus (S^* + S^*)$ és minimal, ja que qualsevol sistema de generadors el conté. Per tant tot semigrup numèric conté un sistema de generadors minimal finit. □

A l'apartat 4.2, veurem que el sistema de generadors minimal és únic.

4.2 Nombre de Frobenius i Pseudo-Nombres de Frobenius

En aquest apartat, s'introduirà el nombre de Frobenius usant la nomenclatura dels semigrups numèrics, així com es veurà per primera vegada els pseudo-nombres de Frobenius, que tenen un especial interès a l'hora de treballar amb els nombres de Frobenius.

Per tal d'indicar el nombre de Frobenius d'un semigrup numèric S usarem la notació $F(S)$, molt semblant a la que hem usat al segon capítol quan indicàvem el nombre de Frobenius d'un conjunt de nombres $a_1, ..., a_n$, usant la notació $F(a_1, ..., a_n)$. Per tant, es farà un abús de notació i s'indicarà $F(a_1, ..., a_n) = F(\langle a_1, ..., a_n \rangle)$.

Definició 4.18. *Sigui S un semigrup numèric, el nombre de Frobenius de S, $F(S)$ és el major nombre natural no contingut en S.*

En alguns textos, no es parla del nombre de Frobenius de S, sinó del conductor de S, $c(S)$, que és aquell element contingut en S tal que $c(S) + n \in S \ \forall n \in \mathbb{N}$, és a dir, $F(S) + 1$.

A la següent proposició veurem la gran importància que té el conjunt d'Apèry $Ap(S,n)$ per a qualsevol n a l'hora de calcular el nombre de Frobenius de S.

Proposició 4.19. *Siguin S un semigrup numéric i $n \in S^*$, aleshores:*

$$F(S) = \max \mathrm{Ap}(S,n) - n.$$

Demostració. Per definició del conjunt d'Apèry, $\max(\mathrm{Ap}(S,n)) - n \notin S$.
Si $x > \max \mathrm{Ap}(S,n) - n \Rightarrow x + n > \max \mathrm{Ap}(S,n)$.
Sigui $w \in \mathrm{Ap}(S,n)$ tal que w i $x+n$ són congruents mòdul n, que hem vist que existeix.
Com que $x + n > \max \mathrm{Ap}(S,n)$, obtenim que $x + n > w$ i $x > w - n$. Per tant existeix $k \geq 0$ entera tal que $x = w + kn$.

Si $k = 0$ aleshores $x \in S$.

Si $k > 0$ aleshores $x - n = w + (k-1)n$ veient així que $x - n$ pertany a S i x també.

Per tant, si $x > \max \mathrm{Ap}(S,n) - n$ aleshores $x \in S$, demostrant així la proposició. □

Cal remarcar que la importància d'aquesta proposició és que n no ha de ser necessàriament d'un generador, sinó que pot ser qualsevol natural que pertanyi a S.

Exemple 4.20.

$$F(4,7) = \max \mathrm{Ap}(\langle 4,7\rangle, 15) - 15 = 32 - 15 = 17 = 4 \cdot 7 - 4 - 7$$

$$F(6,7,8) = \max \mathrm{Ap}(\langle 6,7,8\rangle, 12) - 12 = 29 - 12 = 17$$

Corol·lari 4.21. *Siguin $a_1, \ldots, a_n$ nombres coprimers, aleshores*

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

on t_l és l'enter més petit congruent a l mòdul a_n que és expressable com a suma no negativa de $a_1, \ldots, a_{n-1}$.

Demostració. S'obté directament de la proposició 4.14 i de la proposició 4.19. □

Corol·lari 4.22. *Siguin a i b nombres naturals tals que $gcd(a,b) = 1$, llavors*

$$Ap(\langle a,b\rangle, b) = \{0, a, 2a, ..., (b-1)a\}$$

que dona una tercera demostració del teorema 3.1:

$$F(a,b) = (b-1)a - b = ab - a - b.$$

Demostració. Com que $\gcd(a,b) = 1$, a és un element invertible mod b . Per tant $\{0, a, 2a, \ldots, (b-1)a\}$ són els diferents residus mòdul b. Tots aquests conformen $Ap(\langle a,b\rangle, b)$, doncs pertanyen a $\langle a,b\rangle$ i al restar b no hi pertanyen. □

El següent resultat és molt útil alhora de calcular el nombre de Frobenius, i a més ens servirà sobretot per a la fórmula en el cas $n = 3$, doncs es demanarà que els generadors del semigrup $\{a_1, a_2, a_3\}$ siguin coprimers entre ells.

Proposició 4.23. *Siguin S un semigrup numèric amb un sistema de generadors $\{a_1, ..., a_n\}$, $d = gcd(a_1, ...a_{n-1})$ i T el semigrup numèric generat per $\langle \frac{a_1}{d}, ..., \frac{a_{n-1}}{d}, a_n\rangle$. Llavors,*

$$F(S) = dF(T) + (d-1)a_n.$$

Aquesta proposició es demostra molt fàcilment a partir del següent lema:

Lema 4.24. *Siguin S un semigrup numèric amb un sistema de generadors $\{a_1, ..., a_n\}$, $d = gcd(a_1, ...a_{n-1})$ i T el semigrup numèric generat per $\langle \frac{a_1}{d}, ..., \frac{a_{n-1}}{d}, a_n\rangle$. Llavors,*

$$Ap(S, a_n) = dAp(T, a_n).$$

Demostració. Veiem les dues inclusions:

Si $w \in Ap(T, a_n)$ veurem que $dw \in S$ i que $dw - a_n \notin S$.
$w \in Ap(T, a_n) \Rightarrow w \in T$ i $w - a_n \notin T$.
Com que $w \in T$, $w \in \langle \frac{a_1}{d}, ..., \frac{a_{n-1}}{d} \rangle \Rightarrow dw \in \langle a_1, \ldots, a_{n-1} \rangle$, que és un monoid que pertany a S, $\Rightarrow dw \in S$.
Veurem que $dw - a_n \notin S$, per fer-ho suposarem que sí i arribarem a una contradicció.
Si $dw - a_n \in S$ llavors existeixen $\lambda_1, ..., \lambda_n \in \mathbb{N}$ tal que $dw - a_n = \lambda_1 a_1 + ... + \lambda_n a_n$ i $dw = \lambda_1 a_1 + ... + (\lambda_n + 1)a_n$.
Com que $d \mid dw$ i $d \mid a_i \ \forall i \in \{1, ..., n-1\}$, obtenim que $d \mid (\lambda_n + 1)a_n$. Però $gcd(a_1, ..., a_n) = 1$ i per la propietat del màxim comú divisor: $gcd(a_1, ...a_{n-1}, a_n) = gcd(gcd(a_1, ..., a_{n-1}), a_n) = gcd(d, a_n) = 1$, per tant:

$$w = \lambda_1 \frac{a_1}{d} + ... + \lambda_{n-1} \frac{a_{n-1}}{d} + \frac{(\lambda_n + 1)}{d} a_n$$

amb $\frac{(\lambda_n+1)}{d} > 0$, contradient que $w \in Ap(T, a_n) \Rightarrow dw - a_n \notin S \Rightarrow dw \in Ap(S, a_n)$.

Si $w \in Ap(S, a_n)$ llavors $w \in \langle a_1, ..., a_{n-1} \rangle$, per tant, $w/d \in \langle a_1/d, ..., a_{n-1}/d \rangle \subseteq T$.
Si $w/d - a_n \in T \Rightarrow w - da_n \in S$, contradient que $w \in Ap(S, a_n)$.

□

I a partir d'aquest lema, obtenim la demostració de la proposició 4.23 de forma immediata:

Demostració de la Proposició 4.23. Usant que

$$F(T) = \max Ap(S, a_n) - a_n \Rightarrow \max Ap(T, a_n) = F(T) + a_n$$

obtenim que

$$F(S) = \max Ap(S, a_n) - a_n = \max dAp(T, a_n) - a_n = dF(T) + da_n - a_n.$$

□

Com ja havíem dit, aquest resultat serveix per a facilitar el càlcul del nombre de Frobenius de molts semigrups:

Exemple 4.25.

$$F(17, 20, 30) = 10F(2, 3, 17) + 9 \cdot 17 = 10(2 \cdot 3 - 2 - 3) + 153 = 163$$

$$F(6, 7, 8) = 2F(3, 4, 7) + 1 \cdot 7 = 2(3 \cdot 4 - 3 - 4) + 7 = 17$$

Seguidament, veurem la definició del conjunt dels pseudo-nombres de Frobenius d'un semigrup numèric S qualsevol, que anotarem com $PF(S)$.

Definició 4.26. *Sigui S un semigrup numèric, llavors un enter $x \in PF(S)$ si $x \notin S$ i $x + s \in S$ per a tot $s \in S \setminus \{0\}$.*

A partir de la definició, es veu clarament que no només $F(S) \in PF(S)$, sinó que $F(S) = \max PF(S)$. Com a conseqüència, l'estudi d'aquest és l'estudi del nombre de Frobenius.

En aquest apartat, veurem la relació entre el conjunt dels pseudo-nombres de Frobenius i el conjunt d'Apèry. Però per fer-ho, s'ha de definir abans una relació d'ordre als enters de la manera següent:

Definició 4.27. *Siguin S un semigrup numèric i a i b dos nombres enters, diem que $a \leq_S b$ si $b - a \in S$.*

Aquest ordre donarà una caracterització dels elements de $PF(S)$ a partir dels elements maximals de $\mathbb{Z} \setminus S$ en aquest ordre.

Proposició 4.28. *Sigui S un semigrup numèric, llavors la relació $\leq_S$ a $\mathbb{Z}$ és una relació d'ordre no necessàriament total.*

Demostració. Per a veure que és relació d'ordre, hem de veure que és reflexiva, transitiva i antisimètrica:

Reflexiva Com que S és un semigrup numèric, és obvi que $a \leq_S a$, doncs $a - a = 0 \in S$.

Transitiva Si $a \leq_S b$ i $b \leq_S c$, obtenim que $a - b \in S$ i que $b - c \in S$, i com que S és tancat per la suma, la suma d'aquestes dues també pertany a S: $(a - b) + (b - c) \in S \Rightarrow a - c \in S \Rightarrow a \leq_S c$.

Antisimètrica Si $a \leq_S b$ i $b \leq_S a$, obtenim que $a - b \in S$ i $b - a = -(a - b) \in S$, però com que tots els elements de S o bé són positius o bé són el 0, obtenim que $a - b = 0 \Rightarrow a = b$.

Per a veure que l'ordre no és necessàriament total, només fa falta un contraexemple:

$$S = \langle 5, 7, 9 \rangle$$

Observem que ni $4 \leq_S 2$ ni $2 \leq_S 4$. □

Abans de seguir avançant, cal fer incís a la hora de la notació. L'ordre $\leq_S$ pot tenir elements maximals, que, al no ser ordre total, poden ser més d'un. Aquests seran anotats $\max_{\leq_S}$, a diferència de max, que s'entén com el màxim de l'ordre traddicional en els enters, que denotarem per $\leq$.

Corol·lari 4.29. *Siguin S un semigrup numèric i a i b dos nombres naturals tals que $a \leq_S b$, llavors $a \leq b$.*

Proposició 4.30. *Sigui S un semigrup numèric. Aleshores:*

$$PF(S) = \max_{\leq_S} \mathbb{Z} \setminus S.$$

Demostració. Veiem les dues inclusions:
Sigui $x \in PF(S)$, és a dir, $x \notin S$ i $x + s \in S$ per a tot $s \in S \setminus \{0\}$.
Suposem que existeix un enter $y \notin S$ tal que $x \leq_S y$, aleshores $y - x \in S$. Anomenem $t = (y - x) \in S$, $x + t = y \in S$ ja que $x \in PF(S)$ contradient que $y \notin S$.
Siguin $x \in \max_{\leq_S}(\mathbb{Z} \setminus S)$ i $s \in S \setminus \{0\}$ qualsevol. Volem veure que $x + s \in S$. Si $y = x + s \notin S$, $x \leq_S y$, ja que $y - x = s \in S$, contradient que $x \in \max_{\leq_S}(\mathbb{Z} \setminus S)$ i per tant $x \in PF(S)$. □

Obtenim així una caracterització del conjunt dels pseudo-nombres de Frobenius a partir d'aquesta relació d'ordre. A més a més, obtenim aquesta altra proposició, que caracteritza el sistema de generadors minimal d'un semigrup numèric S usant aquest ordre:

Proposició 4.31. *Sigui S un semigrup numèric, aleshores* $\min_{\leq_S} S \setminus \{0\}$ *és el sistema de generadors de S minimal.*

Demostració. Siguin S un semigrup numèric i $\{a_1, ..., a_r\}$ un sistema de generadors de S, amb $a_1 < ... < a_r$, veurem que $\min_{\leq_S} S \setminus \{0\} = \{b_1, ..., b_s\}$, amb $b_1 < ... < b_s$ és el sistema de generadors de S minimal.
La demostració d'aquesta proposició es donarà en forma d'algoritme, l'algoritme 1, del qual donat un sistema de generadors d'un semigrup numèric se'n obté un altre minimal, que serà $\min_{\leq_S} S \setminus \{0\}$.
Observem que la existència de $y = max\{x \in S \mid x \leq_S a_t, x \neq a_t\}$ en l'algoritme 1

Algoritme 1 Trobar sistema de generadors minimal

Inicialitzem:
$\{b_1, ..., b_s\} = \{0, ..., 0\}$;
$b_1 = a_1$;
$t = 1$;
$h = 1$;
Mentre $t \leq r$
Si a_t és $\min_{\leq_S} S \setminus \{0\}$
Llavors
$b_h = a_t$;
$t = t + 1$;
$h = h + 1$;
Si $\exists \lambda_1, ..., \lambda_h \mid a_t = \lambda_1 b_1 + ... + \lambda_h b_h$
Llavors
$t = t + 1$;
Si no passa cap de les dues anteriors:
Llavors
Sigui $y = max\{x \in S \mid x \leq_S a_t, x \neq a_t\}$;
$b_h = a_t - y$;
$t = t + 1$;
$h = h + 1$;

és deguda a que a_t no és minimal.

Observem també que existeix $b_h = a_t - y \in S$, per la definició de $\leq_S$.
Finalment, veiem que b_h és minimal: si $\exists x \in S \mid x \leq_S b_h \Rightarrow b_h - x = a_s - x - y \in S$, i per la definició de y, obtenim que $b_t = x$. □

D'aquesta propietat, obtenim que tot semigrup numèric admet un únic sistema de generadors minimal. Direm dimensió d'immersió de S i escriurem $e(S)$ al nombre d'elements del sistema de generadors minimal d'un semigrup S qualsevol.

La següent proposició, si bé no sembla molt rellevant, serà essencial a l'hora de calcular el nombre de Frobenius per $n = 3$.

Proposició 4.32. *Siguin S un semigrup numèric i n un element de S diferent de zero. Aleshores:*

$$PF(S) = \{w - n \mid w \in \max_{\leq_S} \mathrm{Ap}(S, n)\}$$

Demostració. Veurem les dues inclusions:
Sigui $x \in PF(S)$, és a dir, $x \notin S$ i $x + n \in S$, per tant, $x + n \in \mathrm{Ap}(S, n)$.
Veiem ara que aquesta $x + n$ és maximal. Sigui $w \in \mathrm{Ap}(S, n)$ tal que $x + n \leq_S w \Rightarrow w - x - n \in S \Rightarrow w - n = x + s$ per a certa $s \in S$. Però per definició de $\mathrm{Ap}(S, n)$, $w - n \notin S$, però $x \in PF(S)$, implicant que $s = 0$. Per tant, $w = x + n$, obtenint així que $x + n$ és maximal.
Sigui ara $w \in \max_{\leq_S} \mathrm{Ap}(S, n)$. Per tant, $w - n \notin S$ i donat un element $s \in S$ qualsevol si $w - n + s \notin S$ implicaria que $w + s \in \mathrm{Ap}(S, n)$, contradient que $w \in \max_{\leq_S} \mathrm{Ap}(S, n)$ doncs $w \leq_S w + s$. □

Com ja s'ha vist abans, si $S = \langle a, b \rangle$ amb $gcd(a, b) = 1$, aleshores:

$$Ap(S, b) = \{0, a, 2a, ..., (b - 1)a\}$$

I per tant $\max_{\leq_S} Ap(S, b) = \{(b - 1)a\}$, sent així $PF(S) = \{ab - a - b\}$.

Anomenarem tipus d'S i escriurem $t(S)$ al nombre d'elements de $PF(S)$.

Corol·lari 4.33.

$$t(S) \leq e(S) - 1.$$

Demostració. Observem que si $\{a_1, \ldots, a_n\}$ és una base minimal de S, aleshores tots aquests pertanyen a $Ap(S, a_n)$ menys l'element a_n, per tant $t(S) \leq e(S) - 1$ doncs $\#PF(S) = \#\max_{\leq_S} Ap(S, a_n) \leq \#Ap(S, a_n) = e(S) - 1$. □

4.3 Semigrups numèrics en l'estudi del nombre de Frobenius quan $n = 3$

En aquesta secció, donarem una demostració del Teorema 3.5 usant el conjunt d'Apèry i els pseudo-nombres de Frobenius.

Recordem la nomenclatura usada en el Teorema 3.5:

Sigui $S = \langle a_1, a_2, a_3 \rangle$, amb $gcd(a_i, a_j) = 1$ per a tot $\{i, j\} \in \{1, 2, 3\}$ tal que $i \neq j$, definim per $i \in \{1, 2, 3\}$:

$$c_i = \min\{k \in \mathbb{N} \setminus \{0\} \mid ka_i \in \langle \{a_1, a_2, a_3\} \setminus \{a_i\} \rangle\}.$$

Com que $gcd(a_j, a_k) = 1$ obtenim que $\langle a_j, a_k \rangle$ forma un semigrup numèric, i per tant existeixen c_i per a tot $\{i, j, k\} = \{1, 2, 3\}$.

D'aquí, obtenim que existeixen $r_{12}, r_{13}, r_{21}, r_{23}, r_{31}, r_{32}$ tal que:

$$\begin{aligned} c_1 a_1 &= r_{12} a_2 + r_{13} a_3, \\ c_2 a_2 &= r_{21} a_1 + r_{23} a_3, \\ c_3 a_3 &= r_{31} a_1 + r_{32} a_2. \end{aligned}$$

Cal dir que aquesta fórmula no dona el nombre de Frobenius per tres nombres naturals qualsevols, ja que té una hipòtesi addicional, que és que els tres nombres naturals, a_1, a_2, a_3, han de ser relativament primers entre ells. Aquesta hipòtesi, però, no és tant forta com sembla, per la proposició 4.23.

La idea general de la demostració serà caracteritzar el conjunt $\max_{\leq_S} Ap(S, a_i)$ amb els generadors de S quan $\{a_1, a_2, a_3\}$ són generadors minimals, per així obtenir $PF(S)$ per la prop 4.32 i per tant $F(S)$.

Lema 4.34. *Si $\{a_1, a_2, a_3\}$ és un sistema minimal de generadors de S, llavors $r_{12}, r_{13}, r_{21}, r_{23}, r_{31}$ i r_{32} són enters positius.*

Demostració. Suposem que r_{ij} és 0. Aleshores, $c_i a_i = r_{ik} a_k$.
Com que c_i és el mínim, obtenim que $c_i \leq a_k$, i usant que $gcd(a_i, a_k) = 1$, obtenim que $c_i a_i \equiv r_{ik} a_k \mod a_k \Rightarrow c_i a_i \equiv 0 \mod a_k \Rightarrow c_i \equiv 0 \mod a_k \Rightarrow c_i = a_k$.
De fet, com que $gcd(a_i, a_k) = 1$, $\exists x \in \{1, \ldots, a_k - 1\} \mid x a_i \equiv a_j \mod a_k$.
D'aquí, veiem que $x a_i = a_j + z a_k$, i per la definició de c_i, obtenim que $c_i \leq x < a_k$, contradient que $c_i = a_k$. □

Veiem ara que les c_i estan determinades per les r_{ji} i r_{ki}, però abans s'ha de veure aquest lema:

Lema 4.35. *Si $\{a_1, a_2, a_3\}$ és un sistema minimal de generadors de S, llavors $c_i \geq r_{ji}$ per a tot $\{i, j, k\} = \{1, 2, 3\}$.*

Demostració. Sumant i movent termes de dues equacions, obtenim:

$$(c_i - r_{ji}) a_i = (r_{ij} - c_j) a_j + r_{ik} a_k$$

Si $(c_i - r_{ji}) < 0 \Rightarrow (r_{ji} - c_i) > 0 \Rightarrow (c_j - r_{ij}) a_j = (r_{ji} - c_i) a_i + r_{ik} a_k$ amb $(r_{ji} - c_i) \in \mathbb{N} \Rightarrow (c_j - r_{ij}) \in \mathbb{N} \setminus \{0\}$, però $(c_j - r_{ij}) \leq c_j$, contradient la definició de c_j. □

Lema 4.36. *Si $\{a_1, a_2, a_3\}$ és un sistema minimal de generadors de S, llavors per a tot $\{i, j, k\} = \{1, 2, 3\}$,*

$$c_i = r_{ji} + r_{ki}.$$

Demostració. Demostrarem que $c_3 = r_{13}+r_{23}$, i fent una permutació dels $\{i,j,k\} = \{1,2,3\}$ obtindrem que $c_2 = r_{12} + r_{32}$ i $c_1 = r_{21} + r_{31}$.
Sumant la primera i la segona equació, obtenim que

$$c_1a_1 + c_2a_2 = (r_{23} + r_{13})a_3 + r_{12}a_2 + r_{21}a_1$$

$$(r_{23} + r_{13})a_3 = (c_1 - r_{21})a_1 + (c_2 - r_{12})a_2.$$

I per la definició de c_3, obtenim que $r_{23} + r_{13} \geq c_3$, doncs $(c_1 - r_{21})$ i $(c_2 - r_{12}) \in \mathbb{N}$ pel lema 4.35.
Fent la permutació, obtenim que $c_2 \leq r_{12} + r_{32}$ i $c_1 \leq r_{21} + r_{31}$.
I com que la suma de les tres equacions és:

$$c_1a_1 + c_2a_2 + c_3a_3 = (r_{21} + r_{31})a_1 + (r_{12} + r_{32})a_2 + (r_{13} + r_{23})a_3$$

obtenim que per a tot $\{i,j,k\} = \{1,2,3\}$,

$$c_i = r_{ji} + r_{ki}.$$

□

I usant el lema anterior, obtenim una caracterització del conjunt dels $PF(S)$:

Lema 4.37. *Si $\{a_1, a_2, a_3\}$ és un sistema minimal de generadors de S, llavors per a tot $\{i,j,k\} = \{1,2,3\}$,*

$$\max_{\leq_S} Ap(S, a_i) = \{(c_j - 1)a_j + (r_{ik} - 1)a_k, (c_k - 1)a_k + (r_{ij} - 1)a_j\}.$$

Demostració. Veiem que $(c_j - 1)a_j + (r_{ik} - 1)a_k \in Ap(S, a_i)$, ho farem amb reducció a l'absurd:
Si $(c_j - 1)a_j + (r_{ik} - 1)a_k \notin Ap(S, a_i)$ existeixen $\{\lambda_i, \lambda_j, \lambda_k\}$ naturals tals que $(c_j - 1)a_j + (r_{ik} - 1)a_k = \lambda_i a_i + \lambda_j a_j + \lambda_k a_k$, amb $\lambda_i \neq 0$.

$$\Rightarrow (c_j - 1 - \lambda_j)a_j + (r_{ik} - 1 - \lambda_k)a_k = \lambda_i a_i$$

Veurem que $\lambda_j < c_j - 1$ i que $\lambda_k < r_{ik} - 1$ per a afirmar que $\lambda_i \geq c_i$:
Si $\lambda_j \geq c_j - 1$, llavors

$$(r_{ik} - 1)a_k = \lambda_i a_i + (\lambda_j - c_j + 1)a_j + \lambda_k a_k$$

com que $\lambda_i > 0$, $\lambda_j - c_j + 1 \geq 0$ i $\lambda_k \geq 0$, aleshores $r_{ik} - 1 > \lambda_k$ i

$$(r_{ik} - 1 - \lambda_k)a_k = \lambda_i a_i + (\lambda_j - c_j + 1)a_j,$$

contradient la minimalitat de $c_k > r_{ik} > r_{ik} - 1 - \lambda_k$, per tant, $\lambda_j < c_j - 1$. Veiem ara que $r_{ik} - 1 > \lambda_k$:

$$(c_j - 1 - \lambda_j)a_j = \lambda_i a_i + (\lambda_k + 1 - r_{ik})a_k$$

per tant, si $c_j - 1 - \lambda_j > 0$ aleshores $\lambda_k + 1 - r_{ik} < 0$ i $r_{ik} - 1 > \lambda_k$.
Així, obtenim que $\lambda_i \geq c_i$.

Si fem la divisió entera de λ_i entre c_i obtenim que $\lambda_i = qc_i + r$, amb $q \in \mathbb{N} \setminus \{0\}$, $0 \leq r < c_i$.

$$\Rightarrow (c_j - 1 - \lambda_j)a_j + (r_{ik} - 1 - \lambda_k)a_k = (qc_i + r)a_i = (qr_{ij}a_j) + (qr_{ik}a_k) + ra_i$$

$$\Rightarrow (c_j - 1 - \lambda_j - qr_{ij})a_j = ra_i + (1 + \lambda_k + (q-1)r_{ik})a_k.$$

D'aquí obtenim que $(c_j - 1 - \lambda_j - qr_{ij}) \geq 0$, contradient amb la definició de c_j.

Observem que és $\max_{\leq_S} Ap(S, a_i)$. Per fer-ho, usarem el corol·lari 4.33, que ens diu que com a molt són 2 elements.
Sigui $fa_j + ga_k \in Ap(S, a_i)$, veiem que o bé $(f, g) \leq (c_j - 1, r_{ik} - 1)$ o bé $(f, g) \leq (r_{ij} - 1, c_k - 1)$, entenent que $(f, g) \leq (h_1, h_2) \iff f \leq h_1$ i $g \leq h_2$.
Veiem que $f < c_j$: si $f = c_j$, obtenim que:

$$fa_j + ga_k = c_j a_j + ga_k = r_{ji}a_i + (r_{jk} + g)a_k \notin Ap(S, a_i)$$

i si $f > c_j$, fent la divisió entera: $f = qc_j + r$ amb $q > 0$ i $r \geq 0$:

$$fa_j + ga_k = (qc_j + r)a_j + ga_k = q(r_{ji}a_i + r_{jk}a_k) + ra_j + ga_k \notin Ap(S, a_i)$$

ja que $r_{ij} > 0$.
I pel mateix raonament $g \leq c_k$.
Per tant, si $(f, g) \nleq (c_j - 1, r_{ik} - 1)$ és degut a que $g \geq r_{ik}$, i veiem que sota aquesta hipòtesi $f < r_{ij}$.
Ho veurem amb la reducció a l'absurd: si $f \geq r_{ij}$, llavors

$$fa_j + ga_k = (f - r_{ij})a_j + r_{ij}a_j + (g - r_{ik})a_k + r_{ik}a_k$$

I com que $r_{ij}a_j + r_{ik}a_k = c_i a_i$:

$$fa_j + ga_k = c_i a_i + (f - r_{ij})a_j + (g - r_{ik})a_k \notin Ap(S, n_i).$$

De forma equivalent, es demostra que si $(f, g) \nleq (r_{ij} - 1, c_k - 1)$ és degut a que $f \geq r_{ij}$, i sota aquesta hipòtesi $g \leq c_k$.
Per tant, obtenim que tots els elements del $Ap(S, n_i)$ estan acotats superiorment per $\{(c_j - 1)a_j + (r_{ik} - 1)a_k, (c_k - 1)a_k + (r_{ij} - 1)a_j\}$ amb l'ordre traddicional $(\leq)$, exceptuant ells dos, que es veurà que ni $(c_j - 1)a_j + (r_{ik} - 1)a_k \nleq_S (c_k - 1)a_k + (r_{ij} - 1)a_j$ ni $(c_k - 1)a_k + (r_{ij} - 1)a_j \nleq_S (c_j - 1)a_j + (r_{ik} - 1)a_k$.
Si fem la resta:

$$(c_j - 1)a_j + (r_{ik} - 1)a_k - (c_k - 1)a_k - (r_{ij} - 1)a_j = r_{ji}a_i - r_{ij}a_j$$

que veurem que no pertany a S.
Suposem que $r_{ji}a_i - r_{ij}a_j > 0$, sinó intercanviem i per j.

$$(r_{ji}a_i - r_{ij}a_j) = \lambda_i a_i + \lambda_j a_j + \lambda_k a_k$$

$$(r_{ji} - \lambda_i)a_i = (\lambda_j + r_{ij})a_j + \lambda_k a_k$$

amb $r_{ji} - \lambda_i > 0$ i contradient que $r_{ji} < c_i$.
Així, hem vist que tots els elements de $Ap(S, a_i)$ són més petits que algun d'aquests dos, que cap d'ells és més gran amb la relació $\leq_S$ que l'altre i que pel corol·lari 4.33 com a molt hi ha 2 elements ja que $e(S) = 3$, demostrant així el lema. $\square$

I amb aquest últim Lema, podem fer la demostració del Teorema 3.5:

Demostració del Teorema 3.5. O bé $\{a_1, a_2, a_3\}$ és un sistema minimal de generadors de $S = \langle a_1, a_2, a_3 \rangle$ o bé no.

Si és un sistema de generadors minimal, pel lema 4.37 obtenim que:

$$\max_{\leq_S} Ap(S, a_i) = \{(c_j - 1)a_j + (r_{ik} - 1)a_k, (c_k - 1)a_k + (r_{ij} - 1)a_j\}.$$

Ara, per la proposició 4.32 obtenim que

$$PF(S) = \{(c_j - 1)a_j + (r_{ik} - 1)a_k - a_i, (c_k - 1)a_k + (r_{ij} - 1)a_j - a_i\}.$$

I per tant

$$F(S) = \max\{(c_j - 1)a_j + (r_{ik} - 1)a_k - a_i, (c_k - 1)a_k + (r_{ij} - 1)a_j - a_i\} =$$

$$\max\{c_j a_+ r_{ik} a_k, c_k a_k + r_{ji} a_j\} - \sum_{s=1}^{3} a_s.$$

I en aquest cas, pel lema 4.34, $r_{ij} > 0$ per a tot $i, j \in \{1, 2, 3\}$

Si $\{a_1, a_2, a_3\}$ no és un sistema de generadors minimal, aleshores S està generat per només dos elements, i per tant $a_i = \lambda a_j + \beta a_k$ per uns certs $\{i, j, k\} = \{1, 2, 3\}$. Si c_1, c_2, c_3 són els enters més petits tals que existeixen $r_{12}, r_{13}, r_{21}, r_{23}, r_{31}$ i r_{32} nombres naturals amb:

$$c_1 a_1 = r_{12} a_2 + r_{13} a_3,$$

$$c_2 a_2 = r_{21} a_1 + r_{23} a_3,$$

$$c_3 a_3 = r_{31} a_1 + r_{32} a_2.$$

Obtenim que $c_i = 1$, $r_{ij} = \lambda$ i $r_{ik} = \beta$, i suibstituint a_i per $\lambda a_j + \beta a_k$:

$$a_i = \lambda a_j + \beta a_k,$$

$$c_j a_j = r_{ji}(\lambda a_j + \beta a_k) + r_{jk} a_k,$$

$$c_k a_k = r_{ki}(\lambda a_j + \beta a_k) + r_{kj} a_j.$$

Que resulta:

$$a_i = \lambda a_j + \beta a_k,$$

$$(c_j - r_{ji}\lambda) a_j = (r_{ji}\beta + r_{jk}) a_k,$$

$$(c_k - r_{ki}\beta) a_k = (r_{ki}\alpha + r_{kj}) a_j,$$

amb $(c_j - r_{ji}\lambda)$ i $(c_k - r_{ki}\beta)$ positius i més petits que c_j i c_k relativament.
Per tant, el sistema amb c_1, c_2, c_3 sent són els enters més petits tals que és:

$$a_i = \lambda a_j + \beta a_k,$$

$$c_j a_j = r_{jk} a_k$$

$$c_k a_k = r_{kj} a_j$$

Si ens fixem en la segona igualtat, i fem classes d'equivalència mod a_k, amb a_j sent coprimer amb a_k, obtenim que $c_j = sa_k$ i $r_{jk} = sa_j$. Imposant que són els més petits, obtenim que $c_j = a_k$ i $r_{jk} = a_j$. Fent el mateix procediment amb la tercera equació, veiem que $c_k = a_j$ i $r_{kj} = a_k$, i, juntament amb el corol·lari 4.22, obtenim que

$$F(a_1, a_2, a_3) = F(a_j, a_k) = a_j a_k - a_j - a_k = c_j a_j + c_i a_i - \sum_{s=1}^{3} a_s,$$

amb algun $r_{ij} = 0$, demostrant així el Teorema 3.5. □

Com a apunt, cal dir que hi ha una diferència molt gran de tractament un cas que l'altre. Aquesta diferenciació és deguda al tipus del semigrup. Es pot observar que el cas minimament generat el tipus és 2 i que en l'altre el tipus és 1. Aquest fet, que sembla a primeres anecdòtic, es repeteix molt al llarg de l'estudi de semigrups numèrics: depenent d'un tipus o un altre, els semigrups tenen propietats molt diferents.

A més de la demostració del Teorema 3.5, cal veure un resultat que necessitarem més endavant que és conseqüència del Lema 4.37.

Proposició 4.38. *Si a_1, a_2, a_3 formen un sistema de generadors minimal, aleshores*

$$\begin{aligned} a_1 &= r_{12}r_{13} + r_{12}r_{23} + r_{13}r_{32}, \\ a_2 &= r_{13}r_{21} + r_{21}r_{23} + r_{23}r_{31}, \\ a_3 &= r_{12}r_{31} + r_{21}r_{32} + r_{31}r_{32}. \end{aligned}$$

Demostració. Veurem que $a_1 = r_{12}r_{13} + r_{12}r_{23} + r_{13}r_{32}$ i per raonaments idèntics s'arriba a les altres dues conclusions.
Sabem que $\#Ap(S, a_1) = a_1$, i a partir del Lema 4.37 contem els elements que hi ha en aquest conjunt però per fer-ho observem abans que si $\lambda_2 a_2 + \lambda_3 a_3 = \beta_2 a_2 + \beta_3 a_3$ amb $\lambda_i, \beta_i \in \{0, \dots, c_i\}$ llavors $(\lambda_2, \lambda_3) = (\beta_2, \beta_3)$ per la minimalitat de c_2 i c_3. Veiem aquest raonament més detingudament:
Si $\lambda_2 a_2 + \lambda_3 a_3 = \beta_2 a_2 + \beta_3 a_3$ aleshores $(\lambda_2 - \beta_2)a_2 = (\beta_3 - \lambda_3)a_3$ i o bé $\lambda_2 - \beta_2 > 0$ o bé $\lambda_2 - \beta_2 < 0$ o bé $\lambda_2 - \beta_2 = 0$ i tant el primer com el segon cas entrarien amb contradicció amb la definició de c_2.

$$\#Ap(S, a_1) = \#\{(\alpha, \beta) \in \mathbb{N}^2 \mid (\alpha, \beta) \leq (r_{12} - 1, c_3 - 1) \,\text{o}\, (\alpha, \beta) \leq (c_2 - 1, r_{13} - 1)\}.$$

Sabent que

$$\begin{aligned} \#\{(\alpha, \beta) \in \mathbb{N}^2 \mid (\alpha, \beta) \leq (r_{12} - 1, c_3 - 1)\} &= r_{12}c_3, \\ \#\{(\alpha, \beta) \in \mathbb{N}^2 \mid (\alpha, \beta) \leq (c_2 - 1, r_{13} - 1)\} &= c_2 r_{13}. \\ \#\{(\alpha, \beta) \in \mathbb{N}^2 \mid (\alpha, \beta) \leq (c_2 - 1, r_{13} - 1) \,\text{i}\, (\alpha, \beta) \leq (c_2 - 1, r_{13} - 1)\} &= \\ = \#\{(\alpha, \beta) \in \mathbb{N}^2 \mid (\alpha, \beta) \leq (r_{12} - 1, r_{13} - 1)\} &= r_{12}r_{13}, \end{aligned}$$

ja que $c_2 > r_{12}$ i $c_3 > r_{13}$, obtenim que

$$\#Ap(S, a_1) = r_{12}c_3 + c_2 r_{13} - r_{12}r_{13}.$$

Fent servir el Lema 4.36 obtenim que $a_1 = r_{12}r_{13} + r_{12}r_{23} + r_{13}r_{32}$ i de forma equivalent les altres dues equacions. □

4.4 Càlcul d'alguns nombres de Frobenius usant semigrups numèrics

En aquesta secció es treballaran alguns casos particulars del nombre de Frobenius usant els semigrups numèrics i les seves propietats.

Davison [9] al 1992, trobà la següent cota inferior de $F(a_1, a_2, a_3)$. De fet, ell estudiava $G(a_1, \ldots, a_n)$, que és l'enter més gran no representable positivament per $a_1, \ldots, a_n$, és a dir, que no existeixen $\lambda_1, \ldots, \lambda_n > 0$ tal que $G(a_1, \ldots, a_n) = \lambda_1 a_1 + \ldots + \lambda_n a_n$. Es pot veure fàcilment que

$$G(a_1, \ldots, a_n) = F(a_1, \ldots, a_n) + a_1 + \ldots + a_n.$$

Teorema 4.39. *Siguin a_1, a_2, a_3 enters tals que $\gcd(a_1, a_2, a_3) = 1$. Aleshores,*

$$F(a_1, a_2, a_3) \geq \sqrt{3}\sqrt{a_1 a_2 a_3} - a_1 - a_2 - a_3.$$

Lema 4.40. *Sigui $T = \{(x, y, z, w) : x, y, z, w \geq 0; xw + xy + zy = 1\} \subset \mathbb{R}^4$. Si considerem $H : T \longrightarrow \mathbb{R}$ definida per $H(x, y, z, w) = x + y + \max(z, w)$. Llavors*

$$\min_{(x,y,z,w)\in T} H(x, y, z, w) \geq \sqrt{3}.$$

Demostració. Si $\max(x, y, z, w) > 2$ aleshores $H(x, y, z, w) > 2 > \sqrt{3}$. Definim $M = S \cap \{(x, y, z, w) : \max(x, y, z, w) \leq 2\}$, i per tant M és un compacte a $\mathbb{R}^4$. Demostrarem que

$$\min_{(x,y,z,w)\in M} H(x, y, z, w) = \sqrt{3}.$$

Sigui $M_1 = M \cap (z \leq w)$ i $M_2 = M \cap (z \leq w)$, aleshores M_1 i M_2 són compactes i

$$\min_M H = \min(\min_{M_1} H, \min_{M_2} H).$$

A M_1, la funció H és la funció lineal $x + y + w$, i per tant els seus extrems estan a la seva frontera, ∂M_1:

En $x = 0$: Veiem que $\min H = \min(y + w : zy = 1) \geq \min(y + z : zy = 1)$, doncs $w \geq z$. Si $zy = 1$, aleshores $\min(y + z : z = 1/y) = \min\{f(y) = y + 1/y, 0 < y \leq 2\}$. Derivant $f(y)$, igualant a zero i comparant en els extrems, s'obté que el mínim de $f(y)$ és 2. Per tant, $\min H \geq 2$.

En $y = 0$: Veiem que $\min H = \min(x + w : xw = 1)$. Fent serivr l'últim apartat, estudiant $f(x) = x + 1/x$, obtenim que $\min H = 2$.

En $z = 0$: Veiem que $\min H = \min(x + y + w : x(y + w) = 1)$. Podem tornar a definir $f(t) = t + 1/t$, on $t = (y + w)$, amb $t \in (0, 4]$. I també, el seu mínim és 2.

En $w = 0$: En aquest cas, $z = 0$, i $\min H = \min(x + y : xy = 1) = 2$, el raonament és equivalent que el del cas $y = 0$.

En $z = w$: Veurem que $\min H = \min(x+y+z : xz+xy+zy = 1) = \sqrt{3}$. Aplicant els multiplicadors de Lagrange:

$$\Delta(x, y, z, \lambda) = x + y + z - \lambda(xz + xy + zy - 1)$$

i

$$\begin{aligned}\partial_x\Delta &= 1 - \lambda z - \lambda y = 0\\ \partial_y\Delta &= 1 - \lambda x - \lambda z = 0\\ \partial_z\Delta &= 1 - \lambda x - \lambda y = 0\\ \partial_\lambda\Delta &= xz + xy + zy - 1 = 0.\end{aligned}$$

De les tres primeres equacions obtenim que $\lambda \neq 0$ i

$$x = y = z = \frac{1}{2\lambda},$$

i per tant

$$\frac{1}{4\lambda^2} + \frac{1}{4\lambda^2} + \frac{1}{4\lambda^2} = 1 \Longrightarrow \lambda = \frac{\sqrt{3}}{2} \Longrightarrow x = y = z = \frac{1}{\sqrt{3}}$$

i així $\min H = \min(x + y + z : xz + xy + zy = 1) = \sqrt{3}$.

El cas de M_2 és el mateix raonament intercanviant la z per la w, obtenint així que

$$\min_M H = 2.$$

□

Demostració del Teorema 4.39. Definim

$$\Theta(a_1, a_2, a_3) = \frac{F(a_1, a_2, a_3) + a_1 + a_2 + a_3}{\sqrt{a_1a_2a_3}}.$$

L'objectiu d'aquesta demostració serà veure que $\Theta(a_1, a_2, a_3) \geq \sqrt{3}$.
En el cas que $\gcd(a_1, a_2) = d > 1$, definim $a_1' = a_1/d$ i $a_2' = a_2/d$ i per la proposició 4.23:

$$\Theta(a_1, a_2, a_3) = \frac{dF(a_1', a_2', a_3) + (d-1)a_3 + a_1 + a_2 + a_3}{\sqrt{a_1a_2a_3}} =$$

$$= \frac{d(F(a_1', a_2', a_3) + a_1' + a_2' + a_3)}{d\sqrt{a_1'a_2'a_3}} = \Theta(a_1', a_2', a_3).$$

El mateix passa si $\gcd(a_1, a_3) = d > 1$ i $\gcd(a_2, a_3) = d > 1$. Així podem suposar que a_1, a_2, a_3 són coprimers dos a dos i $a_1 < a_2 < a_3$, per tant podem aplicar el Teorema 3.5.
Suposem que a_3 és expressable com a sumes positives de a_1 i a_2. Aleshores,

$$\Theta(a_1, a_2, a_3) = \frac{a_1a_2 + a_3}{\sqrt{a_1a_2a_3}}.$$

Veiem que en aquest cas $\Theta(a_1, a_2, a_3) \geq 2$:

$$\begin{aligned}\Big(\frac{a_1a_2 + a_3}{2}\Big)^2 - a_1a_2a_3 &= \frac{1}{4}(a_1^2a_2^2 + 2a_1a_2a_3 + a_3^2) - a_1a_2a_3 \\ &= \frac{1}{4}(a_1^2a_2^2 - 2a_1a_2a_3 + a_3^2) = \Big(\frac{a_1a_2 - a_3}{2}\Big)^2 \geq 0\end{aligned}$$

i per tant

$$\frac{a_1a_2 + a_3}{\sqrt{a_1a_2a_3}} \geq 2.$$

Com a curiositat, aquesta desigualtat és la famosa desigualtat de la mitjana aritmètica i geomètrica.
Suposem que a_1, a_2, a_3 són un sistema de generadors minimal. En aquest cas, aplicant el Teorema 3.5:

$$\Theta(a_1, a_2, a_3) = \max\Big(\frac{c_2a_2 + r_{13}a_3}{\sqrt{a_1a_2a_3}}, \frac{c_3a_3 + r_{12}a_2}{\sqrt{a_1a_2a_3}}\Big),$$

on c_i, r_{kj} són els definits en el mateix Teorema.
Per la proposició 4.38 i el lema 4.36,

$$a_1 = r_{12}r_{13} + r_{12}r_{23} + r_{13}r_{32} = c_2c_3 - r_{32}r_{23}. \tag{4.1}$$

Definim

$$\begin{aligned}\alpha_1 &= c_2\sqrt{\frac{a_2}{a_1a_3}}, \\ \alpha_2 &= r_{32}\sqrt{\frac{a_2}{a_1a_3}}, \\ \beta_1 &= r_{23}\sqrt{\frac{a_3}{a_1a_2}}, \\ \beta_2 &= c_3\sqrt{\frac{a_3}{a_1a_2}}.\end{aligned}$$

De $c_2a_2 = r_{21}a_1 + r_{23}a_3$, obtenim que $c_2a_2 > a_3r_{23}$ (pel lema 4.34), i per tant $\alpha_1 > \beta_1$.
Per un raonament equivalent, $\beta_2 > \alpha_2$.
D'aquí, definim

$$\epsilon_i = \alpha_i - \beta_i$$

amb i sent 1 o 2.
De l'equació 4.1, $\alpha_1\beta_2 - \alpha_2\beta_1 = \epsilon_1\alpha_2 + \epsilon_1\epsilon_2 + \beta_1\epsilon_2 = 1$.
Reescrivim $\Theta(a_1, a_2, a_3) = \Theta(\epsilon_1, \epsilon_2, \alpha_2, \beta_3) = \epsilon_1 + \epsilon_2 + \max(\alpha_2, \beta_2)$ i pel Lema 4.40,

$$\Theta(a_1, a_2, a_3) \geq \sqrt{3}.$$

□

De fet, $\sqrt{3}$ és la millor constant que hi pot haver, ja que al calcular

$$F(3,3k{+}1,3k{+}2) = \max\{2(3k{+}1){+}1(3k{+}2),(2k{+}1)3{+}1(3k{+}2)\}{-}3{-}3k{-}1{-}3k{-}2$$

$$= 3k-1$$

doncs $c_2 = 2$, $r_{13} = 1$, $c_1 = 2k+1$ i $r_{23} = 1$.

I calculant

$$\lim_{k\to\infty} \frac{F(3,3k+1,3k+2)+3+3k+1+3k+2}{\sqrt{3(3k+1)(3k+2)}} = \lim_{k\to\infty} \frac{9k+5}{\sqrt{3(3k+1)(3k+2)}} = \sqrt{3}.$$

La següent proposició [8] dona el nombre de Frobenius de tres nombres naturals que compleixen unes hipòtesis molt específiques.Aquesta serà necessària per a la demostració del teorema 3.3.

Proposició 4.41. *Sigui $S = \langle s_1, s_2, s_3\rangle$, amb $2 < s_1 < s_2 < s_3$ i k tals que:*

i) $2 \leq k \leq \frac{s_1-1}{2} + 1$

ii) $s_1 - k < \frac{s_3}{s_2} < s_1 - k + 1$

iii) $s_2 \equiv 1 \mod s_1$

iv) $s_3 \equiv s_1 - k + 1 \mod s_1$.

Aleshores, $F(s_1,s_2,s_3) = (k-2)s_2 + s_3 - s_1$.

Demostració. Comencem veient que $(k-2)s_2 + s_3 \in Ap(S,s_1)$.
Multiplicant **iii)** per k i sumant-li **iv)**, obtenim que $ks_2 + s_3 \equiv s_1 + 1 \mod s_1$.
Restant $2 \equiv 2s_2 \mod s_1$ a cada costat, $(k-2)s_2 + s_3 \equiv s_1 - 1 \mod s_1$.
Suposem que $(k-2)s_2 + s_3 \notin Ap(S,s_1)$, és a dir, que existeixen a i b positives tals que

$$as_2 + bs_3 \equiv (k-2)s_2 + s_3 \mod s_1$$

amb $as_2 + bs_3 < (k-2)s_2 + s_3$.
Per casos en b, arribarem a una contradicció.

Si $b = 0$

$$as_2 \equiv s_1 - 1 \mod s_1 \Longrightarrow a \equiv s_1 - 1 \mod s_1 \Longrightarrow a \geq s_1 - 1$$

i per tant

$$(s_1-1)s_2 < (k-2)s_2 + s_3 \Longrightarrow s_2s_1 - s_2 - ks_2 < -2s_2 + s_3 \Longrightarrow s_1 + 1 - k < \frac{s_3}{s_2}$$

contradient **ii)**.

Si $b = 1$

$$as_2 + s_3 \equiv (k-2)s_2 + s_3 \mod s_1 \Longrightarrow a \equiv (k-2) \mod s_1$$

i com que d'**i)** obtenim que $k - 2 < k < s_1$ i per tant $a \geq k - 2$,

$$\Longrightarrow as_2 + s_3 \geq (k-2)s_2 + s_3$$

entrant amb contradicció amb la definició de a i b.

Si $b \geq 2$ observem que si $2s_3 \leq as_2 + bs_3 < (k-2)s_2 + s_3 \Longleftrightarrow s_3/s_2 < k - 2$.
I per **ii)**, obtenim que $s_1 - k < s_3/s_2 < k - 2$.
Per tant, $s_1 - k < k - 2 \Longrightarrow (s_1 + 2)/2 < k$, entrant en contradicció, ja que $(s_1 - 1)/2 + 1 = (s_1 + 2)/2 - 3/2 < (s_1 + 2)/2 < k$, contradient **i)**.

Per tant, $(k-2)s_2 + s_3 \in Ap(S, s_1)$. Veiem ara que és el seu màxim. Ho veurem per tots els possibles residus mod s_1, que anomenarem m.

Si $m \in \{0, \ldots, s_1 - k\}$ com que $s_3/s_2 > s_1 - k \geq m$, aleshores $s_3 > ms_2 \Longrightarrow$ $(k-2)s_2 + s_3 > ms_2$, amb $ms_2 \in S$ i $ms_2 \equiv m \mod s_1$.

Si $m \in \{s_1 - k, \ldots, s_1 - 2\}$ a partir de **iv)**, $s_3 \equiv s_1 - k + 1 \mod s_1 \Longrightarrow$

$$(m - (s_1 - k + 1))s_2 - s_3 \equiv m \mod s1$$

i veient que $(m - (s_1 - k + 1))s_2 - s_3 < k - 2$ ja que $m \in \{s_1 - k, \ldots, s_1 - 2\}$.

Obtenim que $F(s_1, s_2, s_3) = (k-2)s_2 + s_3 - s_1$. □

En aquest capítol s'ha introduït un conjunt de resultats i d'eines bàsiques per a l'estudi del nombre de Frobenius. Com que moltes d'aquestes apareixen de forma natural al plantejar-nos el problema de Frobenius, al llarg d'aquesta memòria tornaran a sorgir moltes d'elles. En aquest capítol també s'ha pogut comprovar la diferència de dificultat entre el càlcul del cas $n = 2$ al cas $n = 3$.

5 Sobre la fórmula del nombre de Frobenius

Hem vist al capítol 3 el següent resultat que impossibilita trobar fórmules pel nombre de Frobenius si n és més gran o igual a 3:

Teorema 3.3. *Sigui* $A = \{(s_1, s_2, s_3) \in \mathbb{N}^3 \mid s_1 < s_2 < s_3,\ s_1 \text{ i } s_2 \text{ són primers, i } s_i \nmid s_3 \text{ per } i = 1, 2\}$. *Llavors, no existeix cap polinomi diferent de zero* $f \in \mathbb{C}[X_1, X_2, X_3, Y]$ *tal que* $f(s_1, s_2, s_3, F(s_1, s_2, s_3)) = 0$ *per a tot* $(s_1, s_2, s_3) \in A$.

L'objectiu d'aquest capítol és donar una demostració d'aquest Teorema, un resultat que es donà demostrat per primera vegada el 1990 per Frank Curtis [8], on aquí s'exposa una explicació detallada d'aquesta.

Per fer-ho, abans s'hauran de veure uns resultats previs, així com una petita introducció de les eines que es faran servir.

Lema 5.1. *Siguin* $\{x_n\}_n$ *i* $\{y_n\}_n$ *dues successions als* $\mathbb{N}$ *i* α *un nombre irracional qualsevol tal que*

$$\frac{y_n}{x_n} \longrightarrow \alpha$$

aleshores $x_n \longrightarrow \infty$ *i* $y_n \longrightarrow \infty$.

Demostració. Sigui $a \in \mathbb{N}$ tal que $\#\{n \mid x_n = a\}$ és infinit i $b \in \mathbb{N}$ tal que $\#\{n \mid y_n = b\}$ és infinit.
Si a no existeix, llavors $x_n \longrightarrow \infty$.
Si b no existeix, llavors $y_n \longrightarrow \infty$.
Veurem que no poden existir ni a ni b.
Si tant a com b existissin, llavors considerem les successions parcials:

$$x_{\sigma(n)} = a,\ y_{\varphi(n)} = b,$$

i

$$z_{\psi(n)} = \frac{y_{\varphi(n)}}{x_{\sigma(n)}}.$$

Com que $z_n = \frac{y_n}{x_n}$ té el mateix límit que $z_{\psi(n)}$, aleshores

$$z_{\psi(n)} = \frac{y_{\varphi(n)}}{x_{\sigma(n)}} \longrightarrow \frac{b}{a} = \alpha$$

contradient que α sigui irracional.
I si a existís i b no, llavors

$$\frac{y_n}{x_n} \longrightarrow \infty.$$

I si b existís i a no, llavors

$$\frac{y_n}{x_n} \longrightarrow 0,$$

contradient que $\alpha = 0$ sigui irracional. □

Sigui I un ideal a $\mathbb{C}[X_1, \ldots, X_n]$. Anomenem varietat algebraica de I al conjunt:

$$\mathcal{V}(I) = \{p \in \mathbb{C}^n | f(p) = 0 \forall f \in I\}.$$

En aquest capítol es farà l'abús de notació següent:

$$\mathcal{V}(f) = \mathcal{V}(\langle f \rangle).$$

I de forma recíproca, sigui X un subconjunt de $\mathbb{C}^n$, anomenem .... al ideal I:

$$I(X) = \{f \in \mathbb{C}[X_1, \ldots, X_n] | f(p) = 0 \forall p \in X\}.$$

Veure que $I(X)$ és un ideal és un resultat trivial. D'aquí farem servir el següent resultat:

Proposició 5.2. *Si X i Y són dos subconjunts de $\mathbb{C}^n$, aleshores:*

$$X \subseteq Y \Longrightarrow I(Y) \subseteq I(X)$$

Demostració. Siguin X i Y dos subconjunts de $\mathbb{C}^n$ tals que $X \subseteq Y$ i sigui $f \in I(Y)$. Si $p \in X$, aleshores, com $p \in Y$, $f(p) = 0$, i per tant, $f \in I(X)$. □

Sigui $\mathbb{K}$ un cos i f un polinomi $f \in \mathbb{K}[X_1, \ldots, X_n]$, la homogeneïtzació de f en $\mathbb{K}[X_1, \ldots, X_n, Y]$ és un polinomi $f^* \in \mathbb{K}[X_1, \ldots, X_n, Y]$ que apareix al multiplicar cada monomi X^d de f, amb $d = (d_1, \ldots, d_n)$, per Y^r on $r = \deg f - d_1 - \ldots - d_n$. Cal dir que tots els monomis de f^* tenen el mateix grau i coincideix amb el de f.

Exemple 5.3. Si $f(X, Y) = X^3 + XY + Y^2 + Y$ amb coordenades reals, la seva homogeneïtzació respecte a Z en $\mathbb{R}[X, Y, Z]$ és el polinomi $f^*(X, Y, Z) = X^3 + XYZ + Y^2Z + YZ^2$.

Observació 5.4. Un resultat directe de la definició de polinomis homogeneïtzats, és que si f^* és un polinomi homogeneïtzat d'un altre polinomi f respecte Z, llavors:

$$Z \mid f^* \Longleftrightarrow f = 0.$$

La proposició 5.2 i la observació 5.4 també són vàlides per l'espai projectiu $\mathbb{PC}^n$ amb polinomis homogeneitzats, que és el que farem servir a la demostració del teorema.

També usarem els següents resultats de varietats algebraiques:

Lema 5.5. *Sigui f un polinomi $f \in \mathbb{C}[X_1, \ldots, X_n]$ tal que s'anula en un nombre r d'hiperplans diferents, llavors* $\deg f \geq r$.

Lema 5.6. *Sigui $\mathcal{V}(f_1, \ldots, f_s)$ una varietat algebraica a $\mathbb{C}[X_1, X_2]$ que conté un segment de la forma $(s, 0)$, amb $s \in (a, b)$ d'una recta r, aleshores $\mathcal{V}(f_1, \ldots, f_s)$ conté la recta r.*

Una successió de Farey d'ordre n és una successió de fraccions irreductibles entre 0 i 1 que tenen un denominador menor o igual a n en ordre creixent. Cada successió de Farey comença pel $0/1$ i acaba pel $1/1$. Per a una explicació més detallada d'aquesta, es recomana [1].

Un resultat interessant d'aquestes successions és que dos elements a/b i c/d són consecutius si i només si la seva diferència és $1/bd$, és a dir, si $ad - bc = 1$.

A més, per a tot $\varepsilon > 0$ proposat, existeix una n tal que per a tot parell d'elements consecutius a/b i c/d de la successió de Farey d'ordre n, $|a/b - c/d| < \varepsilon$.

En la demostració del següent lema, usarem diverses vegades el famós Teorema de Dirichlet de progressions aritmètiques, que diu el següent:

Teorema 5.7 (Teorema Dirichlet)**.** *Siguin a i d dos nombres coprimers entre ells, aleshores la progressió aritmètica $a_n = a + n \cdot d$ conté infinits nombres primers.*

Lema 5.8. *Siguin $\alpha \in \mathbb{R}^+$, $\varepsilon > 0$, p un nombre primer i i i j dos nombres naturals donats tals que $\gcd(p, i) = \gcd(p, j) = 1$, aleshores existeixen x i y tal que:*

i) *x primer*

ii) $\gcd(x, y) = 1$

iii) $x \equiv i \mod p$ *i* $y \equiv j \mod p$

iv) $|\alpha - \frac{y}{x}| < \varepsilon$.

Demostració. Siguin q/r i s/t dos elements consecutius de la successió de Farey per n suficient petita tal que ambdós pertanyin en $[0, 1] \cap (-\varepsilon, \varepsilon)$.
Per tant, $|rs - qt| = 1$.
Veiem que:

$$\alpha + \frac{q}{r} = \frac{r\alpha + q}{r}$$

i

$$\alpha + \frac{s}{t} = \frac{t\alpha + s}{t}$$

pertanyen a $(\alpha - \varepsilon, \alpha + \varepsilon)$.
Definim a i b de la següent manera:

$$a = r\alpha + q$$

$$b = t\alpha + s$$

i veiem que $|rb - at| = |r\alpha t + rs - tr\alpha - qt| = |rs - qt| = 1$.
Considerem el següent sistema d'equacions a $\mathbb{Z}/p\mathbb{Z}$:

$$rU + tV \equiv i \mod p$$

$$aU + bV \equiv j \mod p$$

que té solució doncs hem vist que $|rb - at| = 1$ i per la definició de i i j aquesta és diferent a $\begin{bmatrix}0\\0\end{bmatrix}$.
Siguin u i v enters positius tals que $u \equiv U \mod p$ i $v \equiv V \mod p$.
Si $p \mid u$, fem el canvi:

$$\frac{a}{b} \longleftrightarrow \frac{b}{t}$$

per tal que $p \nmid u$ (que el podem fer doncs $\begin{bmatrix}0\\0\end{bmatrix}$ no és solució).
Per tant, podem suposar que $\gcd(p, u) = 1$, i per tant podem aplicar el Teorema de Dirichlet escollint una k tal que $u' = kp + u$ és primer, amb $u' > \max(v, t)$. I per tant, $\gcd(u', v) = 1$.
Considerem ara $ru' + tv$, que mod p és equivalent a $ru + tv \equiv i \mod p$, i per tant $\gcd(p, ru' + tv) = (p, i) = 1$. Observem que de $|at - rb| = 1$ i Bezout, obtenim que $\gcd(t, r) = 1$.
A més a més, de que $u' > \max(v, t)$, obtenim que $\gcd(t, u') = 1$ i $\gcd(u', v) = 1$. Per tant,

$$\gcd(u', ru' + tv) = (t, ru') = (t, r) = 1$$

$$\gcd(u', ru' + tv) = (u', tv) = (u', t) = 1.$$

I d'aquí obtenim que $\gcd(ptu', ru' + tv) = 1$.
Tornant a aplicar el Teorema de Dirichlet, obtenim que $\exists k_2$ tal que $ru' + tv + k_2ptu'$ és primer.
I considerant $v' = v + k_2pu'$, definint

$$x = ru' + tv'$$

$$y = au' + bv',$$

obtenim la x i la y que satisfan el lema:

i) $x = ru' + tv' = ru' + tv + k_2ptu'$ és primer.

iii) $x \equiv ru' + tv' \equiv ru + tv \equiv i \mod p$ i $y \equiv au' + bv' \equiv j \mod p$.

iv) $|\alpha - y/x| < \varepsilon$:

$$\frac{y}{x} = \frac{(r\alpha + q)u' + (\alpha t + s)v'}{ru' + tv'} = \alpha\frac{ru' + tv'}{ru' + tv'} + \frac{qu' + sv'}{ru' + tv'} = \alpha + A_n$$

on A_n és un nombre que pertany a $(-\varepsilon, \varepsilon)$, ja que si $q/r < s/t$:

$$\frac{q}{r} = \frac{qu'}{ru'} < \frac{qu' + sv'}{ru' + tv'} < \frac{sv'}{tv'} = \frac{s}{t},$$

i si $s/t < q/r$ obtenim també $A_n \in (-\varepsilon, \varepsilon)$.

ii) com que x és primer, si $x \mid y$, aleshores $y/x = t \in \mathbb{Z}$, contradient **iv)**.

I així hem demostrat el lema. □

Per a la demostració, també usarem la proposició 4.41.

La idea general de la demostració consisteix en veure que si aquest polinomi f existís, llavors per a tot p primer $f(p, X_2, X_3, (k-2)X_2 + X_3 - p) = 0$ per a tota $2 \leq k \leq (p-1)/2$, per després veure que $\deg f \geq (p-1)/2$, per a tot p primer, arribant així a una contradicció.

Demostració del Teorema. Suposem que el polinomi f existeix, siguin p un nombre primer i k un nombre tal que $2 \leq k \leq (p-1)/2 + 1$, definim $G(X_2, X_3) = f(p, X_2, X_3, (k-2)X_2 + X_3 - p)$. Veurem primerament que $G(X_2, X_3) = 0$.
Sigui $\alpha \in (p-k, p-k+1)$ un irracional, per $n = 1, 2, 3, ...$ escollim pel Lema 5.8 $x_n \equiv 1 \mod p$, $y_n \equiv p-k+1 \mod p$, amb x_n primer, $\gcd(x_n, y_n) = 1$ i $|\alpha - y_n/x_n| < 1/n$.
Veiem que $(p, x_n, y_n) \in A$, ja que x_n és primer, $y_n \nmid p$, doncs $y_n \equiv p-k+1 \mod p$, i com que $y_n/x_n > p-k-1 > 1$, obtenim que $y_n > x_n$. Per aplicar el Lema 5.8, només queda veure que

$$p - k < \frac{y_n}{x_n} < p - k + 1,$$

que s'obté fent servir que $\alpha \in (p-k, p-k+1) \Rightarrow \exists n_0 \mid y_n/x_n \in (p-k, p-k+1)$ $\forall n > n_0$, ja que $|\alpha - y_n/x_n| < 1/n$.
Obtenim que a partir de n_0 per la proposició 4.41:

$$F(p, x_n, y_n) = (k-2)x_n + y_n - p$$

i per la definició de f:

$$G(x_n, y_n) = f(p, x_n, y_n, (k-2)x_n + y_n - p) = 0 \ \forall n > n_0,$$

Sigui $G^*(X_2, X_3, Y)$ la homogeneització del polinomi G respecte Z a $\mathbb{C}[X_2, X_3, Y]$. Lavors, $G^*(x_n, y_n, 1) = 0$, que dividint cada terme de G^* per

$$x_n^{\deg G}$$

obtenim que $G^*(1, y_n/x_n, 1/x_n) = 0$, i com que G és una aplicació contínua, podem aplicar el límit quan $n \longrightarrow \infty$, i pel Lema 5.1, obtenim que:

$$G^*(1, \alpha, 0) = 0 \ \forall \alpha \in (p-k, p-k+1) \text{ irracional.}$$

Considerem ara la corba projectiva $\mathcal{V}(G^*)$, que com acabem de veure, conté infinits punts de la forma $[1 : \alpha : 0]$, amb $\alpha \in (p-k, p-k+1)$ irracional. Per continuïtat, $\mathcal{V}(G^*)$ conté el segment $[1 : r : 0]$, amb $r \in (p-k, p-k+1)$ real. Per tant, també conté la recta $[1 : r : 0]$ $\forall r \in \mathbb{R}$, que és la mateixa que és $\mathcal{V}(Z) = [1 : z : 0]$ $\forall z \in \mathbb{C}$, ja que si $[1 : r : 0]$ per r reals és solució del polinomi G^*, també ho és per r complexos. És a dir, $\mathcal{V}(Z) \subseteq \mathcal{V}(G^*) \Longrightarrow \langle G^* \rangle \subseteq \langle Z \rangle$, per la proposició 5.2, i per tant $Z \mid G^*$.
Però G^* és la homogeneïtzació d'un polinomi respecte Z, per tant $G^*(X_2, X_3, Z) = G(X_2, X_3) = f(p, X_2, X_3, (k-2)X_2 + X_3 - p) = 0$.
Fixat un primer p senar. Sigui $H(X_2, X_3, Y) = f(p, X_2, X_3, Y)$, i $H^*(X_2, X_3, Y, Z)$

la seva homogeneïtzació respecte a Z a $\mathbb{C}[X_2, X_3, Y, Z]$.
Veiem que $H^*(q) = 0$ per a tot q que pertany als hiperplans $\mathcal{V}((k-2)X_2 + X_3 - Y - pZ)$ per $k = 2, \ldots, (p+1)/2 + 1$: sigui $q = (q_1, q_2, q_3, q_4)$ tal que pertany al hiperplà $(k-2)X_2 + X_3 - Y - pZ = 0$:

$$\Longrightarrow q_3 = (k-2)q_1 + q_2 - pq_4.$$

Calculem $H^*(q_1, q_2, q_3, q_4)$:

$$H^*(q_1, q_2, q_3, q_4) = H^*(q_1/q_4, q_2/q_4, (k-2)q_1/q_4 + q_2/q_4 - p, 1) =$$

$$= H(q_1/q_4, q_2/q_4, (k-2)q_1/q_4 + q_2/q_4 - p) = f(p, q_1/q_4, q_2/q_4, (k-2)q_1/q_4 + q_2/q_4 - p)$$
$$= 0,$$

com havíem vist a la primera part de la demostració.
Per tant, H^* és 0 per als hiperplans $(k-2)X_2 + X_3 - Y - pZ = 0$ per a $k = 2, \ldots, (p-1)/2+1$, i pel Lema 5.8 obtenim que $\deg f \geq \deg H^* = \deg H \geq (p-1)/2$ per a tot primer $p > 2$, arribant a una contradicció. □

Així veiem que no hi ha cap conjunt finit de polinomis $\{f_1, \ldots, f_n\}$ tal que per a tot trio (s_1, s_2, s_3) hi ha alguna i tal que $f_i(s_1, s_2, s_3) = F(s_1, s_2, s_3)$.

Observem també el ventall d'àmbits de les matemàtiques que s'han usat per a demostrar aquest teorema.

6 Sèrie de Hilbert i denumerant de Sylvester

Una altra manera d'estudiar el nombre de Frobenius completament diferent de la que hem fet fins ara és amb la mirada posada sobre les sèries de Hilbert.

La importància d'aquest capítol recau en el fet que es presenta una teoria que permet trobar de forma directa el nombre de Frobenius, sense cap hipòtesi addicional. Tot i que el càlcul d'aquest usant els elements que es presentaran aquí pot resultar complicat, sí que s'han trobat molts resultats importants d'aquest nombre a partir de les sèries de Hilbert.

Per començar, presentarem la teoria de l'àlgebra de mòduls graduats, successions exactes de mòduls graduats i sèries de Hilbert, i, introduint el concepte de denumerant de Sylvester, veurem la relació d'aquestes últimes amb el nombre de Frobenius, doncs aquest és el grau de la funció racional donada per una sèrie de Hilbert. Finalment, es veurà un exemple d'aquest càlcul en tornar a demostrar el Teorema 3.5.

La línia de treball d'aquest capítol està extreta de [18], però aquí aquesta s'ha estudiat més en detall.

6.1 Mòduls graduats, successions exactes i sèries de Hilbert

Sigui R un anell, un mòdul M sobre un anell R és un conjunt amb una operació binària i una operació de R a M que satisfà les següents propietats:

- M és un grup abelià amb l'operació binària
- Per a tot $a \in R$ i per a tot $f, g \in M$, $a(f+g) = af + ag$
- Per a tot $a, b \in R$ i per a tot $f \in M$, $(a+b)f = af + bf$
- Per a tot $a, b \in R$ i per a tot $f \in M$, $(ab)f = a(bf)$
- Si 1 és la identitat amb la multiplicació a R, llavors $1f = f$ per a tot $f \in M$.

No cal dir que la importància dels mòduls com a àlgebra va molt més enllà de la que se li donarà aquí. En aquest capítol s'estudiaran exclusivament els mòduls graduats, doncs a partir d'aquests s'arriben als resultats presentats.

Diem que un anell R és positivament graduat si es pot escriure R com a suma directa (com a grup abelià) de la forma:

$$R = \bigoplus_{i=0}^{\infty} R_i$$

tal que per a tots els enters $m, n \geq 0$, es compleix que $R_n R_m \subseteq R_{n+m}$. En particular, R_0 és un subanell i que cada component A_i és un mòdul sobre A_0.

Aquesta definició es pot traslladar als mòduls de la següent manera: un mòdul M és graduat si es pot escriure com a suma directa de la forma:

$$M = \bigoplus_{i \in \mathbb{Z}} M_i$$

tal que per a tots els enters $m, n \geq 0$, es compleix que $R_n M_m \subseteq M_{n+m}$. Anomenarem als elements de M_n com a elements homogenis de $\deg n$.

Si M és finitament generat, llavors existeix una r tal que $M_i = 0$ per a tota $i < r$, ja que R és positivament graduat.

Exemple 6.1. Siguin $\mathbb{K}$ un cos, $X_0, \ldots, X_r$ variables indepedents. Si considerem l'anell polinomial graduat $\mathbb{K}[X_1, \ldots, X_r]$, on cada X_j té $\deg X_j = 1$, llavors els homogenis de $\deg n$ són els polinomis generats pels monomis de $\deg n$.

Es diu que M és un mòdul lliure si conté un conjunt R-linealment independent que el genera, és a dir, una base. El mòdul lliure R^m és un mòdul graduat si definim $(R^m)_t = (R_t)^m$.

Definim $M(d)$ com la regraduació de M si:

$$M(d) = \bigoplus_{i \in \mathbb{Z}} M(d)_i$$

on $M(d)_i = M_{d+i}$.

El mòdul graduat $R^m(d) = R(d)^m$ té la mateixa base que R^m, tot i així, com que $R(d)_{-d} = R_0$, aquesta base està formada pels homogenis de grau $-d$. Aquests mòduls de la forma $R(d)^m$ estan denominats mòduls lliures *shifted* graduats. Si $d_1, \ldots, d_m$ són enters, llavors:

$$M = R(d_1) \bigoplus R(d_2) \bigoplus \ldots \bigoplus R(d_m)$$

és un mòdul lliure graduat on la base són els homogenis de grau $-d_i$ per i de 1 a m.

Si M i N són mòduls graduats sobre un anell R, llavors

$$\psi : M \longrightarrow N$$

és un morfisme homogeni (de grau d) si ψ és un morfisme lineal sobre R i $\psi(M_i) \subseteq N_{i+d}$. Recordem que un morfisme ψ és un morfisme lineal si $\psi(af + bh) = a\psi(f) + b\psi(h)$ per a tot $a \in R$ i per a tot $f, h \in M$.

Exemple 6.2. Sigui $M = \mathbb{Z}[X, Y]$ i $N = \mathbb{Z}[X, Y, Z]$, considerem φ el morfisme d'anells tal que:

$$\begin{array}{rccc} \varphi : & M & \longrightarrow & N \\ & X & \longmapsto & Y^2 \\ & Y & \longmapsto & XZ \end{array}$$

i $\varphi(d) = d$ per a tot $d \in \mathbb{Z}$. φ és un morfisme homogeni de grau 2.

Exemple 6.3. Suposem que $M = \langle f_1, \ldots, f_m \rangle$ és un mòdul graduat on els polinomis f_i són homogenis amb $\deg f_i = d_i$, llavors el següent morfisme és homogeni de grau 0:

$$\phi: \quad R(-d_1) \bigoplus R(-d_2) \bigoplus \ldots \bigoplus R(-d_m) \quad \to \quad M,$$

on $\phi(e_i) = f_i$, amb e_i la base dels elements de R^m, però $\deg(e_i) = d_i$.

Vista tota aquesta introducció, podem per fi definir la funció i sèrie de Hilbert de la manera següent:

Definició 6.4. *Sigui M un mòdul graduat finitament generat sobre $R = \mathbb{K}[X_1, \ldots, X_n]$, llavors, la funció de Hilbert és:*

$$H_M(t) = \dim_{\mathbb{K}}(M_t),$$

on $\dim_{\mathbb{K}}$ sent la dimensió com a espai vectorial.

Com que és finitament generat, les dimensions de les peces homogènies de M com $\mathbb{K}$-espais vectorials són finites.

Definició 6.5. *Sigui M un mòdul graduat finitament generat sobre $R = \mathbb{K}[X_1, \ldots, X_n]$, llavors, la sèrie de Hilbert és:*

$$H(M, z) = \sum_{t \in \mathbb{Z}} H_M(t) z^t.$$

Com que el mòdul és finitament generat, la sèrie de Hilbert és una sèrie de Laurent.

Seguidament, veurem quina és la relació entre les sèries i funcions de Hilbert i les successions exactes.

Una resolució lliure graduada és aquella successió exacte:

$$\ldots \to F_2 \xrightarrow{\psi_2} F_1 \xrightarrow{\psi_1} F_0 \xrightarrow{\psi_0} M \to 0,$$

on cada F_i és un *shifted* R-mòdul lliure graduat, i els morfismes ψ_i són morfismes homogenis de grau 0.

El principal teorema que relaciona aquests dos conceptes, és el següent:

Teorema 6.6. *[5] Siguin $R = \mathbb{K}[X_1, \ldots, X_n]$ i M un R-mòdul graduat finitament generat. Llavors, per a tota resolució lliure de M graduada de la forma:*

$$0 \to F_m \to F_{m-1} \to \ldots \to F_0 \to M \to 0,$$

obtenim que

$$H_M(z) = \textstyle\sum_{j=0}^{m} (-1)^j H_{F_j}(z) \text{ i que } H(M, z) = \sum_{j=0}^{m} (-1)^j H(F_j, z).$$

Aquest teorema ens dona una eina molt útil per al càlcul de la sèrie de Hilbert, a canvi de la hipòtesi que ha d'existir una successió lliure graduada exacte amb aquella forma. Si bé pot semblar una hipòtesi molt estricta, amb el teorema 6.8 obtenim, no només l'existència d'aquesta, sinó una cota superior molt bona de la seva longitud. Per a la demostració del Teorema 6.6 introduirem el concepte de funció aditiva i usarem un lema.

Siguin C una família de R-mòduls, M, M', M'' R-mòduls i

$$0 \to M' \to M \to M'' \to 0$$

una successió exacte, llavors la funció

$$\lambda : C \to \mathbb{Z}$$

és aditiva si i només si $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

Lema 6.7. *Sigui* $0 \to M_0 \to \ldots \to M_n \to 0$ *una successió exacte de R-mòduls tals que tots els mòduls* M_i *i tots els* ker *de tots els homomorfismes pertanyen a* C*, llavors per a tota funció aditiva* λ *a* C *obtenim:*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$$

Demostració. Si separem la successió exacte $0 \xrightarrow{f_0} M_0 \xrightarrow{f_1} \ldots \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} 0$ en aquestes successions exactes més petites:

$$\begin{aligned}
M_0 &\to N_1 \to 0\,, \\
0 \to N_1 &\to M_1 \to N_2 \to 0\,, \\
&\vdots \\
0 \to N_{n-1} &\to M_{n-1} \to N_n \to 0\,, \\
0 \to N_n &\to M_n
\end{aligned}$$

on $N_i = \operatorname{im} f_i = \ker f_{i+1}$ per a tot i amb $N_0 = N_{n+1} = 0$, obtenim que $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$ i per tant al fer el càlcul $\sum_{i=0}^{n} (-1)^i \lambda(M_i)$ tots els termes es cancel·len i acaba sent igual a 0. □

Demostració del Teorema 6.6. Només queda veure que $\dim_{\mathbb{K}} M_t$ és una funció aditiva. Per a veure-ho, farem servir la idea que si f és un morfisme lineal d'un espai U, aleshores $\dim \ker f + \dim \operatorname{im} f = \dim U$.
Sigui la successió exacte

$$0 \to M'_t \xrightarrow{f} M_t \xrightarrow{g} M''_t \to 0$$

aleshores $\dim M''_t = \dim \operatorname{im} g$, doncs g és exhaustiva. I $\dim \ker g = \dim M'_t$, doncs $\ker g = \operatorname{im} f$, sent f injectiva. Per tant $\dim M_t = \dim \ker g + \dim \operatorname{im} g = \dim M'_t +$

dim M''_t demostrant així que dim és una aplicació additiva, aplicant el Lema 6.7 i agrupant tota la sèrie obtenim que:

$$H_M(z) = \sum_{j=0}^{m} (-1)^j H_{F_j}(z).$$

□

Teorema 6.8 ("Graded Hilbert Syzygy Theorem"). *Sigui $R = \mathbb{K}[X_1, \ldots, X_n]$. Llavors, tot R-mòdul graduat finitament generat té una successió lliure graduada amb longitud més petita o igual a n.*

Hi ha diverses demostracions d'aquest teorema. Aquí no se'n explicarà cap per falta d'espai, però sí que se'n donaran referències. A [6] es demostra primer el cas no graduat usant bases de Gröbner, i després s'extrapola al cas graduat. A [13] es demostra mitjançant el Complex de Koszul i àlgebra tensorial.

Amb aquest últim teorema es veu que el càlcul de la funció de Hilbert sempre és factible fent servir el teorema 6.6 doncs no només assegura l'existència de la successió exacte, sinó que en dona una bona cota superior de la longitud.

6.2 Denumerant de Sylvester

Recordem que $p(m)$ significa el nombre de possibles particions de m en sumes d'altres nombres naturals. La teoria de particions ha estat una teoria molt estudiada i treballada per grans matemàtics, des de Euler fins a l'actualitat. En aquesta secció, però, només ens interessa el nombre de particions de m en parts específiques, concepte que introduí Sylvester en [22] l'any 1857. Allà, definí $d(m; a_1, \ldots, a_n)$ com el nombre de particions de m per $a_1, \ldots, a_n$, per exemple:

$$d(12; 2, 3) = 3$$

doncs $12 = 2+2+2+2+2+2$, $12 = 2+2+2+3+3$ i $12 = 3+3+3+3$. La relació entre $p(m)$ i $d(m; a_1, \ldots, a_n)$ és directe, moltes de les propietats que té la funció partició, també les té o en té de semblants el denumerant de Sylvester. Per exemple, si $p(m)$ té funció generadora $f(z) = \prod_{i=0}^{\infty} \frac{1}{1-z^i}$, llavors:

Proposició 6.9. *[23] La funció generadora de $d(m; a_1, \ldots, a_n)$ és:*

$$f(z) = \frac{1}{(1-z^{a_1}) \ldots (1-z^{a_n})}.$$

Demostració.

$$\prod_{i=1}^{n} \frac{1}{(1-z^{a_i})} = (1 + z^{a_1} + z^{2a_1} + \ldots)(1 + z^{a_2} + z^{2a_2} + \ldots) \ldots (1 + z^{a_n} + z^{2a_n} + \ldots) =$$

$$= \sum_{i_1=0}^{\infty} \sum_{i_2=0}^{\infty} \cdots \sum_{i_n=0}^{\infty} z^{i_1 a_1 + \ldots + i_n a_n} = \sum_{i=0}^{\infty} c_i z^i,$$

on $c_i = d(i, a_1, \ldots, a_n)$. □

Abans de continuar, cal fer un incís en que $F(a_1, \ldots, a_n)$ és el major m tal que $d(m; a_1, \ldots, a_n) = 0$. És per aquesta raó que ens interessa l'estudi del denumerant de Sylvester i, amb el conjunt de resultats que hi ha a continuació, es veurà la relació directa entre la sèrie de Hilbert, el nombre de Frobenius i el denumerant de Sylvester.

Començarem amb el Teorema de Hilbert-Serre, que ens presenta un resultat molt interessant. Abans, però, cal esmentar un parell de resultats. El primer, és que tot submòdul d'un mòdul finitament generat és finitament generat, i el segon resultat és que passa el mateix amb un mòdul quocient d'un mòdul finitament generat. El primer és conseqüència del Teorema de la Base de Hilbert i el segon del Lema de Nakayama.

Teorema 6.10 ([2], Teorema de Hilbert-Serre)**.** *Siguin s el nombre de generadors d'un anell R finitament generat com a R_0-àlgebra i M un mòdul graduat finitament generat sobre l'anell graduat R, llavors $H(M, z)$ és una funció racional sobre z de la forma*

$$f(z)/\prod_{t=1}^{s}(1 - z^{k_i}),$$

on $f(z) \in \mathbb{Z}[z]$ i k_i enters.

Demostració. Per inducció sobre s, el nombre de generadors de R sobre R_0. Si $s = 0$, aleshores $R_n = 0$ per a tot $n > 0$, per tant $R = R_0$ i com que M és un R_0-mòdul finitament generat, $M_n = 0$ per a tot n. En aquest cas, $H(M, z)$ és un polinomi.
Suposem ara que $s > 0$, i que el teorema és cert per $s - 1$. La multiplicació per x_s, amb $\deg x_s = k_s$, sobre M ens dona la següent successió exacte:

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0.$$

Sigui $K = \bigoplus K_n$ i $L = \bigoplus L_n$, que són R-mòduls finitament generats perquè K i L són respectivament un submòdul i un mòdul quocient de M, i ambdós són anulats per x_s, per tant són $R_0[x_1, \ldots, x_{s-1}]$-mòduls. Aplicant λ i el Lema 6.7, obtenim:

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0.$$

I multiplicant per z^{n+k_s} i fent el sumatori respecte n, ens queda:

$$(1 - z^{k_s})H(M, z) = H(L, z) - z^{k_s}H(K, z) + g(z),$$

on $g(z)$ és un polinomi. Aplicant la hipòtesi d'inducció obtenim el resultat que buscàvem. □

Proposició 6.11. *Sigui $R = \mathbb{K}[X_1, \ldots, X_n]$ l'anell polinomial graduat on X_i té grau a_i. Llavors, la sèrie de Hilbert de R és:*

$$H(R, z) = \frac{1}{(1 - z^{a_1}) \ldots (1 - z^{a_n})}.$$

Demostració. Per la definició de sèrie de Hilbert i la proposició 6.9, només s'ha de veure que

$$\dim_{\mathbb{K}} R_t = d(t; a_1, \ldots, a_n).$$

Aquest resultat és directe veient que la base de R_t són els monomis de la forma X^t on $t = a_1b_1 + \ldots + a_nb_n$. Per tant, per a cada $(b_1, \ldots, b_n)$ tal que $a_1b_1 + \ldots + a_nb_n = t$ hi haurà un element més en aquesta base: $X_1^{b_1} \cdot \ldots \cdot X_n^{b_n}$. I de forma simètrica, per a cada element en aquesta base hi haurà una combinació de $(b_1, \ldots, b_n)$ tal que $a_1b_1 + \ldots + a_nb_n = t$. □

Proposició 6.12. *Siguin S el semigrup generat per $a_1, \ldots, a_n$ i $A[S] = \mathbb{K}[z^{a_1}, \ldots, z^{a_n}]$, llavors existeix un polinomi $Q(z)$ tal que:*

$$H(A[S], z) = \sum_{s \in S} z^s = \frac{Q(z)}{(1 - z^{a_1}) \ldots (1 - z^{a_n})}.$$

Demostració. Veiem primer que $H(A[S], z) = \sum_{s \in S} z^s$. Sigui $\sum_{n \in \mathbb{N}} c_n z^n$ la sèrie de Hilbert de $H(A[S], z)$.

Si $n \notin S$ Per la definició de $A[S]$, no hi ha espai vectorial $A[S]_n$, per tant $c_n = 0$.

Si $n \in S$ L'únic element de la base de $A[S]_n$ com a espai vectorial serà z^n, per tant $c_n = 1$.

I conjuntament amb el Teorema 6.10 obtenim el resultat que volíem. □

La diferència entre la proposició 6.11 i la proposició 6.12 és que en la primera hi ha n variables diferents i en la segona totes les variables són les mateixes. Tot i així, ambdues són casos concrets del Teorema de Hilbert-Serre.

Proposició 6.13. *$F(a_1, \ldots, a_n)$ és el grau de la funció racional $H(A[S], z)$, és a dir, el grau de $Q(z)$ menys $a_1 + \ldots + a_n$.*

Demostració. Usant que

$$\sum_{s \in S} z^s + \sum_{s \notin S} z^s = \sum_{s=0}^{\infty} z^s = \frac{1}{1 - z},$$

i aplicant la proposició 6.12

$$\sum_{s \notin S} z^s = \frac{(1 - z^{a_1}) \ldots (1 - z^{a_n}) - Q(z)(1 - z)}{(1 - z^{a_1}) \ldots (1 - z^{a_n})(1 - z)}$$

per tant, veient que $F(a_1, \ldots, a_n) = \deg \sum_{s \notin S} z^s = \deg Q(z) - (a_1 + \ldots + a_n)$. □

D'aquest sistema en podem treure dues conclusions interessants. La primera és que apareix de forma natural $G(a_1, \ldots, a_n)$ (veure pàgina 26). La segona és que en el cas trivial $F(1) = F(\mathbb{N})$ seria igual a $0 - 1 = -1$, ja que el denominador de la sèrie de Hilbert seria $(1 - z)$ i $Q(z)$ seria igual a 1; aquest -1 vindria a ser l'enter més gran que no pertany als naturals, més enllà de la pròpia definició de nombre de Frobenius.

6.3 Càlculs del nombre de Frobenius a partir de la sèrie de Hilbert

En aquesta secció donarem una idea d'una altra demostració del Teorema 3.5 per tal que es vegi com s'usa la sèrie de Hilbert en el càlcul del nombre de Frobenius. Aquesta està basada en resultats que arribà Herzog a [11]. En aquesta dissertació es fan el següents càlculs usant la nomenclatura de semigrups numèrics introduida en aquest treball.

Recordem abans la notació emprada en el Teorema 3.5: siguin $\{a_1, a_2, a_3\}$ nombres naturals amb màxim comú divisor dos a dos 1 i c_1, c_2 i c_3 els enters més petits tals que existeixen enters $r_{ij} \geq 0$, $1 \leq i, j \leq 3, i \neq j$ amb:

$$c_1 a_1 = r_{12} a_2 + r_{13} a_3,$$

$$c_2 a_2 = r_{21} a_1 + r_{23} a_3,$$

$$c_3 a_3 = r_{31} a_1 + r_{32} a_2.$$

A la secció 4.3 havíem vist que si $r_{ij} > 0$ per a tota i, j llavors

$$c_1 = r_{21} + r_{31},$$

$$c_2 = r_{12} + r_{32},$$

$$c_3 = r_{31} + r_{23}.$$

I si $r_{ij} = 0$ per a algunes i, j, llavors $c_i a_i = c_k a_k$, $k \neq j$ i $c_j a_j = r_{ji} a_i + r_{jk} a_k$ amb r_{ji} i $r_{jk} > 0$.

Herzog [11] demostrà que si $R = \mathbb{K}[X, Y, Z]$ és un anell polinomial graduat amb $\deg X = a_1$, $\deg Y = a_2$ i $\deg Z = a_3$ amb $r_{ij} > 0$ per a tot i, j, llavors $A[S] = \mathbb{K}[z^{a_1}, z^{a_2}, z^{a_3}]$ té la següent successió exacte:

$$0 \longrightarrow R^2 \xrightarrow{M_2} R^3 \xrightarrow{M_1} R \xrightarrow{I} A \longrightarrow 0,$$

on I és el morfisme donat per $X \longrightarrow z^{a_1}$, $Y \longrightarrow z^{a_2}$ i $Z \longrightarrow z^{a_3}$ i

$$M_1 = \begin{bmatrix} X^{c_1} - Y^{r_{12}} Z^{r_{13}} \\ Y^{c_2} - X^{r_{21}} Z^{r_{23}} \\ Z^{c_3} - X^{r_{31}} Y^{r_{32}} \end{bmatrix}.$$

Herzog [11] també demostrà un resultat equivalent si $r_{ij} = 0$. Sense perdre generalitat podem suposar que $r_{12} = 0$, llavors la successió exacte és:

$$0 \longrightarrow R \xrightarrow{M_2} R^2 \xrightarrow{M_1} R \xrightarrow{I} A \longrightarrow 0,$$

i

$$M_1 = \begin{bmatrix} X^{c_1} - Z^{c_3} \\ Y^{c_2} - X^{r_{21}} Z^{r_{23}} \end{bmatrix}.$$

Demostració del Teorema 3.5. Igual que en la primera demostració d'aquest teorema, veurem els dos casos:

Cas I Si $r_{ij} > 0$ per a tot i, j la matriu M_2 és:

$$M_2 = \begin{bmatrix} Z^{r_{23}} & X^{r_{31}} & Y^{r_{12}} \\ Y^{r_{32}} & Z^{r_{13}} & X^{x_{21}} \end{bmatrix}.$$

Observem que

$M_2 \times M_1 =$

$$\begin{bmatrix} Z^{r_{23}}X^{c_1} - Y^{r_{12}}Z^{r_{13}+r_{23}} + X^{r_{31}}Y^{c_2} - X^{r_{21}+r_{31}}Z^{r_{23}} + Y^{r_{12}}Z^{c_3} - X^{r_{31}}Y^{r_{32}+r_{12}} \\ Y^{r_{32}}X^{c_1} - Y^{r_{12}+r_{32}}Z^{r_{13}} + Z^{r_{13}}Y^{c_2} - X^{r_{21}}Z^{r_{23}+r_{13}} + X^{r_{21}}Z^{c_3} - X^{r_{31}+r_{21}}Y^{r_{32}} \end{bmatrix}$$

$$= \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Com que tots els termes són homogenis, obtenim que

$$u = a_3r_{21} + a_1c_1 = a_1r_{31} + a_2c_2 = a_2r_{12} + a_3c_3$$

$$v = a_2r_{32} + a_1c_1 = a_3r_{13} + a_2c_2 = a_1r_{21} + a_3c_3.$$

Fent servir la teoria vista en aquest capítol, la sèrie de Hilbert és:

$$H(A[S], z) = \frac{1 - z^{a_1c_1} - z^{a_2c_2} - z^{a_3c_3} + z^u + z^v}{(1 - z^{a_1})(1 - z^{a_2})(1 - z^{a_3})}.$$

I per tant, el seu grau és $\max\{u, v\} - a_1 - a_2 - a_3$.

Cas II Si $r_{ij} = 0$, sense perdre generalitat podem suposar que $r_{12} = 0$, i, com hem vist abans,

$$M_1 = \begin{bmatrix} X^{c_1} - Z^{c_3} \\ Y^{c_2} - X^{r_{21}}Z^{r_{23}} \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}.$$

En aquest cas, $M_2 = \begin{bmatrix} b & -a \end{bmatrix}$ i pel mateix raonament que en el cas anterior, obtenim

$$H(A[S], z) = \frac{1 - z^{a_1c_1} - z^{a_2c_2} + z^{a_1c_1+a_2c_2}}{(1 - z^{a_1})(1 - z^{a_2})(1 - z^{a_3})}$$

i per tant el seu grau és $a_1c_1 + a_2c_2 - a_1 - a_2 - a_3$, com voliem demostrar.

□

Observem que, de la mateixa manera que en l'altra demostració, hi ha una diferenciació molt gran en un cas i en un altre. Això és perquè els semigrups numèrics, com ja s'ha dit, actuen de forma molt diferent depenent del seu tipus, $t(S)$.

La importància de les sèries de Hilbert en el nombre de Frobenius és que presenten una estructura de càlcul que no depèn de cap hipòtesi addicional.

Tot i que hom es podria pensar que hem trobat una manera molt bona per a trobar el nombre de Frobenius des d'un punt de vista computacional, a [3] es veu que la computació de la sèrie de Hilbert és un problema $\mathcal{NP}$-hard.

7 Aspectes algorítmics

El nombre de Frobenius és un problema difícil en termes computacionals. De fet, en aquest apartat es demostrarà que és un problema $\mathcal{NP}$-hard, per tant no hi ha cap algoritme en temps polinòmic ràpid que el resol, a no ser que $\mathcal{NP}$=$\mathcal{P}$.

En aquest capítol es veurà un algorisme que computa el nombre de Frobenius i una prova que és $\mathcal{NP}$-hard en termes de Turing a partir del problema de *Knapsack*.

7.1 Algoritme de Wilf

Aquest algoritme computa $F(a_1, \ldots, a_n)$ amb $1 < a_1 < \ldots < a_n$ en un ordre de $O(na_n^2)$. La seva autoria és de Herbert Wilf (1931-2012) [24], matemàtic nord-americà especialitzat en combinatòria i teoria de grafs.

Aquest procedeix així:

Algoritme 2 Algoritme de Wilf

Es forma un cercle de a_n llums, etiquetades $l_0, \ldots, l_{a_n-1}$, i amb una agulla assenyalant a l_0.
La llum l_0 s'inicialitza encesa i la resta apagades.
L'agulla gira en sentit de les agulles del rellotge començant per l_0.
Per a cada llum assenyalada per l'agulla, aquesta s'encén si qualsevol de les altres situades a una distància $a_1, \ldots, a_n$ estan enceses. En l'altre cas, es queda apagada.
El procés acaba quan hi ha a_1 llums seguides enceses.
Siguin $s(l_{a_i})$ el nombre de vegades que l'agulla passa per la llum l_{a_i} i l_r la última llum assenyalada per l'agulla. Llavors , $F(a_1 \ldots, a_n) = r + (s(l_r) - 1)a_n$.

Veiem un exemple en el càlcul de $F(4, 9, 10)$. Observant la figura 7.2, podem veure com en aquest cas l_5 és l'última llum assenyalada i $s(l_5) = 2$, i per tant:

$$F(4, 9, 10) = 5 + (2 - 1)10 = 15.$$

La prova de la seva certesa ve donada pel corol·lari 4.21, on es veu $F(a_1, \ldots, a_n) = \max_{l \in \{1,2,\ldots,a_n-1\}} t_l - a_n$, on t_l és l'enter més petit congruent a l mòdul a_n que és expressable com a suma no negativa de $a_1, \ldots, a_{n-1}$.

L'algoritme de Wilf ens dona la següent cota superior:

Teorema 7.1.

$$F(a_1 \ldots, a_n) \leq a_n^2.$$

Demostració. Si ens fixem, cada volta que fa l'agulla, almenys s'encén una llum (sinó $F(a_1 \ldots, a_n)$ no existiria). Per tant, com a molt hi haurà a_n voltes, $s(l_r) \leq a_n$ i $r \leq a_{n-1} \leq a_n$, i així

$$F(a_1, \ldots, a_n) \leq a_n + (a_n - 1)a_n = a_n^2.$$

□

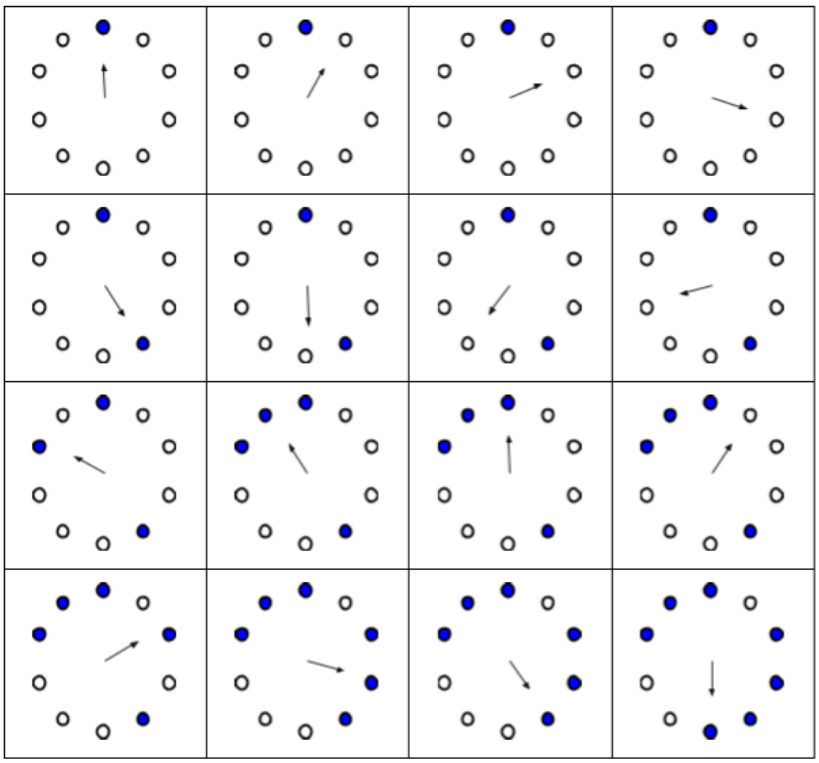

Figura 3: Exemple de càlcul de $F(4, 9, 10)$ mitjançant l'algoritme de Wilf

Albert Nijenhuis [15] en donà un altre uns anys més tard fent servir grafs. Per exemple, en el càlcul de $F(271, 277, 281, 283)$ en un ordinador corrent l'algoritme de Wilf tarda una hora, en comparació del de Nijenhuis, que tarda uns pocs minuts. Això és degut que aquest segon és de l'ordre $O(na_1 \log a_1)$, tenint en compte que $1 < a_1 < \ldots < a_n$.

Com a curiositat, Nijenhuis i Wilf van publicar junts resultats sobre el nombre de Frobenius molt interessants, per exemple que:

$$\frac{F(a_1, \ldots, a_n) + 1}{2} \leq N(a_1, \ldots, a_n),$$

on $N(a_1, \ldots, a_n)$, anomenat gènere, és igual al nombre de naturals que no pertanyen al semigrup numèric generat per $a_1, \ldots, a_n$, i altres resultats com aquest en [14].

Wilf també té entre els seus resultats del nombre de Frobenius, una conjectura, coneguda com la conjectura de Wilf [24].

Conjectura 7.2 (Conjectura de Wilf)**.** *Sigui S un semigrup numèric, $e(S)$ la seva dimensió d'immersió i $n(S)$ el nombre d'elements de S més petits o iguals a $F(S)$, aleshores*

$$F(S) + 1 \leq e(S)n(S).$$

Tornant als algorismes, n'hi ha molts de diferents que resolen el problema de Frobenius fixat el nombre de generadors. Per exemple, quan està generat per tres

elements, J. L. Davison [9] millora la computació de $F(a_1, a_2, a_3)$ de l'algoritme de Rodseth [20], que tot i que la majoria de vegades és $O(\log a_2)$ en el pitjor dels casos és $O(a_1 + \log a_2)$, a un nou que sempre és $O(\log a_2)$. Aquesta $O(\log a_2)$ ve donada pel càlcul del màxim comú divisor.

En el cas $n = 4$, Killingbergtro [12] en presentà un basat en la construcció d'una figura geomètrica.

7.2 Complexitat computacional

Aquesta secció es basa en l'estudi de la complexitat des d'un punt de vista computacional del nombre de Frobenius, que, mitjançant la comparació amb el problema de Knapsack (**IKP**), es veurà que és $\mathcal{NP}$-hard.

Recordem que un problema de decisió és aquell que consta d'una pregunta i d'un candidat, i té dues possibles respostes, **Sí** o **No**. Un problema computacional és $\mathcal{NP}$ si quan x és un candidat a la solució del problema hi ha un certificat concís (és a dir, amb temps polinòmic que depèn de x) que retorna **Sí** o **No**. Donats dos problemes de decisió $\prod_1$ i $\prod_2$, diem que $\prod_1$ és polinòmicament reductible a $\prod_2$ si existeix un algoritme en temps polinòmic que donat un candidat x del problema $\prod_1$ ens retorna un candidat y del problema $\prod_2$ tal que x és un **Sí** si i només si y és **Sí**.

Un problema de decisió $\prod$ és $\mathcal{NP}$-complet si tots els altres problemes que són $\mathcal{NP}$ es poden reduir polinòmicament a $\prod$.

Suposem que $\prod_1$ i $\prod_2$ són problemes, una reducció de Turing en temps polinòmic és un algoritme A que resol $\prod_1$ fent servir un hipotètic algoritme A' que resol $\prod_2$ tal que si A' fos un algoritme en temps polinòmic, llavors A també seria de temps polinòmic. En aquest cas, diem que $\prod_1$ pot ser reduit en termes de Turing en $\prod_2$.

Un problema $\prod_1$ és $\mathcal{NP}$-hard en termes de Turing si hi ha un prolema de decisió $\prod_2$ $\mathcal{NP}$-complet tal que $\prod_1$ pot ser reduit en termes de Turing en $\prod_2$.

Teorema 7.3. *Trobar el nombre de Frobenius és un problema $\mathcal{NP}$-hard en termes de Turing.*

Aquest teorema es desmostrarà donant una reducció de Turing del problema de *Knapsack* (**IKP**), també conegut com el problema de la motxilla, de fet, d'un cas particular d'aquest, que se sap per [17] que és $\mathcal{NP}$-complet. Aquest cas particular és el problema de decisió següent:
Entrada: Enters positius $a_1, \ldots, a_n$ i t.
Pregunta: Existeixen enters $x_i \geq 0$ amb $1 \leq i \leq n$ tal que $\sum_{i=1}^{n} x_i a_i = t$?

Seguidament, donarem la reducció de Turing, [19]. En l'algoritme, assumirem que $r = \gcd(a_1, \ldots, a_n) = 1$, i si això no passa, considerarem l'entrada següent: $a'_i = \frac{a_i}{r}$ i $t' = \frac{t}{r}$. D'aquesta manera, sí que existirà $F(a'_1, \ldots, a'_n)$.

La prova de la seva certesa ve donada per la següent proposició que es demostrarà fent servir un lema.

Algoritme 3 Reducció de Turing del **IKP**

Trobar $F(a_1, \ldots, a_n)$
Si $t > F(a_1, \ldots, a_n)$ **Llavors** es respon afirmativament al **IKP**
Sinó
Si $t = F(a_1, \ldots, a_n)$ **Llavors** es respon negativament al **IKP**
Sinó
Es defineixen $\overline{a}_i = 2a_i$ per $1 \leq i \leq n$ i $\overline{a}_{n+1} = 2F(a_1, \ldots, a_n) + 1$
Trobar $F(\overline{a}_1, \ldots, \overline{a}_n, \overline{a}_{n+1})$

Es defineix $\overline{a}_{n+2} = 2F(\overline{a}_1, \ldots, \overline{a}_n, \overline{a}_{n+1}) - 2t$
Trobar $F(\overline{a}_1, \ldots, \overline{a}_n, \overline{a}_{n+1}, \overline{a}_{n+2})$

Es respon afirmativament al **IKP** si i només si
$F(\overline{a}_1, \ldots, \overline{a}_n, \overline{a}_{n+1}, \overline{a}_{n+2}) < F(\overline{a}_1, \ldots, \overline{a}_n, \overline{a}_{n+1})$

Proposició 7.4. *Sigui $t < F(a_1, \ldots, a_n)$ i $\overline{a}_i$ definides al algoritme 7.2, aleshores existeixen enters x_i amb $1 \leq i \leq n$, tal que $\sum_{i=1}^{n} x_i a_i = t$ si i només si:*

$$F(\overline{a}_i, \ldots, \overline{a}_{n+2}) < F(\overline{a}_1, \ldots, \overline{a}_{n+1}).$$

Lema 7.5. *Siguin a_i i $\overline{a}_i$ definides al algoritme 7.2, aleshores:*

$$F(\overline{a}_1, \ldots, \overline{a}_{n+1}) = 4F(a_1, \ldots, a_n) + 1.$$

Demostració del Lema 7.5. Sigui M tal que $M > 4F(a_1, \ldots, a_n) + 1$. Veurem primer que M és representable com a suma positiva de $\overline{a}_1, \ldots, \overline{a}_{n+1}$.
Siguin $l \equiv M \mod 2$ i $M' = M - l\overline{a}_{n+1}$, llavors:

Si $l = 0$ $M' = M > 4F(a_1, \ldots, a_n) + 1 > 2F(a_1, \ldots, a_n)$.

Si $l = 1$ $M' = M - \overline{a}_{n+1} > 4F(a_1, \ldots, a_n) + 1 - (2F(a_1, \ldots, a_n) + 1) = 2F(a_1, \ldots, a_n)$.

Veiem que M' és parell. Si M és parell, és obvi. Sinó, com que $\overline{a}_{n+1}$ és imparell, la seva resta és parella.
Així, podem afirmar que $M' > 2F(a_1, \ldots, a_n)$ i per tant M' és representable com a suma positiva de $a_1, \ldots, a_n$ i com que és parell també per $\overline{a}_1, \ldots, \overline{a}_n$. Com que $M' + l\overline{a}_{n+1} = M$, obtenim que M és representable com a suma positiva de $\overline{a}_1, \ldots, \overline{a}_{n+1}$.
Hem vist que $4F(a_1, \ldots, a_n) + 1 \geq F(\overline{a_1}, \ldots, \overline{a}_{n+1})$.
Veiem ara que $4F(a_1, \ldots, a_n) + 1$ no és representable com a suma positiva de $\overline{a}_1, \ldots, \overline{a}_{n+1}$ per reducció al absurd.
Suposem que existeixen $x_i \geq 0$, $1 \leq i \leq n + 1$ tals que:

$$\sum_{i=1}^{n+1} x_i \overline{a}_i = 4F(a_1, \ldots, a_n) + 1.$$

Observem que $\overline{x}_{n+1} \geq 1$, ja que $4F(a_1, \ldots, a_n) + 1$ és imparell.
Si $x_{n+1} \geq 2$, aleshores $x_{n+1}\overline{a}_{n+1} = x_{n+1}(2F(a_1, \ldots, a_n) + 1) > 4F(a_1, \ldots, a_n) + 1$, per tant, podem afirmar que $x_{n+1} = 1$. Per tant,

$$\sum_{i=0}^{n} x_i\overline{a}_i + \overline{a}_{n+1} = 4F(a_1, \ldots, a_n) + 1,$$

$$\sum_{i=0}^{n} x_i\overline{a}_i = 2F(a_1, \ldots, a_n)$$

i

$$\sum_{i=0}^{n} x_i a_i = F(a_1, \ldots, a_n)$$

que és impossible. □

Demostració de la proposició 7.4. Suposem que $t < F(a_1, \ldots, a_n)$ i veiem les dues implicacions.
Si existeixen enters $x_i \geq 0$, $1 \leq i \leq n$, tals que $\sum_{i=0}^{n} x_i a_i = t$, aleshores

$$\sum_{i=0}^{n} x_i\overline{a}_i = 2t$$

i per la definició de $\overline{a}_{n+2} = F(\overline{a}_1, \ldots, \overline{a}_{n+1}) - 2t$ obtenim que

$$F(\overline{a}_1, \ldots, \overline{a}_{n+1}) = \sum_{i=0}^{n} x_i\overline{a}_i + \overline{b}_{n+2}$$

i prenent $x_{n+1} = 0$ i $x_{n+2} = 1$

$$F(\overline{a}_1, \ldots, \overline{a}_{n+1}) = \sum_{i=0}^{n+2} x_i\overline{a}_i$$

$$\Longrightarrow F(\overline{a}_1, \ldots, \overline{a}_{n+2}) < F(\overline{a}_1, \ldots, \overline{a}_{n+1}).$$

Assumim ara que $F(\overline{a}_1, \ldots, \overline{a}_{n+2}) < F(\overline{a}_1, \ldots, \overline{a}_{n+1})$ i veurem que existeixen enters $x_i \geq 0$, $1 \leq i \leq n$, tals que $\sum_{i=0}^{n} x_i a_i = t$.
Per l'hipòtesi que hem assumit i pel lema 7.5 obtenim que existeixen $x_i \geq 0$, $1 \leq i \leq n$, tals que

$$F(\overline{a}_1, \ldots, \overline{a}_{n+1}) = 4F(a_1, \ldots, a_n) + 1 = \sum_{i=0}^{n+2} x_i\overline{a}_i.$$

Com que $\overline{a}_i$ és parell sempre que $1 \leq i \leq n + 1$, podem afirmar que $x_{n+2} \geq 1$.
I per la definició de $\overline{a}_{n+2}$:

$$x_{n+2}\overline{a}_{n+2} = x_{n+2}(F(\overline{a}_1, \ldots, \overline{a}_{n+1}) - 2t)$$

i que

$$2t < 2F(a_1, \ldots, a_n) < \frac{4F(a_1, \ldots, a_n) + 1}{2}$$

obtenim que

$$x_{n+2}\overline{a}_{n+2} > x_{n+2}\left(4F(a_1, \ldots, a_n) + 1 - \frac{4F(a_1, \ldots, a_n) + 1}{2}\right)$$

$$= x_{n+2}\left(\frac{4F(a_1, \ldots, a_n) + 1}{2}\right).$$

Ara, si $x_{n+2} \geq 2$, llavors $x_{n+2}\overline{a}_{n+2} \geq 2\overline{a}_{n+2} > 4F(a_1, \ldots, a_n) + 1$, contradient que

$$4F(a_1, \ldots, a_n) + 1 = \sum_{i=0}^{n+2} x_i\overline{a}_i$$

i per tant, $x_{n+2} = 1$. Així

$$4F(a_1, \ldots, a_n) + 1 = \sum_{i=0}^{n+1} x_i\overline{a}_i + \overline{a}_{n+2}$$

i

$$4F(a_1, \ldots, a_n) + 1 = \sum_{i=0}^{n+1} x_i\overline{a}_i + F(\overline{a}_1, \ldots, \overline{a}_{n+1}) - 2t,$$

i per tant

$$2t = \sum_{i=0}^{n+1} x_i\overline{a}_i$$

Només queda veure que $x_{n+1} = 0$. Per la definició de $\overline{a}_{n+1} = 2F(a_1, \ldots, a_n) + 1$ i havent vist que $2t < 2F(a_1, \ldots, a_n)$ podem afirmar $\overline{a}_{n+1} > 2t$, que implica que $x_{n+1} = 0$. Per tant:

$$2t = \sum_{i=0}^{n} x_i\overline{a}_i \Longrightarrow t = \sum_{i=0}^{n} x_i a_i$$

demostrant així la proposició. □

Així observem que aquest problema algorísmicament requereix més del que un es podia imaginar al principi. En aquest capítol també s'ha vist de manera indirecta que el càlcul de les series de Hilbert és un problema complicat des d'un punt de vista computacional. De fet, és $\mathcal{NP}$-hard en termes de Turing, com es publica en [3].

8 Conclusions

Podem concloure que s'han assolit els dos objectius plantejats a l'inici del projecte:

Pel que fa al primer objectiu, s'han analitzat alguns dels resultats més importants que hi ha sobre el nombre de Frobenius i s'han establert unes eines bàsiques que facilitin el seu càlcul.

Pel que fa al segon objectiu, les demostracions d'aquests resultats s'han escrit de forma entenedora, clara, precisa i ordenada, per tal que estiguin a l'abast del màxim nombre de lectors possible. A més, s'ha facilitat una demostració de la gran majoria dels resultats exposats. També, s'ha explicat cada concepte nou que s'introduïa.

Des d'un punt de vista personal, la riquesa d'aquesta memòria està, en part, en l'amplitud d'aspectes matemàtics que s'han usat al treballar el nombre de Frobenius, doncs un resultat que pot semblar purament relacionat amb sumes de nombres naturals pot ser vist des de molts àmbits de les matemàtiques diferents. Per exemple, al tema 5 s'han usat des de successions parcials, varietats algebraiques i el teorema de Dirichlet de progressions aritmètiques fins a la successió de Farey, tot aquest ventall només per donar un sol resultat.

Per acabar, és necessari remarcar que el problema de Frobenius és un problema molt més complicat del que es podria arribar a pensar al principi, com s'ha anat veient a mesura que s'ha anat avançant.

Una bona part dels coneixements que s'han usat en aquest projecte han estat treballats en les assignatures d'Anells de Polinomis en Diverses Variables, Mètodes Algebraics per a la teoria de Nombres i Algorísmica, assignatures optatives del Grau de Matemàtiques; i altres com Geometria Projectiva o Anàlisi Matemàtica Real, assignatures obligatòries del Grau de Matemàtiques, que han establert la base per a donar explicacions pròpies d'alguns resultats. Tot i així, la majoria de coneixements els hem hagut d'adquirir alhora que es treballava aquesta memòria, per exemple en el tema 4 i el tema 6.

Com es pot comprovar, a causa de l'estructura del treball, la recerca bibliogràfica que s'ha fet és extensa, doncs s'ha intentat resoldre el problema de Frobenius des del màxim nombre de punts de vista matemàtics diferents.

Referències

[1] Apostol, T. M.: *Modular Functions and Dirichlet Series in Number Theory*, Graduate Texts in Mathematics, 41, 1990, pàg. 99.

[2] Atiyah, M. F.; MacDonald, I. G.: *Introduction to Commutative Algebra*, Addison-Wesley Series in Mathematics, 1969, pàg. 117.

[3] Bayer, D.; Stillman, M.: Computation of Hilbert functions, *J. Symbolic Computation, 14*, 1992, pàg. 31-50.

[4] Brauer, A.: On a problem of partitions, *Am. J. Math., 64*, 1942.

[5] Cohn, P. M.: *Basic Algebra: Groups, Rings and Fields*, Springer, 2003, pàg. 173-174.

[6] Cox, D. A.; Little, J.; O'Shea, D.: *Using Algebraic Geometry*, Springer, 2000, pàg. 271.

[7] Coxeter, H. S. M.: *Introduction to Geometry*, Miley Classics Library, 1961, pàg. 208-209.

[8] Curtis, F.: On Formulas for the Frobenius Number of a Numerical Semigroup, *Math. Scand, 67*, 1990, pàg. 190-192.

[9] Davison, J. L.: On the Linear Diophantine Problem of Frobenius, *Journal of Number Theory 48*, 1994, pàg. 353-363.

[10] Dulmage, A. L.; Mendelsohn, N. S.: Gaps in the exponent set of primitive matrices, *Illinois J. Math, 8*, 1964, 642-656.

[11] Herzog, G.: Generators and Relations of Abelian Semigroups and Semigroup Rings, *LSU Historical Dissertations and Theses*, 1969, pàg. 30-41.

[12] Killingbergtro, H. G.: Betjening av figur i Frobenius' problem (Usar figures per a resoldre el problema de Frobenius, Noruec), *Normat, 2*, 2000, 75-82.

[13] Lang, S.: *Algebra*, Springer, 1927, pàg. 862.

[14] Nijenhuis, A.; Wilf H. S.: Representations of Integers by Linear Forms in Nonnegative integers , *Journal of Number Theory 4*, 1972, pàg. 98-106.

[15] Nijenhuis, A: A Minimal-Path Algorithm for the "Money Changing Problem", *The American Mathematical Monthly Vol. 86, No. 10*, desembre 1979, pàg. 832-835.

[16] Ong, D. C.; Ponomarenko, V.: The Frobenius number of geometric sequences, *Electronic journal of combinatorial number theory, 8*, 2008.

[17] Papadimitriou, C. H.; Steiglitz, K.: *Combinatorial Optimization: Algorithms and Complexity*, Dover Books on Computer Science, 1982, pàg. 376.

[18] Ramírez Alfonsín, J. L.: *The Diophantine Frobenius Problem*, Oxford Lecture Series in Mathematics and its Applications, 30, 2005.

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

[20] Rodseth, O. J.: On a linear diophantine problem of Frobenius, *J. Reine Angewandte Math. 307/308*, 1979, pàg. 431-440.

[21] Rosales, J. C.; García-Sánchez, P. A.: *Numerical Semigroups*, Springer, Developments in Mathematics, 20, 2009.

[22] Sylvester, J. J.: On the partitions of numbers, *Quart. J. Pure Appl. Math., 1*, 1857, pàg. 141-152.

[23] Sylvester, J. J.: On subinvariants, i.e. semi-invariants to binary quanties of an unlimited order, *Am. J. Math., 5*, 1882, pàg. 119-136.

[24] Wilf H. S.: A circle-of-lights algorithm for the "money changing problem", *The American Mathematical Monthly, Vol. 85, No. 7*, agost-setembre del 1978, pàg. 562-565.

A Annex

En aquest annex demostrarem dos resultats esmentats al tema 3.

Teorema A.1. *Siguin a, d i s enters positius amb* $\gcd(a,d) = 1$. *Aleshores,*

$$F(a, a+d, \ldots, a+sd) = \Big(\Big[\frac{a-2}{s}\Big] + 1\Big)a + (d-1)(a-1) - 1.$$

Lema A.2. *Un nombre natural L té representació de la forma $\sum_{i=0}^{s}(a+id)x_i = L$ si i només si $L = ay_0 + d(y_1 + \ldots + y_s)$, amb $y_i = \sum_{j=i}^{s} x_j$.*

Demostració del Lema.

$$L = ax_0 + (a+d)x_1 + a(2d)x_2 + \ldots + (a+sd)x_s =$$

$$= a\sum_{j=0}^{s} x_j + d\sum_{j=1}^{s} x_j + d\sum_{j=2}^{s} x_j + \ldots + dx_s = ay_0 + d(y_1 + \ldots + y_s).$$

□

Lema A.3. *Fixat un y_0, els enters que poden ser representats per $y_1, \ldots, y_s$ amb valors $y_0 \geq \ldots \geq y_s$ són els z tal que $0 \leq z \leq sy_0$.*

Demostració. Observem que si $y_1 = y_2 = \ldots = y_s = 0$, aleshores $z = 0$. El mateix per $y_1 = 1$ i $y_2 = \ldots = y_s = 0$, aleshores $z = 1$. D'aquesta manera z pot tenir tots els valors fins a $y_0 = y_1 = y_2 = \ldots = y_s$, amb $z = sy_0$. □

Amb els dos lemes anteriors, obtenim de forma directa aquest tercer:

Lema A.4. *L és representable no negativament de la forma $\sum_{i=0}^{s}(a+id)x_i$, amb $x_i \geq 0$, si i només si existeixen y, z tal que $L = ay + dz$ amb $0 \leq z \leq ys$.*

Demostració del Teorema. Veurem que $R = \Big(\Big[\frac{a-2}{s}\Big] + 1\Big)a + (d-1)(a-1)$ és el conductor de $\langle a, a+d, \ldots, a+sd\rangle$, és a dir, que $R-1$ és el nombre de Frobenius. Sigui r un enter tal que $r \geq R$. $(a,d) = 1 \Rightarrow \exists z \mid dz \equiv r \mod a$ i $0 \leq z \leq a-1$. Per tant, $r - dz = ay$ on y és un enter. Podem escriure $ay = r - dz \geq r - d(a-1) \geq R - d(a-1)$.

$$R - d(a-1) = \Big(\Big[\frac{a-2}{s}\Big] + 1\Big)a - (a-1) = \Big[\frac{a-2}{s}\Big] + 1 > \Big[\frac{a-2}{s}\Big]a$$

$$\Rightarrow y \geq \Big[\frac{a-2}{s}\Big] + 1.$$

Observem que $s\Big(\Big[\frac{a-2}{s}\Big] + 1\Big) > a - 2$, per tant, $sy \geq s\Big(\Big[\frac{a-2}{s}\Big] + 1\Big) \geq a - 1 \geq z \Rightarrow$ $r = ay + dz$ amb $0 \leq z \leq sy$, i pels lemes vistos, obtenim que r té representació no negativa per $a, a+d, a+2d, \ldots, a+sd$.
Sigui $r = R - 1$, suposem que existeixen z, y amb $r = ay + dz$.

$$r = \Big(\Big[\frac{a-2}{s}\Big] + 1\Big)a + d(a-1) - a \Rightarrow z \equiv a - 1 \mod a \Rightarrow z \geq a - 1.$$

$$ay + (a-1)d \leq ay + dz = \Big(\Big[\frac{a-2}{s}\Big] + 1\Big)a + d(a-1) - a \Rightarrow y \leq \Big[\frac{a-2}{s}\Big].$$

Així

$$sy \leq s\Big[\frac{a-2}{s}\Big] \leq a-2 < a-1 \leq z$$

i per tant r no és representable no negativament de la forma $\sum_{i=0}^{s}(a+id)x_i$, amb $x_i \geq 0$. □

Teorema A.5. *Siguin m, n, k enters positius tals que* $\gcd(m,n) = 1$. *Aleshores,*

$$F(m^k, m^{k-1}n, m^{k-2}n^2, \ldots, n^k) = n^{k-1}(mn - m - n) + \frac{(n-1)m^2(m^{k-1} - n^{k-1})}{(m-n)}.$$

Per a la demostració d'aquest teorema i per fer-ho més fàcil de llegir, anomenarem $A(m,n,k)$ al semigrup numèric generat per $\{m^k, m^{k-1}n, m^{k-2}n^2, \ldots, mn^{k-1}, n^k\}$ i $G(m,n,k)$ al seu nombre de Frobenius.

Aquest es demostrarà per inducció, però abans s'hauran de veure dos lemes previs.

Lema A.6. *Siguin m i n dos nombres naturals relativament primers i $k \geq 1$, aleshores $G(m,n,k+1) \geq (n-1)m^{k+1} + nG(m,n,k)$.*

Demostració del lema. Hem de veure que $(n-1)m^{k+1} + nG(m,n,k+1)$ no està contingut en $A(m,n,k+1)$. Ho veurem per reducció a l'absurd. Suposem que $(n-1)m^{k+1} + nG(m,n,k+1) \in A(m,n,k+1)$, aleshores

$$(n-1)m^{k+1} + nG(m,n,k) = \sum_{i=0}^{k+1} c_i m^i n^{k+1-i}, c_i \in \mathbb{Z}_{\geq 0}.$$

Si apliquem $\bmod n$ als dos costats de la igualtat, ens queda

$$-m^{k+1} \equiv c_{k+1}m^{k+1}.$$

Com que m i n són relativament primers, concluim que $c_{k+1} \equiv -1 \bmod n$, per tant $c_{k+1} = bn - 1$ per una b enter més gran que 0. Llavors,

$$(n-1)m^{k+1} + nG(m,n,k) = \sum_{i=0}^{k-1} c_i m^i n^{k+1-i} + c_k m^k n + c_{k+1}m^{k+1} =$$

$$= \sum_{i=0}^{k-1} c_i m^i n^{k+1-i} + ((b-1)m + c_k)m^k n + (n-1)m^{k+1}$$

i per tant

$$G(m,n,k) = \sum_{i=0}^{k-1} c_i m^i n^{k-i} + ((b-1)m + c_k)m^k.$$

Fet que implica que $G(m,n,k) \in A(m,n,k)$, que és absurd. Així, podem concloure que $(n-1)m^{k+1} + nG(m,n,k) \notin A(m,n,k+1)$ i per tant $G(m,n,k+1) \geq (n-1)m^{k+1} + nG(m,n,k)$. □

Lema A.7. *Siguin m i n relativament primers i $k \geq 1$, aleshores $G(m,n,k+1) \leq (n-1)m^{k+1} + nG(m,n,k)$.*

Demostració del lema. Veure que si $y > (n-1)m^{k+1} + nG(m,n,k)$, aleshores $y \in A(m,n,k+1)$. Siguin d tal que $y \equiv dm^{k+1} \bmod n$, $d \in [0, n-1]$ i $z = y - dm^{k+1}$. Com que $z \equiv 0 \bmod n$, obtenim que $z = nw$ per un enter no negatiu w. Que $y > (n-1)m^{k+1} + nG(m,n,k)$ implica que $z > nG(m,n,k)$, per la definició de d. Per tant, $w > G(m,n,k)$, i així $w \in A(m,n,k)$. Però això implica que $y = nw + dm^{k+1} \in A(m,n,k+1)$ i $G(m,n,k+1) \leq (n-1)m^{k+1} + nG(m,n,k)$. □

Dels últims dos lemes, obtenim que $G(m,n,k+1) = (n-1)m^{k+1} + nG(m,n,k)$.

Demostració del teorema. Ho demostrarem per inducció sobre k. Per $k = 1$, sabem que $G(m,n,1) = F(m,n) = mn - m - n$, pel teorema 3.1. Suposem que és cert per $k = t$, és a dir,

$$G(m,n,t) = n^{t-1}(mn - m - n) + \frac{(n-1)m^2(m^{t-1} - n^{t-1})}{m-n}.$$

Pels resultats que acabem de veure

$$\begin{aligned} G(m,n,t+1) &= (n-1)m^{t+1} + n\Big(n^{t-1}(mn - m - n) + \frac{(n-1)m^2(m^{t-1} - n^{t-1})}{m-n}\Big) \\ &= n^t(mn - m - n) + (n-1)\Big(m^{t+1} + \frac{nm^2(m^{t-1} - n^{t-1})}{m-n}\Big) \\ &= n^t(mn - m - n) + \frac{(n-1)m^2(m^t - n^t)}{m-n}, \end{aligned}$$

que és el que volíem veure per $k = t + 1$. □