UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES I ENGINYERIA INFORMÀTICA

Treball final de grau

Expander Graphs i una aplicació a la informàtica

Autor: Guillermo Mariscal Vizcaya

Directors: Dr. Ignasi Mundet Riera
Dr. Oriol Pujol Vila

Realitzat a: Departament Matemàtiques i Informàtica

Barcelona, 10 de juny de 2024

Abstract

The aim of this project is to study an explicit construction of a family of expander graphs, and give an application to computer science. The mathematical part of the project gives the definition of a family of expander graphs and then it has four main blocks: in the first one we will use Linear Algebra to define expander graphs using the eigenvalues of the adjacency matrix of the family graphs. The second block gives some definitions and results about Number Theory and the third one defines the $PGL_(K)$ i $PSL_2(K)$, and also gives some interesting properties about those. Finally, the fourth block uses the previous ones to define a family of graphs known as $X^{p,q}$, and ends proving the fact that it actually is a family of expander graphs. Then, for the application, we will study an example on how expander graphs help with the propagation in Graph Neural Networks.

Resum

L'objectiu d'aquest treball és estudiar una construcció d'una família d'*expander graphs* i veu-re una aplicació a la informàtica. La part matemàtica del treball, defineix el que és una família d'*expanders* i després té 4 blocs: el primer dedicat a una visió més algebraica dels grafs, a partir de la seva matriu d'adjacència, per acabar donant un resultat que relaciona els valors propis d'aquesta matriu amb els *expanders*. El segon bloc dona alguns conceptes i resultats de teoria de nombres i el tercer defineix els grups $PGL_(K)$ i $PSL_2(K)$, i dona algunes propietats interessants d'aquests. Finalment, al quart bloc, es fan servir els tres anteriors per donar una construcció explícita d'una família de grafs, coneguda com a grafs $X^{p,q}$, i acaba amb la demostració del fet que, efectivament, es tracta d'una família d'*expanders*. Després, a la part informàtica estudiarem l'aplicació dels mateixos a la propagació d'informació a través de xarxes neuronals de graf.

2020 Mathematics Subject Classification. 05C50, 05C25, 05C90

Agraïments

Vull donar gràcies a tothom que m'ha ajudat, tant amb aquest treball com al llarg dels sis anys de doble grau.

En primer lloc, gràcies als meus tutors, Drs. Ignasi Mundet i Oriol Pujol, per la seva ajuda en l'orientació, sobretot en les primeres etapes, on a vegades costa veure el camí a seguir, a més, en el cas del primer, vull agrair el fet de parlar-me sobre els *expander graphs*, cosa que em va ajudar molt a escollir tema de treball i a trobar-ne un sobre el qual m'ha encantat aprendre.

També vull donar moltes gràcies a la meva família per tot el suport al llarg d'aquests sis anys, per haver-me fet sentir sempre recolzat, fins i tot als moments de dificultat.

Gràcies també a tots els meus amics, als que he fet durant el grau i als que ja venien d'abans, i en especial a la Marta i a l'Arnau per ser el meu petit cercle de confiança durant gran part de la meva vida.

Finalment, però no menys important, gràcies a tothom que es prengui el temps per llegir aquest treball.

Índex

Capítol 1

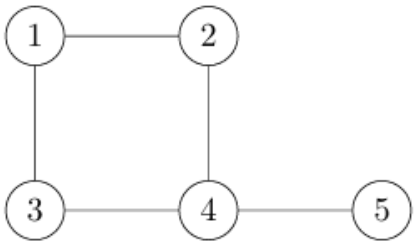
Introducció

1.1 Notació i definicions bàsiques

En aquesta primera secció definirem els conceptes bàsics i la notació que farem servir a la resta del treball.

Denotarem per X = (V,E) un **graf**. On V serà el conjunt de vèrtexs i E el conjunt d'arestes del graf. Assumirem en tot moment que es tracta d'un graf **no dirigit** (és a dir, que les seves arestes no tenen orientació) i, llevat que s'indiqui el contrari, **finit**.

Exemple 1.1.1. La següent figura:



És un graf $X = (V, E)$ amb $V = \{1, 2, 3, 4, 5\}$ i $E = \{(1, 2), (1, 3), (2, 4), (3, 4), (4, 5)\}$

Direm que un graf és **simple** si per cada parella de vèrtexs hi ha, com a màxim, una aresta que els uneix.

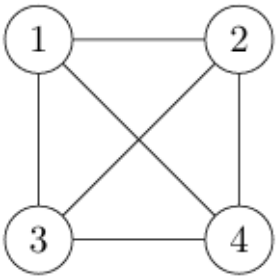
Exemple 1.1.2. El graf de l'exemple 1.1.1 és un graf simple.

Donat $v \in V$ un vèrtex de X definim el **grau** de v (denotat com deg(v)) com el nombre d'arestes que són incidents a v.

Un **bucle** és una aresta de X que va d'un vèrtex a ell mateix.

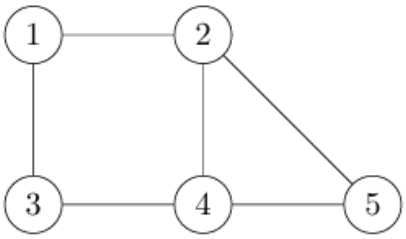
Direm que un graf és **k-regular** si tots els seus vèrtexs tenen exactament K veïns, o, el que és equivalent, que cada vèrtex del graf té grau k.

Exemple 1.1.3. El següent graf és un graf 3-regular:



Un **camí** sobre X és una seqüència de vèrtexs $v_1, v_2, ..., v_k$ tal que v_i és adjacent a v_{i+1}. Diem que X és un graf **connex** si existeixen camins estre qualsevol parella de vèrtexs.

Exemple 1.1.4. El següent graf és un graf connex:



I un possible camí sobre X podria ser $1, 2, 5, 4$ per anar del vèrtex 1 al vèrtex 4.

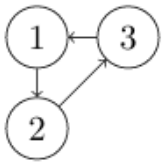
Un **cicle** de X és un camí tancat. Si X no té cicles direm que és un graf **acíclic**.

Sigui X = (V,E) un graf k-regular, simple i no necessàriament finit. Un camí de mida r **sense marxa enrere** sobre X és una seqüència $\underline{e} = (x_0, x_1, \ldots, x_r)$ de vèrtexs de V tal que x_i és adjacent a x_{i+1} $(i = 0, \ldots, r-1)$ i $x_{i+1} \neq x_{i-1}$ per tot $(i = 1, \ldots, r-1)$. x_0 és **l'origen** de $\underline{e}$ i x_r **l'extrem**.

Si X és un graf connex, definirem la **circumferència** de X, i la denotarem $g(X)$ a la longitud del cicle més curt de X. Si X és acíclic direm que $g(X) = +\infty$.

Així mateix, si X està format per un sol cicle i té m vèrtex, denotarem X com C_m i l'anomenarem cicle de n vèrtexs.

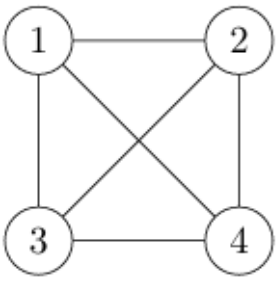
Exemple 1.1.5. Aquest seria el graf C_3, és a dir, el cicle de 3 vèrtexs:



I la seva circumferència seria $g(C_3) = 3$.

Anomenem **graf complet de m vèrtexs** i el denotem K_m al graf de m vèrtexs on cada vèrtex està connectat a cadascun dels altres.

Exemple 1.1.6. Aquest seria el graf K_4:



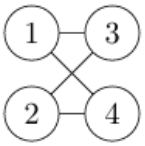
Donat un conjunt $F \subseteq V$, definim la **frontera de F**, que la denotarem com ∂F al conjunt d'arestes que uneixen F amb V - F.

Exemple 1.1.7. Si agafem el graf K_4 de l'exemple 1.1.6 i definim $F = \{1, 2\}$ aleshores $\partial F = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$.

Direm que X és un graf **bipartit** si podem dividir el seu conjunt de vèrtexs en dos subconjunts de manera que les arestes de X només poden unir vèrtexs d'un dels subconjunts a l'altre.

Diem que X és un graf **vèrtex-transitiu** i el grup $AutX$ dels automorfismes a X actua de forma transitiva al conjunt de vèrtexs V. És a dir, que per cada parella de vèrtexs x i y, existeix $\alpha \in AutX$ tal que $\alpha(x) = y$.

Exemple 1.1.8. El següent graf:



És un graf bipartit. Podem definir les següents particions: $V_1 = \{1, 2\}$ i $V_2 = \{3, 4\}$.

Sigui K un cos commutatiu, denotarem per $A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n} \in K^{mxn}$ una matriu de m files i n columnes amb coeficients a K. Denotarem per A^t la seva **transposada**.

Notarem el **determinant** d'una matriu quadrada (és a dir, nxn) A com det(A).

Definirem el **rang** d'una matriu $A \in K^{mxn}$ com el nombre més gran de files/columnes linalment independents, és a dir, la dimensió de la submatriu quadrada d'A més gran amb determinant no nul.

Definirem els **valors propis** d'una matriu $A \in K^{nxn}$ com les arrels λ del polinomi $det(A - \lambda Id) = 0$. Aquest polinomi s'anomena el **polinomi característic** d'A.

Al conjunt de valors propis de la matriu A l'anomenarem **espectre** de A i el denotarem com $Spec(A)$.

1.2 Expander Graphs

Definició 1.2.1. *Definim la* ***constant d'expansió o constant isoperimètrica*** *d'un graf X (i la denotarem per h(X)) de la següent forma:*

$$h(X) = \inf \left\{ \frac{|\partial F|}{\min\{|F|, |V - F|\}} \ : \ F \subseteq V, \ 0 < |F| < +\infty \right\} \tag{1.2.1}$$

Aquesta constant ens permet valorar X quant a la seva qualitat com a xarxa, ja que a major valor de h(X), millor es propaga la informació. Això és degut al fet que si h(X) té un valor gran, aleshores existeixen moltes arestes unint qualsevol divisió de V en dos conjunts disjunts, per tant, caldria eliminar moltes arestes per tal que quedessin dues seccions del graf sense connectar. Per il·lustrar millor aquest concepte anem a veure un parell d'exemples:

Exemple 1.2.2. El **graf complet** K_m, compleix el següent:

Si tenim un conjunt F tal que $|F| = l$ aleshores $|\partial F| = (m - l)$, i per tant: $h(K_m) = m - [\frac{m}{2}] \sim \frac{m}{2}$

Com podem veure, la constant isoperimètrica creix de forma directament proporcional al nombre de vèrtexs del graf, cosa que té sentit, ja que com més gran és K_m, més difícil és deixar seccions del mateix desconnectades.

Definició 1.2.3. *Sigui $k \in \mathbb{N}, k \geq 2$ $(X_m)_{m\geq 1}$, $X_m = (V_m, E_m)$ una família de grafs amb $m \in \mathbb{N}$ tal que X_m és K-regular, finit i connex. Diem que $(X_m)_{m\geq 1}$ és una família d'****expander graphs*** *si $|V_m| \to \infty$ per $m \to \infty$, i si existeix $\epsilon > 0$ tal que $h(X_m) \geq \epsilon$ per tot $m \geq 1$.*

El que volem són famílies de grafs arbitràriament grans de manera que tots tinguin la constant isoperimètrica acotada inferiorment, és a dir, que per molt gran que fem el graf, continuï fent falta "tallarün nombre molt gran d'arestes per tal que el graf deixi de ser connex.

Cal destacar la condició que els X_m siguin k-regulars és perquè es vol tenir controlat el nombre d'arestes a mesura que creix el nombre de nodes de X_m. En particular, la k-regularitat ens assegura un creixement lineal del nombre d'arestes respecte al nombre de nodes. Això és important, ja que, sobretot en l'àmbit computacional, volem una xarxa que sigui econòmica, i això implica controlar el nombre d'arestes, que és un dels aspectes que fa cara la xarxa.

Aquest és el motiu pel qual, tot i que hem vist que la família de grafs complets K_m garanteix una constant isoperimètrica creixent amb el valor de m, el nombre

d'arestes creix a una velocitat de l'ordre de m^2 (K_m té $\frac{m(m-1)}{2}$ arestes), per tant, no és una bona candidata a familia d'*expander graphs*.

La primera demostració de l'existència d'*expander graphs* va ser donada per Mark Pinsker als anys setanta al seu article "On the Complexity of a Concentrator"[4], els detalls de la demostració es poden trobar a l'article esmentat, però el que és rellevant comentar és que no aporta un argument constructiu, és a dir, no dona una construcció de la família d'*expander graphs* sinó que dona arguments probabilístics. Posteriorment, es van donar diferents construccions de famílies d'expanders amb diversos arguments diferents, com per exemple la que veurem en aquest treball, que està basada en grafs de Cayley.

1.3 Objectiu del treball

Per tant, el que volem és una forma relativament senzilla de poder construir una família d'*expander graphs*, per això, en el nostre cas, farem servir una construcció basada en el graf de Cayley d'un grup, concretament, els grups $PGL_2(K)$ i $PSL_2(K)$, que ja definirem al capítol corresponent.

Al llarg del treball donarem definicions i resultats que aportaran el context necessari per arribar a definir aquesta construcció i, finalment, demostrarem que la família construïda és efectivament una família d'*expander graphs*. Abans d'això, però, cal donar un primer resultat que ens permeti demostrar que una família de grafs és una família d'*expanders* de forma que no haguem de fer servir la mateixa definició, ja que aquesta és molt poc pràctica. El resultat que volem aconseguir fa servir el segon valor propi de la matriu d'adjacència del graf.

Finalment, donarem una aplicació de la construcció donada a la informàtica, concretament a la propagació d'informació a través de xarxes neuronals de graf (GNN).

Capítol 2

Matrius d'Adjacència i Expander Graphs

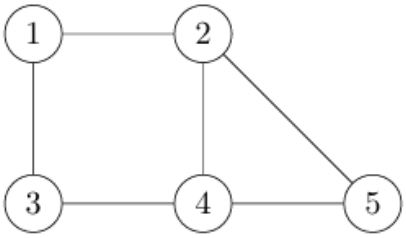
2.1 La matriu d'adjacència

Com hem mencionat al capítol anterior, el primer que necessitem és una eina per poder demostrar que una família de grafs donada es tracta d'una família d'*expanders*. El primer que definirem és la matriu d'adjacència d'un graf i donarem algunes de les seves propietats:

Definició 2.1.1. *Sigui X = (V,E) un graf on V és el seu conjunt de vèrtexs i E el conjunt d'arestes. Escrivim* $V = \{v_1, v_2, ...\}$. *Llavors la* ***matriu d'adjacència*** *del graf X és la matriu* $A = (A_{i,j})$ *tal que:*

$A_{i,j}$ = *nombre d'arestes que uneixen* v_i *amb* v_j.

Exemple 2.1.2. Considerem el següent graf:



La seva matriu d'adjacència serà:

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

Notem que A determina completament el graf X i d'aquí podem extreure les seves propietats, enumerem algunes que seran rellevants per futurs resultats:

- X serà simple sí i només si $A_{i,j} \in \{0,1\} \forall\ v_i, v_j \in V$.
- Com hem assumit que X es tracta d'un graf no dirigit, A serà una matriu simètrica.
- X no tindrà bucles si i només si $A_{i,i} = 0\ \forall v_i \in V$.
- X és k-regular si per cada $v_i \in V$ tenim que $\sum_{v_j \in V} A_{i,j} = k$.

En aquest treball ens centrarem en els valors propis de la matriu d'adjacència. En particular, si agafem X un graf de n vèrtexs, finit i no dirigit, aleshores, per ser A simètrica i de mida n x n sabem que té n valors propis reals comptant multiplicitats, que podem denotar, ordenant-los de major a menor, de la següent manera:

$$\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}.$$

Al conjunt de valors propis d'A se l'anomena **l'espectre** de X.

Definició 2.1.3. *Sigui X = (V,E) un graf arbitrari i considerem les funcions $f : V \to \mathbb{C}$ que van del conjunt de vèrtexs de X als complexos. Definim el següent espai:*

$$l^2(V) = \left\{ f : V \to \mathbb{C} : \sum_{v \in V} |f(v)|^2 < +\infty \right\}.$$

Anàlogament, definim $l^2(E)$ per les arestes de X.

Si V és finit, posem $|V| = n$, aleshores totes les funcions $f : V \to \mathbb{C}$ pertanyen a $l^2(V)$. Podem pensar cada funció f com un vector en $\mathbb{C}^n$ en el que la matriu d'adjacència actua de la següent manera:

$$Af = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix} \begin{pmatrix} f(v_1) \\ f(v_2) \\ \vdots \\ f(v_n) \end{pmatrix} = \begin{pmatrix} A_{11}f(v_1) + A_{12}f(v_2) + \cdots + A_{1n}f(v_n) \\ A_{21}f(v_1) + A_{22}f(v_2) + \cdots + A_{2n}f(v_n) \\ \vdots \\ A_{n1}f(v_1) + A_{n2}f(v_2) + \cdots + A_{nn}f(v_n) \end{pmatrix}$$

És a dir, $(Af)(v_i) = \sum_{j=1}^{n} A_{ij} f(v_j)$. A nivell de notació, és útil ignorar el nombre de vèrtexs i indexar la matriu directament segons les parelles de vèrtexs de la següent forma: $(Af)(x) = \sum_{y \in V} A_{xy} f(y)$, per cada $x \in V$.

Proposició 2.1.4. *Sigui X un graf finit, k-regular amb n vèrtexs. Aleshores:*

a) $\mu_0 = k$;

b) $|\mu_i| \leq k$ *per* $1 \leq i \leq n-1$

c) μ_0 *té multiplicitat 1, si i només si X és connex.*

Demostració: Podem provar a) i b) simultàniament fent notar que la funció $f \equiv 1$ a V és una funció pròpia d'A associada al valor propi k. Tot seguit veiem que, si μ és un valor propi qualsevol, aleshores $|\mu| \leq k$. Certament, suposem que f és una funció pròpia real associada a μ i $x \in V$ tal que $|f(x)| = \max_{y \in V} |f(y)|$. Substituint f per $-f$ en cas que sigui necessari, podem assumir $f(x) > 0$. Aleshores:

$$f(x)|\mu| = |f(x)\mu| = |\sum_{y \in V} A_{xy} f(y)| \leq \sum_{y \in V} A_{xy}|f(y)| \leq f(x) \sum_{y \in V} A_{xy} = f(x)k$$

. I cancel·lant $f(x)$ obtenim el resultat.

Per provar c) primer suposem que X és connex. Sigui f una funció pròpia real associada al valor propi k. Hem de demostrar que f és constant. Sigui $x \in V$ un vèrtex tal que $|f(x)| = \max_{y \in V} |f(y)|$. Com que $f(x) = \frac{(Af)(x)}{k} = \sum_{y \in V} \frac{(Af)(x)}{k} f(y)$ podem veure que $f(x)$ és una combinació convexa de nombres reals que són, en mòdul, menors que $|f(x)|$. Això implica que $f(x) = f(y)$ per cada $y \in V$ tal que $A_{xy} \neq 0$, és a dir, per cada y veí de x. Apliquem el mateix argument i veiem que f té el mateix valor $f(x)$ per a cada veí dels vèrtexs y veïns de x i així successivament, com X és connex, veiem que f és constant. L'altra implicació queda com exercici pel lector. □

Com es pot veure a l'enunciat c) de la proposició 2.1.3, hi ha una connexió entre l'espectre de la matriu d'adjacència i les propietats combinatòries del graf. Aquest és un dels temes principals d'aquest capítol.

Proposició 2.1.5. *Sigui X un graf connex, k-regular i amb n vèrtexs. Els següents enunciats són equivalents:*

a) X és bipartit.

b) L'espectre de X és simètric respecte a 0.

c) $\mu_{n-1} = -k$.

Demostració:

a) $\implies$ b): Suposem que $V = V_+ \cup V_-$ és una bipartició de X. Suposem també que f és una funció pròpia d'A associada al valor propi μ. Definim:

$$g(x) = \begin{cases} f(x) & \text{si } x \in V_+ \\ -f(x) & \text{si } x \in V_- \end{cases}$$

. És directe veure aleshores que $(Ag)(x) = -\mu g(x)$ per tot $x \in V$.

b) $\implies$ c): És conseqüència de la proposició 1.1.2.

c) $\implies$ a): Sigui f una funció pròpia real d'A amb valor propi $-k$. Sigui també $x \in V$ tal que $|f(x)| = \max_{y \in V} |f(y)|$. Substituint f per $-f$ en cas que sigui necessari, podem assumir $f(x) > 0$. Aleshores:

$$f(x) = -\frac{(Af)(x)}{k} = -\sum_{y \in V} \frac{A_{xy}}{k} f(y) = \sum_{y \in V} \frac{A_{xy}}{k}(-f(y))$$

. Aleshores $f(x)$ és una combinació convexa dels $-f(y)$ que són, en mòdul, menors que $|f(x)|$. Per tant, $-f(y) = f(x)$ per tot $y \in V$ tal que $A_{xy} \neq 0$, és a dir, per cada y adjacent a x. Anàlogament, si z és adjacent a qualsevol dels y adjacents a x, aleshores $f(z) = -f(y) = f(x)$. Repetim el procés per tot el graf, ja que és connex i definim $V_+ = \{y \in V : f(y) > 0\}$ i $V_- = \{y \in V : f(y) < 0\}$, novament per ser X connex, definim una bipartició de X. □

2.2 La bretxa espectral

A la secció anterior hem vist que cada graf X connex i k-regular té com a major valor propi positiu $\mu_0 = k$, a més, si és bipartit, tenim que el menor valor propi $\mu_{n-1} = k$. μ_0 (i μ_{n-1} en el cas que X sigui bipartit) s'anomenen valors propis **trivials** de X. Si denotem per μ_1 el valor propi no trivial més gran, aleshores tenim que la diferència $\mu_0 - \mu_1 = k - \mu_1$ s'anomena **bretxa espectral** de X.

Per aquesta secció tornem a rescatar les definicions de **constant isoperimètrica ($h(X)$)** i **família d'expanders** del capítol 1. Ara enunciarem el primer gran resultat del treball, que és el que ens permetrà demostrar que una família de grafs es tracta d'una família d'expanders sense haver de fer servir la definició.

Teorema 2.2.1. [1, *Theorem* 1.2.3, *pg.* 13] *Sigui $X = (V, E)$ un graf finit, connex, k-regular i sense bucles. Sigui μ_1 el primer valor propi no trivial de X. Aleshores:*

$$\frac{k - \mu_1}{2} \leq h(X) \leq \sqrt{2k(k - \mu_1)}.$$

Demostració: Comencem amb la primera desigualtat. El primer que fem serà dotar el conjunt d'arestes E d'una orientació escollida arbitràriament, de forma que cada aresta $e \in E$ té un origen e^- i un extrem e^+. Això ens permet definir el ***simplicial coboundary operator*** $d : l^2(V) \to l^2(E)$ que, per $f \in l^2(V)$ i $e \in E$, es defineix com $df(e) = f(e^+) - f(e^-)$.

Donem a $l^2(V)$ el producte escalar hermitià $\langle f|g\rangle = \sum_{x\in V} \overline{f(x)}g(x)$, on $\overline{f(x)}$ denota el conjugat complex de $f(x)$, i $l^2(E)$ amb l'anàleg. Tot seguit definim l'operador adjunt $d^* : l^2(E) \to l^2(V)$, caracteritzat per $\langle df|g\rangle = \langle f|d^*g\rangle$ per tota $f \in l^2(V)$, $g \in l^2(E)$. Definim una funció $\delta : VxE \to \{-1, 0, 1\}$ com

$$\delta(x, e) = \begin{cases} 1 & \text{si } x = e^+ \\ -1 & \text{si } x = e^- \\ 0 & \text{altrament.} \end{cases}$$

És fàcil comprovar que, per $e \in E$ i $f \in l^2(V)$ es compleix que

$$df(e) = \sum_{x\in V} \delta(x, e)f(x);$$

mentre que, per $v \in V$ i $g \in l^2(E)$,

$$d^*g(x) = \sum_{e\in E} \delta(x, e)g(e).$$

Aleshores definim l'**operador combinatori de Laplace** com $\Delta = d^*d : l^2(V) \to l^2(V)$. És fàcil comprovar que $\Delta = k \cdot Id - A$. En particular, Δ no depèn de l'orientació escollida. Per una base ortonormal de funcions pròpies d'A, l'operador Δ pren la següent forma:

$$\Delta = \begin{pmatrix} 0 & & & \\ & k-\mu_1 & & \bigcirc \\ & & \ddots & \\ \bigcirc & & & k-\mu_{n-1} \end{pmatrix},$$

corresponent el valor propi 0 a les funcions constants a V. Per tant, si f és una funció a V amb $\sum_{x\in V} f(x) = 0$, (és a dir, f és ortogonal a les funcions constants a $l^2(V)$), tenim:

$$||df||_2^2 = \langle df|df\rangle = \langle \Delta f|f\rangle \geq (k-\mu_1)||f||_2^2.$$

Fixem un subconjunt F de V i escollim f de la següent forma:

$$f(x) = \begin{cases} |V-F| & \text{si} x \in F \\ -|F| & \text{si} x \in V-F. \end{cases}$$

Aleshores $\sum_{x\in V} f(x) = 0$ i $||f||_2^2 = |F||V-F|^2 + |V-F||F|^2 = |F||V-F||V|$. A més:

$$df(e) = \begin{cases} 0 & \text{si } e \text{ connecta dos vèrtexs a } F \text{ o a } V-F \\ \pm|V| & \text{si connecta un vèrtex a } F \text{ amb un vèrtex a } V-F \end{cases}$$

. Per tant, $||df||_2^2 = |V|^2|\partial F|$. Llavors, per la desigualtat anterior, tenim que $|V|^2|\partial F| \geq (k-\mu_1)|F||V-F||V|$. Per tant,

$$\frac{|\partial F|}{|F|} \geq (k-\mu_1)\frac{|V-F|}{|V|}$$

.

Si assumim $|F| \leq \frac{|V|}{2}$, obtenim $\frac{|\partial F}{|F|} \geq \frac{k-\mu_1}{2}$, per tant, per definició, $h(X) \geq \frac{k-\mu_1}{2}$.

Ara volem demostrar la segona desigualtat. Fixem una funció no negativa f a V i definim

$$B_f = \sum_{e\in E} |f(e^+)^2 - f(e^-)^2|$$

. Denotem per $\beta_r > \beta_{r-1} > \ldots > \beta_1 > \beta_0$ els valors de f i definim

$$L_i = \{x \in V : f(x) \geq \beta_i\}(i = 0, 1, \ldots, r)$$

. Notem que $L_0 = V$, ja que $\partial L_0 = \emptyset$. Abans de continuar amb la demostració, provarem alguns resultats sobre B_f que necessitem per continuar.

Remarca 1: $B_f = \sum_{i=1}^r |\partial L_i|(\beta_i^2 - \beta_{i-1}^2)$.

Per provar-ho denotem per E_f el conjunt d'arestes $e \in E$ tals que $f(e^+) \neq f(e^-)$. Clarament $B_f = \sum_{e\in E_f} |f(e^+)^2 - f(e^-)^2|$. Ara agafem una aresta $e \in E_f$ que

connecta un vèrtex x tal que $f(x) = \beta_{i(e)}$ amb un altre vèrtex y tal que $f(y) = \beta_{j(e)}$. Podem suposar que els índexs compleixen $i(e) > j(e)$ i, per tant:

$$B_f = \sum_{e \in E_f} (\beta^2_{i(e)} - \beta^2_{j(e)})$$

$$= \sum_{e \in E_f} (\beta^2_{i(e)} - \beta^2_{i(e)-1} + \beta^2_{i(e)} - 1 - \ldots - \beta^2_{j(e)+1} + \beta^2_{j(e)+1} - \beta^2_{j(e)})$$

$$= \sum_{e \in E_f} \sum_{l=j(e)+1}^{i(e)} (\beta^2_l - \beta^2_{l-1}).$$

Observem que al sumatori de B_f, el terme $\beta^2_l - \beta^2_{l-1}$ apareix per cada aresta e que connecta x amb $f(x) = \beta_i$ i $i \geq l$ amb un vèrtex y amb $f(y) = \beta_j$ i $j < l$. És a dir, apareix per cada aresta $e \in \partial L_l$, amb el que obtenim la remarca 1.

Remarca 2: $B_f \leq \sqrt{2k}||df||_2||f||_2$ Certament,

$$B_f = \sum_{e \in E} |f(e^+) + f(e^-)| \cdot |f(e^+) - f(e^-)|$$

$$\leq \left[\sum_{e \in E} (f(e^+) + f(e^-))^2\right]^{1/2} \left[\sum_{e \in E} (f(e^+) - f(e^-))^2\right]^{1/2}$$

$$\leq \sqrt{2k} \left[\sum_{e \in E} (f(e^+) + f(e^-))^2\right]^{1/2} ||df||_2$$

$$= \sqrt{2k} \left[\sum_{x \in V} f(x)^2\right]^{1/2} ||df||_2 = \sqrt{2k}||f||_2||df||_2$$

aplicant la desigualtat de Cauchy-Schwarz i el fet que $(a+b)^2 \leq 2(a^2+b^2)$.

Remarca 3: En el context d'aquest teorema, definim el **suport** d'una funció f com $sup(f) = x \in V : f(x) \neq 0$. Suposem que $|sup(f)| \leq \frac{|V|}{2}$. Aleshores, $B_f \geq h(X)||f||_2^2$.

Per demostrar aquesta remarca, observem que $\beta_0 = 0$ i que $|L_i| \leq \frac{|V|}{2}$ per $i = 1, \ldots, r$, aleshores, $|\partial L_i| \geq h(X)|L_i|$ per definició de $h(X)$. De la remarca 1 deduïm que:

$$B_f \geq h(X) \sum_{i=1}^{r} |L_i|(\beta^2_i - \beta^2_{i-1})$$

$$= h(X) \left[|L_r|\beta^2_r + (|L_{r-1}| - |L_r|)\beta^2_{r-1} + \ldots + (|L_1| - |L_2|)\beta^2_1\right]$$

$$h(X) \left[|L_r|\beta^2_r + \sum_{i=1}^{r-1} |L_i - L_{i+1}|\beta^2_i\right];$$

tanmateix, com $L_i - L_{i-1}$ és on f pren el valor β_i, el terme entre claudàtors és $||f||_2^2$.

Un cop provades les remarques tenim les eines que necessitem per acabar de demostrar el teorema. Sigui g una funció pròpia real de Δ (definida anteriorment en aquesta mateixa demostració) amb valor propi $k - \mu_1$. Definim $V^+ = x \in V : g(X) > 0$ i $f = \max g, 0$. Podem assumir que $|V^+| \leq \frac{|V|}{2}$ substituint g per $-g$ en cas que sigui necessari. Observem que $V^+ \neq \emptyset$, ja que $\sum_{x \in V} g(x) = 0$ i $g \neq 0$. Com $g \leq 0$ a $V - V^+$, per $x \in V^+$ tenim que

$$(\Delta f)(x) = kf(x) - \sum_{y \in V} A_{xy} f(y) = kg(x) - \sum_{y \in V^+} A_{xy} g(y)$$

$$\leq kg(x) - \sum_{y \in V} A_{xy} g(y) = (\Delta g)(x) = (k - \mu_1) g(x).$$

A partir d'aquesta estimació puntual, obtenim

$$||df||_2^2 = \langle \delta f | f \rangle = \sum_{x \in V^+} (\Delta f)(x) g(x) \leq (k - \mu_1) \sum_{x \in V^+} g(x)^2$$

$$\leq (k - \mu_1) ||f||_2^2.$$

Combinant les remarques 2 i 3 obtenim el següent

$$h(X) ||f||_2^2 \leq B_f \leq \sqrt{2k} ||df||_2 ||f||_2 \leq \sqrt{2k(k - \mu_1)} ||f||_2^2.$$

que després de cancel·lar termes ens dona el resultat que volem. □

La primera desigualtat del teorema 2.2.1 s'atribueix a N. Alon i Milman [5] mentre que la segona s'atribueix a Dodziuk [6]. El següent corol·lari relaciona el teorema anterior amb la definició de família d'expanders:

Corołari 2.2.2. *Sigui $(X_m)_{m \geq 1}$ una família de grafs finits, connexos, k-regulars i sense bucles tals que $|V_m| \to +\infty$ quan $m \to +\infty$. Aleshores la família $(X_m)_{m \geq 1}$ és una família d'expanders si i només si existeix $\epsilon > 0$ tal que $k - \mu_1(X_m) \geq \epsilon$ per tot $m \geq 1$.*

2.3 Comportament assimptòtic dels valors propis

Hem vist al corol·lari 2.2.2 una forma de caracteritzar famílies d'expanders a partir de la bretxa espectral, a més, es dedueix que la qualitat d'una família d'expanders és major com més gran és aquesta bretxa espectral. Malauradament, com veurem en aquesta secció, aquest valor no pot ser arbitràriament gran, ja que hi ha fites sobre el valor que pot prendre $\mu_1(X_m)$.

Teorema 2.3.1. [1, *Theorem* 1.3.1, *pg.* 18] *Sigui $(X_m)_{m \geq 1}$ una família de grafs finits, connexos, k-regulars i sense bucles tals que $|V_m| \to +\infty$ quan $m \to +\infty$. Aleshores:*

$$\liminf_{m \to +\infty} \mu_1(X_m) \geq 2\sqrt{k - 1}$$

Aquesta desigualtat s'atribueix a Alon i Boppana, i es pot veure la seva demostració a [*7, Proposition 4.2, pg. 9*].

Ara, per un graf X finit, connex i k-regular, sigui $\mu(X)$ el valor propi no trivial més petit de X, i rescatem la definició de circumferència d'un graf X (denotada per $g(X)$). Tenim el següent resultat:

Teorema 2.3.2. [1, *Theorem* 1.3.3, *pg.* 19] *Sigui* $(X_m)_{m\geq 1}$ *una família de grafs connexos, k-regulars i finits tals que* $g(X_m) \to +\infty$ *quan* $m \to +\infty$*. Aleshores:*

$$\limsup_{m\to+\infty} \mu(X_m) \leq -2\sqrt{k-1}$$

Aquest resultat s'atribueix a Li i Solé i es poden consultar més detalls del mateix al seu article a [8].

Aquests dos teoremes ens porten a la següent definició:

Definició 2.3.3. *Un graf X finit, connex i k-regular és un* ***graf de Ramanujan*** *i per cada valor propi no trivial* μ *de X tenim que* $|\mu| \leq 2\sqrt{k-1}$*.*

Si $(X_m)_{m\geq 1}$ és una familia de grafs k-regulars de Ramanujan i sense bucles, tals que $|V_m| \to +\infty$ quan $m \to +\infty$ aleshores és clar veure que els X_m assoleixen la major bretxa espectral possible, i per tant proporcionen una família d'*expanders* que és òptima des del punt de vista del seu espectre.

Si és d'interès del lector, el capítol 1 del llibre *Elementary Number Theory, Group Theory, and Ramanujan Graphs*[1] amplia els continguts d'aquest capítol, especialment la secció 1.4, que dona resultats addicionals sobre el comportament asimptòtic que, si bé tenen relació amb el treball, s'allunyen de l'objectiu d'aquest.

Capítol 3

Teoria de Nombres

En aquest capítol donarem algunes definicions i resultats de teoria de nombres que necessitarem per construir la família d'*expanders* més endavant. Eventualment, parlarem breument sobre cossos, que denotarem per K quan no ens referim a cap cos en concret. En el context d'aquest treball, K serà un cos commutatiu, llevat que s'especifiqui el contrari.

Definim l'anell dels **enters de Gauss** com segueix:

$$\mathbb{Z}[i] = \{a + bi : \, a, b \in \mathbb{Z}, \, i^2 = -1\}$$

Si $\alpha = a + bi$ és un element de $\mathbb{Z}[i]$, el seu conjugat és $\bar{\alpha} = a - bi$. Notem que qualsevol suma de dos enters es pot factoritzar com:

$$n = a^2 + b^2 = (a + bi)(a - bi) = \alpha\bar{\alpha}, \, \alpha \in \mathbb{Z}[i]$$

De la mateixa manera, definim un altre anell, que es coneix com els **quaternions enters**, que denotarem per $\mathbb{H}(\mathbb{Z})$ i es defineix com:

$$\begin{aligned}\mathbb{H}(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k : \, & a_0, a_1, a_2, a_3 \in \mathbb{Z}, \\ & i^2 = j^2 = k^2 = -1, \, ij = k, \, jk = i, \, ki = j, \\ & ji = -k, \, kj = -i, \, ik = -j\}.\end{aligned}$$

Notem que $\mathbb{H}(\mathbb{Z})$ no és commutatiu. Com amb $\mathbb{Z}[i]$, podem definir el conjugat d'un element de $\mathbb{H}(\mathbb{Z})$ de la següent manera:

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k$$

$$\bar{\alpha} = a_0 - a_1 i - a_2 j - a_3 k$$

Si α és un element de $\mathbb{H}(\mathbb{Z})$, podem definir la seva norma com $N(\alpha) = \alpha\bar{\alpha} = \bar{\alpha}\alpha = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Aquesta norma és multiplicativa ($N(\alpha\beta) = N(\alpha)N(\beta)$ i, de forma similar al que hem vist amb els enters de Gauss, els quaternions enters ens serveixen per factoritzar les sumes de quatre quadrats.

Direm que un element α de $\mathbb{H}(\mathbb{Z})$ és una **unitat** si és invertible a $\mathbb{H}(\mathbb{Z})$, o, el que és equivalent, si $N(\alpha) = 1$.

Per $k \geq 2$ i $n \in \mathbb{N}$ denotarem per $r_k(n)$ el nombre de representacions de n com a suma de k quadrats, o, el que és equivalent, el nombre de solucions enteres de l'equació diofàntica $x_0^2 + x_1^2 + \ldots + x_{k-1}^2 = n$:

$$r_k(n) = \left| \left\{ (x_o, \ldots, x_{k-1} =\in \mathbb{Z}^k : \sum_{i=0}^{k-1} x_i^2 = n \right\} \right|$$

Ara donarem un resultat, enunciat per Fermat l'any 1640 i demostrat per Euler al 1793, sobre la suma dels quadrats de dos enters. Recordem que si $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$, diem que a i b són congruents mòdul n (i denotem per $a \equiv b\,(mod.\, n)$) si la seva diferència és divisible per n. Si tenim q primer o potència de primer ($q = p^m$ per p primer) denotarem per $\mathbb{F}_q$ el cos finit de q elements, i per $\mathbb{F}_q^\times$ el grup multiplicatiu dels elements de $\mathbb{F}_q$ diferents de zero.

Teorema 3.0.1. [1, *Theorem* 2.2.7, *pg.* 42] *Sigui p un primer senar. Les següents afirmacions són equivalents:*

a) $p \equiv 1 \pmod 4$*;*

b) -1 és un quadrat a $\mathbb{F}_p$ *(és a dir, existeix* $x \in \mathbb{Z}$ *tal que* $x^2 \equiv -1 \pmod p$)

c) p és la suma de dos quadrats (i, per tant, $r_2(p) > 0$*)*

Demostració: Aquest resultat és àmpliament conegut i, per tant, fàcilment es pot trobar una demostració del mateix. Una possibilitat és a [1], on a la pàgina 43 hi ha una prova detallada, extreta de [9].

En particular, per la construcció de la família d'*expanders* dessitjada necessitem caracteritzar $r_2(n)$ i $r_3(n)$. El següent resultat, conegut com a **fòrmula de Legendre**, ens donarà el que necessitem. Abans, però, hem de donar notació addicional.

Per $n \in \mathbb{N}$ definim:

- $d_1(n)$ com el nombre de divisors de n que són congruents amb 1 mòdul 4;
- $d_3(n)$ com el nombre de divisors de n que són congruents amb 3 mòdul 4;
- $d(n)$ com el nombre de divisors de n.

Teorema 3.0.2. [1, *Theorem* 2.2.11, *pg.* 45] *Per* $n \in \mathbb{N}$, $n > 0 :$ $r_2(n) = 4(d_1(n) - d_3(n))$.

Demostració: Una demostració d'aquest resultat es pot trobar a la secció 2.2 de [1], juntament amb una sèrie de resultats que ajuden a la mateixa prova, però que no he inclòs per allunyar-se de l'objectiu principal del treball.

Malauradament, no tenim una caracterització per $r_3(n)$ tan directa com la que dona el teorema anterior per $r_2(n)$, però els següents corol·laris ens permeten estimar aquest valor.

Corołari 3.0.3. *Per tot* $\epsilon > 0 :$ $r_2(n) = \mathcal{O}_\epsilon(n^\epsilon)$.

Demostració: Del teorema 3.0.2 es pot extreure que $r_2(n) \leq 4(d_1(n)+d_3(n)) \leq 4d(n)$.. El lector pot comprovar que $d(n) = \mathcal{O}_\epsilon(n^\epsilon)$. $\square$

Corolari 3.0.4. *Per tot* $\epsilon > 0$ *:* $r_3(n) = \mathcal{O}_\epsilon(n^{\frac{1}{2}+\epsilon})$.

Demostració:

$$r_3(n) = \sum_{k=0}^{[\sqrt{n}]} r_2(n-k^2)$$

$$\leq C(\epsilon) \sum_{k=0}^{[\sqrt{n}]} (n-k)^\epsilon \quad \text{pel corol·lari 3.0.3}$$

$$\leq C(\epsilon) n^{\frac{1}{2}+\epsilon}. \quad \square$$

L'estructura dels grafs construïts al capítol 5 depèn de l'equació $x^2 \equiv p \pmod{q}$ quan p i q són primers senars. Un resultat que ens serà molt útil en aquest cas és la famosa **Llei de reciprocitat quadràtica** enunciada com a conjectura per Euler i demostrada posteriorment per Gauss. Abans d'enunciar el resultat, però, cal donar una definició prèvia:

Definició 3.0.5. *Sigui p un primer senar i* $m \in \mathbb{Z}$*. Definim el* ***símbol de Legendre*** $\left(\frac{m}{p}\right)$ *com:*

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divideix } m; \\ 1 & \text{si } p \text{ no divideix } m \text{ i } m \text{ és un quadrat mòdul } p; \\ -1 & \text{si } p \text{ no divideix } m \text{ i } m \text{ no és un quadrat mòdul } p. \end{cases}$$

Com a propietat a destacar tenim que el símbol de Legendre és multiplicatiu, és a dir:

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \quad (m, n \in \mathbb{Z}).$$

Teorema 3.0.6. *(Llei de reciprocitat quadràtica) Sigui p un primer senar. Aleshores es compleixen:*

a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

c) si q és un primer senar diferent de p: $\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)$

Demostració: Hi ha moltes demostracions de la llei de reciprocitat quadràtica, fent servir arguments molt variats. A [1; 2.3.2] podem trobar-ne una que està extreta de [10] i que fa servir els arguments que més s'ajusten al que es tracta en aquest treball (tot i que ampliats).

Tornem a rescatar l'anell dels quaternions enters definit abans. En general, aquesta definició la podem aplicar fent servir, en comptes de $\mathbb{Z}$ un cos K, i llavors els quaternions sobre K (denotat $\mathbb{H}(K)$) és el K-mòdul lliure sobre els símbols 1,i,j,k. És a dir, $\mathbb{H}(K) = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in K\}$ on i,j,k compleixen les mateixes igualtats descrites a $\mathbb{H}(\mathbb{Z})$

Volem identificar aquest anell amb el conjunt de les matrius 2 x 2 amb coeficients en un cos K, més específicament, ens interessen els cossos finits $\mathbb{F}_q$.

Definició 3.0.7. *Donat un anell R, definim la característica de R com l'enter positiu m més petit tal que* $0 = m \cdot 1 = 1 + 1 + \ldots + 1$ *(mvegades). Si no existeix aquest m llavors la característica de R serà 0.*

Exemple 3.0.8. Els racionals $\mathbb{Q}$, els reals $\mathbb{R}$ i els complexos $\mathbb{C}$ tenen característica 0, mentre que per $q = p^l$ amb p primer, el cos finit $\mathbb{F}_q$ té característica p.

Proposició 3.0.9. *Sigui K un cos amb característica diferent de 2. Suposem que existeixen* $x, y \in K$ *tals que* $x^2 + y^2 + 1 = 0$*. Aleshores* $\mathbb{H}(K)$ *és isomorf a l'àlgebra* $M_2(K)$ *de les matrius 2 x 2 amb coeficients a K.*

La següent demostració és especialment interessant, ja que no només prova el resultat sinó que dona una construcció explícita d'aquest isomorfisme, que ens serà útil posteriorment, quan construïm la família d'*expanders*.

Demostració: Sigui $\psi : \mathbb{H}(K) \to M_2(K)$ definit per:

$$\psi(a_0 + a_1 i + a_2 j + a_3 k) = \begin{pmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix}$$

És fàcil comprovar, realitzant els càlculs pertinents, que $\psi(q_1 q_2) = \psi(q_1)\psi(q_2)$ per $q_1, q_2 \in \mathbb{H}(K)$. Com ψ és una aplicació K-lineal entre dos K-espais vectorials de la mateixa dimensió (4), per provar que ψ és un isomorfisme n'hi ha prou amb comprovar la injectivitat. Aplicant àlgebra lineal ens trobem que $\psi(a_0 + a_1 i + a_2 j + a_3 k) = 0$ ens porta a un sistema d'equacions 4 x 4 lineal en les variables a_0, a_1, a_2, a_3 amb determinant

$$\begin{vmatrix} 1 & x & 0 & y \\ 0 & -y & 1 & x \\ 0 & -y & -1 & x \\ 1 & -x & 0 & -y \end{vmatrix} = -4(x^2 + y^2) = 4 \neq 0$$

, ja que la característica de K és diferent de 2. □

Ara només ens falta un resultat que ens permeti afirmar que, efectivament existeixen $x, y \in K$ tals que $x^2 + y^2 + 1 = 0$. Pel context d'aquest treball, només ens caldrà provar-ho quan $K = \mathbb{F}_q$ per algun primer senar q.

Proposició 3.0.10. *Sigui q un primer senar. Llavors existeixen* $x, y \in \mathbb{F}_q$ *tals que* $x^2 + y^2 + 1 = 0$.

Demostració: Incloent el 0, hi ha $\frac{q+1}{2}$ quadrats a $\mathbb{F}_q$. Definim

$$A_+ = \{1 + x^2 : x \in \mathbb{F}_q\}; \quad A_- = \{-y^2 : y \in \mathbb{F}_q\}.$$

Com $|A_+| = |A_-| = \frac{q+1}{2}$ tenim que $A_+ \cap A_- \neq \emptyset$, el que prova el resultat. □

Tornem ara als quaternions enters, a [1; 2.6] es pot trobar una secció dedicada a resultats sobre l'aritmètica dels quaternions enters que, si bé dona informació addicional, no és en el que es centra aquest treball.

Nosaltres centrarem la nostra atenció al conjunt de quaternions enters que tenen norma p^k on p és un primer senar. Primer enunciarem el següent teorema, atribuït a Jacobi:

Teorema 3.0.11. [1, *Theorem* 2.4.1, *pg.* 52] *Sigui n un enter positiu senar. Aleshores* $r_4(n) = 8\sum_{d|n} d$.

Demostració: La demostració d'aquest teorema és força extensa i no és l'objectiu principal d'aquest treball, si és de l'interès del lector, pot trobar-ne una demostració detallada a [1;2.4], o també una de Dirichlet a [11].

El teorema ens diu que $a_o^2 + a_1^2 + a_2^2 + a_3^2 = p$ té $8(p + 1)$ solucions enteres, cadascuna d'elles corresponent a un quaternió enter de norma p. Si $p \equiv 1 \pmod 4$, un dels a_i és senar i la resta parells. En canvi, si $p \equiv 3 \pmod 4$, un dels a_i és parell i la resta senars. En qualsevol cas, un dels coeficients, anomenem-lo a_i^0 està diferenciat de la resta.

Si $a_i^0 \neq 0$, aleshores, d'entre els vuit quaternions de la forma $\epsilon\alpha$ associats a α on ϵ és una unitat, exactament un tindrà $|a_i^0|$ com la 0-èssima component (és a dir, a la posició a_0). Escollirem aquest com a distingit. En el cas que $a_i^0 = 0$, que pot passar quan $p \equiv 3 \pmod 4$, aleshores dos associats $\epsilon\alpha$ i $-\epsilon\alpha$ tindran cadascun $a_0 = 0$, i podrem escollir qualsevol dels dos com a distingit.

Per tant, hi ha p+1 solucions distingides de $a_o^2 + a_1^2 + a_2^2 + a_3^2 = p$, això ens determina el conjunt $S_p = \{\alpha_1, \bar{\alpha}_1, \ldots, \alpha_s, \bar{\alpha}_s, \beta_1, \ldots, \beta_t\}$, on els α_i tenen $\alpha_0^{(i)} > 0$ i els β_j tenen $\beta_0^{(j)} = 0$. És a dir, S_p són els p+1 quaternions distingits de norma p.

Definició 3.0.12. *Una* ***paraula reduïda*** *sobre* S_p *és una paraula sobre l'alfabet* S_p *que no té subparaules de la forma* $\alpha_i\bar{\alpha}_i, \bar{\alpha}_i\alpha_i, \beta_j^2$ *(i = 1, . . . , s; j = 1, . . . , t).*

La ***mida*** *d'una paraula és el nombre de símbols que hi apareixen en ella.*

Ara enunciarem un corol·lari que necessitarem més endavant, quan demostrem que la família que volem construir es tracta veritablement d'una família d'*expanders*. Enunciaré també el teorema del qual prové, que és atribuït a Dickson [12]. Si és de l'interès del lector, pot trobar la demostració dels dos resultats a [1; 2.6.12 i 2.6.13].

Teorema 3.0.13. [1, *Theorem* 2.6.13, *pg.* 68] *Siguin* $k \in \mathbb{N}$ *i* $\alpha \in \mathbb{H}(\mathbb{Z})$ *tal que* $N(\alpha) = p^k$. *Aleshores* α *admet una factorització única* $\alpha = \epsilon p^r w_m$ *on* ϵ *és una unitat a* $\mathbb{H}(\mathbb{Z})$, w_m *és una paraula reduïda de mida m sobre* S_p *i* $k = 2r + m$.

Abans d'enunciar el corol·lari, definim el següent subconjunt de $\mathbb{H}(\mathbb{Z})$:

$$\Lambda' = \{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod 2\}$$

Corołari 3.0.14. *Tots els elements $\alpha \in \Lambda'$ amb $N(\alpha) = p^k$ tenen una factorització única $\alpha = \pm p^r w_m$ on $r \in \mathbb{N}, w_m$ és una paraula reduïda de mida m sobre S_p i $k = 2r + m$.*

Capítol 4

Els grups $PGL_2(q)$ i $PSL_2(q)$

La família de grafs $X^{p,q}$, que definirem al capítol 5, estarà associada als dos grups finits $PGL_(q)$ i $PSL_2(q)$. Dedicarem aquest quart capítol a definir-los i donar alguns resultats sobre ells que seran útils posteriorment.

Sigui K un cos, que, llevat que s'indiqui el contrari, serà commutatiu per tot el capítol. Denotem per $GL_2(K)$ el grup de les matrius 2x2 amb coeficients a K invertibles, és a dir, aquelles que tenen determinant diferent de zero. Anomenem a aquest grup **Grup Lineal** de grau 2 sobre K.

Anomenarem **Grup Lineal Especial** (de grau 2 sobre K) i denotarem per $SL_2(K)$ el subgrup de $GL_2(K)$ que té determinant 1. En particular, aquest grup és el nucli de l'aplicació determinant $det : GL_2(K) \to K^\times$, i és un subgrup normal de $GL_2(K)$.

Aleshores denotem per $PGL_2(K)$ el grup quocient:

$$PGL_2(K) = GL_2(K)/\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \quad \lambda \in K^\times \right\}.$$

I per $PSL_2(K)$ el grup quocient:

$$PSL_2(K) = SL_2(K)/\left\{ \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix} : \quad \epsilon = \pm 1 \right\}.$$

Per visualitzar una mica millor com són aquests dos grups, sigui $P^1(K) = K \cup \{\infty\}$. Incrustarem $PGL_2(K)$ i $PSL_2(K)$ al grup de les permutacions de $P^1(K)$ denotat per $SymP^1(K)$. A cada matriu $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ li associem la transformació lineal $\varphi_A : P^1(K) \to P^1(K)$, definida per:

$$\varphi_A(z) = \frac{az+b}{cz+d}.$$

Definim $\varphi(\infty) = \begin{cases} \frac{a}{c} & \text{si } c \neq 0, \\ \infty & \text{si } c = 0. \end{cases}$ i també assignem $\varphi_A(\frac{-d}{c}) = \infty$.

Per tant, obtenim un morfisme de grups $\varphi : GL_2(K) \to SymP^1(K)$ on $\varphi(A) = \varphi_A$ i $PGL_2(K)$ s'identifica $\varphi(GL_2(K))$ i $PSL_2(K)$ s'identifica $\varphi(SL_2(K))$.

En el nostre cas, tindrem que $K = \mathbb{F}_q$ el cos finit d'ordre q, i escriurem $GL_2(q)$, $SL_2(q)$, $PGL_2(q)$ i $PSL_2(q)$ pels quatre grups que hem definit abans.

Proposició 4.0.1. *Es compleix que:*

a) $|GL_2(q)| = q(q-1)(q^2-1)$

b) $SL_2(q) = |PGL_2(q)| = q(q^2-1)$

c) $|PSL_2(q) = \begin{cases} q(q^2-1) & \text{si } q \text{ és parell} \\ \frac{q(q^2-1)}{2} & \text{si } q \text{ és senar.} \end{cases}$

Demostració: a) Una matriu 2 x 2 de $GL_2(q)$ s'obté escollint com a primera columna un vector diferent de zero de $\mathbb{F}_q$, que implica q^2-1 possibles eleccions, i com a segona columna s'escull un altre vector de $\mathbb{F}_q$ que sigui linealment independent del primer escollit, i això són $q^2 - q$ possibles eleccions. Per tant, el total son $q(q-1)(q^2-1)$.

b) i c) s'obtenen partint de a) i aplicant resultats de teoria de grups. □

Recordem que un grup G és **simple** si els seus únics subgrups normals són $\{1\}$ i el total. El següent teorema és un resultat demostrat per Jordan l'any 1861.

Teorema 4.0.2. [1, *Theorem* 3.2.2, *pg.* 74] *Sigui K un cos amb* $|K| \geq 4$. *Aleshores* $PSL_2(K)$ *és un grup simple.*

Demostració: Es pot trobar una demostració detallada d'aquest teorema a [1; 3.2]. □

El resultat és interessant, ja que les propietats dels grafs $X^{p,q}$ que definirem més endavant depenen d'algunes de les propietats estructurals de $PSL_2(q)$. El fet que sigui simple es fa servir, per una banda, per determinar quins $X^{p,q}$ són bipartits, i per l'altra, per establir les propietats d'expansió dels $X^{p,q}$'s.

Així mateix, per estudiar el fet que els $X^{p,q}$ siguin connexos necessitem tenir alguns resultats sobre l'estructura dels subgrups de $PSL_2(q)$.

Abans, però, recordarem que si σ és una permutació d'un conjunt X i $x \in X$, l'**òrbita de x sota** σ és $\Omega_x = \{\sigma^k(x) : k \in \mathbb{Z}$.

Així mateix, recordem també que, donat un grup G i un element $x \in X$ l'**estabilitzador** de x en G és $G_x = \{g \in G | g \cdot x = x\}$.

Lema 4.0.3. *Sigui* σ *una permutació d'un conjunt X. Si* σ *té ordre primer p, aleshores cada òrbita de* σ *en X té o 1 o p elements.*

Demostració: Sigui H el subgrup generat per σ a $Sym(X)$. Per $x \in X$, tenim que $|\Omega_x| = \frac{|H|}{|Hx|}$ on $H_x = \{\alpha \in H : \alpha(x) = x\}$ és l'estabilitzador de x en H. Per suposició $|H| = p$, així que o bé $|H_x| = 1$ i $|\Omega_x| = p$ o bé $|H_x| = p$ i $|\Omega_x| = 1$. □

El següent resultat s'atribueix a Cauchy i parla de l'existència d'elements d'ordre primer en grups finits. Aquest resultat posteriorment va ser reemplaçat pels teoremes de Sylow.

Teorema 4.0.4. [1, *Theorem* 3.3.2, *pg.* 77] *Sigui G un grup finit i p un nombre primer. Si p divideix $|G|$ aleshores G conté algun element d'ordre p.*

Demostració: Una demostració d'aquest teorema es pot trobar a [1; 3.3], que ho demostra aplicant el lema anterior.

Definició 4.0.5. *Direm que un grup G és **metabelià** si admet un subgrup normal N tal que tant N com G/N són abelians.*

En particular, els grups abelians són metabelians i els grups metabelians són resolubles. Els subgrups d'un grup metabelià també són metabelians.

Hi ha una llista atribuïda a Dickson l'any 1901 que conté, llevat d'isomorfisme, tots els subgrups del $PSL_2(q)$ amb q potència de primer, podem trobar la referència a [17]. El que és important d'aquesta llista és que tots els subgrups de $PSL_2(q)$, llevat del total, són metabelians, amb les següents excepcions:

1. $Sym(4)$, que és resoluble però no metabelià.
2. $Alt(5)$, que no és abelià.

Ara enunciarem un resultat que serà útil posteriorment, durant la demostració que $X^{p,q}$ és una família d'*expanders*.

Teorema 4.0.6. [1, *Theorem* 3.3.4, *pg.* 78] *Sigui q primer. Sigui H un subgrup de $PSL_2(q)$ diferent del total tal que $|H| > 60$. Aleshores H és metabelià.*

Demostració: La demostració d'aquest teorema surt directa dels dos resultats següents, que no demostraré perquè fan servir eines que no estan incloses en aquest treball, però es poden consultar a [1;3.3].

Proposició 4.0.7. *Sigui q primer i H un subgrup de $PSL_2(q)$ diferent del total. Si q divideix $|H|$ aleshores H és metabelià.*

Proposició 4.0.8. *Sigui q primer i H un subgrup de $PSL_2(q)$. Si $|H| > 60$ i q no divideix $|H|$ aleshores H té un subgrup abelià d'índex com a molt 2, en particular, H és metabelià.*

Finalment, donarem un últim resultat sobre els grups $PGL_2(q)$ i $PSL_2(q)$, però abans hem de donar una definició.

Definició 4.0.9. *Sigui G un grup. Una **representació** de G és una parella (π, V), on V és un espai vectorial complex i π és un morfisme $G \to GL(V)$ (on $GL(V)$ és el grup de les permutacions lineals de V). El **grau** de (π, V) és la dimensió $dim_{\mathbb{C}}V$ de V.*

Exemples 4.0.10. Veiem alguns exemples de representacions:

a) El morfisme constant $G \to GL(V)$ defineix la representació trivial de G a V.

b) Cada morfisme $G \to \mathbb{C}^\times$ dona lloc a una representació de grau 1 de G a $\mathbb{C}$.

c) Sigui X un G-espai, és a dir, un conjunt no buit dotat d'un morfisme $G \to Sym(X)$ on Sym(X) és el grup de permutacions sobre X. Sigui $\mathbb{C}X$ el conjunt de funcions $X \to \mathbb{C}$ que valen zero excepte a subconjunts finits de X. La **representació de permutacions** λ_X de G a $\mathbb{C}X$ està definida per

$$(\lambda_X(g)f)(x) = f(g^{-1} \cdot x),$$

on $f \in \mathbb{C}X$, $g \in G$, $x \in X$.

Definició 4.0.11. *Sigui (π, V) una representació de G. Un subespai W de V és **invariant** si per cada $g \in G : \pi(g)(W) = W$.*

Definició 4.0.12. *Una representació (π, V) amb $V \neq \{0\}$ és **irreductible** si no té cap subespai no trivial que sigui invariant.*

Ara donarem un resultat que s'atribueix a Frobenius a [18].

Teorema 4.0.13. [1, *Theorem* 3.5.1, *pg.* 102] *Sigui $q \geq 5$ un primer. El grau de qualsevol representació no trivial de $PSL_2(q)$ és, com a mínim $\frac{q-1}{2}$.*

Demostració: A més de la referència ja esmentada, la secció 3.3 de [1] també va dedicada a provar aquest resultat, fent servir eines que queden fora del que tractem en aquest treball. □

Aquest resultat serà útil al capítol següent, ja que ens permetrà veure que pels grafs $X^{p,q}$ que construirem, la multiplicitat dels valors propis no trivials és com a mínim $\frac{q-1}{2}$.

Capítol 5

Els Grafs $X^{p,q}$

Finalment, en aquest capítol donarem una construcció explícita d'una família d'*expanders*, així com la demostració de què es tracta efectivament d'una. Per això ens basarem en el que es coneix com a graf de Cayley d'un grup, i entraran en joc diversos conceptes dels capítols anteriors.

5.1 Grafs de Cayley

Sigui G un grup, no necessàriament finit, i sigui S un subconjunt finit i no buit de G. Suposarem que S és simètric, és a dir, que per cada element de S, també tenim el seu invers, o, el que és el mateix, $S = s^{-1}$.

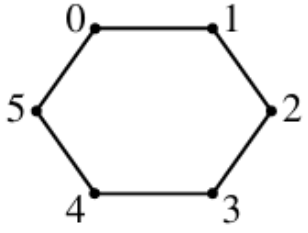
Definició 5.1.1. *Definim el* ***Graf de Cayley*** $\mathcal{G}(G, S)$ *com aquell graf que té per conjunt de vèrtexs* $V = G$ *i com a conjunt d'arestes*

$$E = x, y : x,\ y \in G; \exists s \in S : y = xs.$$

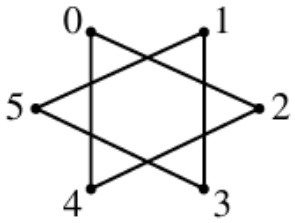
És a dir, dos vèrtexs de $\mathcal{G}(G, S)$ seran adjacents si podem obtenir un d'ells com a resultat de multiplicar per la dreta un element de S a l'altre. Observem que, com S és simètric, la relació d'adjacència dels vèrtexs també és simètrica, i, per tant, els grafs resultants són no dirigits.

Exemples 5.1.2. Ara veurem alguns exemples de grafs de Cayley:

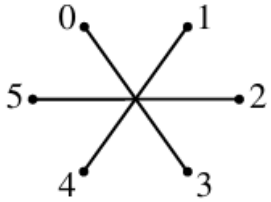
a) $G = \mathbb{Z}/6\mathbb{Z}, \quad S = \{1, -1\}$



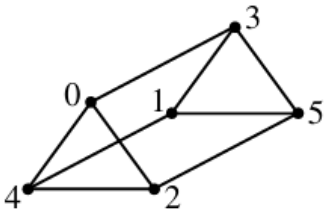
b) $G = \mathbb{Z}/6\mathbb{Z}, \quad S = \{2, -2\}$



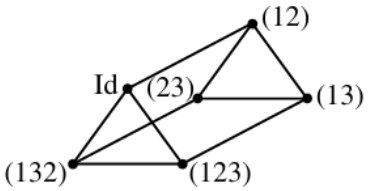
c) $G = \mathbb{Z}/6\mathbb{Z}, \quad S = \{3\}$



d) $G = \mathbb{Z}/6\mathbb{Z}, \quad S = \{2, -2, 3\}$



e) $G = Sym(3), \quad S = \{(123), (132), (12)\}$



Els exemples d) i e) ens mostren que dos grafs de Cayley isomorfs no tenen per què tenir com a origen grups que siguin isomorfs.

Ara enunciarem algunes propietats interessants dels grafs de Cayley:

Proposició 5.1.3. *Sigui $\mathcal{G}(G,S)$ un graf de Cayley, sigui $k = |S|$. Aleshores:*

a) $\mathcal{G}(G,S)$ és simple, k-regular i vèrtex-transitiu.

b) $\mathcal{G}(G,S)$ no té bucles si i només si $1 \notin S$ on 1 es refereix a l'element neutre de G.

c) $\mathcal{G}(G,S)$ es connex si i només si S genera G.

d) Si existeix un morfisme χ de G al grup multiplicatiu $1, -1$ tal que $\chi(S) = -1$, aleshores $\mathcal{G}(G,S)$ és bipartit. El recíproc es compleix si $\mathcal{G}(G,S)$ és connex.

Demostració:

a) La matriu d'adjacència de $\mathcal{G}(G,S)$ és

$$A_{xy} = \begin{cases} 1 & \text{si existeix} s \in S \text{tal que} y = xs; \\ 0 & \text{altrament.} \end{cases}$$

D'aqui es veu que $\mathcal{G}(G,S)$ és simple i k-regular. D'altra banda, G actua per l'esquerra en $\mathcal{G}(G,S)$ per multiplicació per l'esquerra, i aquesta acció és transitiva a $V = G$, per tant, queda provada la vèrtex-transitivitat.

b) Aquest resultat és directe.

c) $\mathcal{G}(G,S)$ és connex si i només si cada $x \in G$ està connectat a $1 \in G$ per un camí d'arestes. Però això es compleix si i només si cada $x \in G$ es pot escriure com una paraula reduïda en l'alfabet S, és a dir, si S genera G.

d) Donat el morfisme $\chi : G \to \pm 1$, podem definir la següent bipartició de $\mathcal{G}(G,S)$:

$$V_{\pm} = \{x \in G : \chi(x) = \pm 1\}$$

Per veure el recíproc suposarem que $\mathcal{G}(G,S)$ és connex i bipartit. Denotem per V_+ la classe de la bipartició per $1 \in G$ i per V_- l'altra (observem que $S \subseteq V_-$). Aleshores definim una aplicació $\chi : G \to \pm 1$ com

$$\chi(x) = \begin{cases} 1 & \text{si } x \in V^+ \\ -1 & \text{si } x \in V^- \end{cases}$$

Falta comprovar que χ és un morfisme de grups. Primer de tot observem que, com S genera G, $\chi(x) = (-1)^{l_S(x)}$ on $l_S(x)$ és la longitud de paraula reduïda de x respecte a S, és a dir, la distància entre x i 1 a $\mathcal{G}(G,S)$. Aplicant que $G = V_+ \cup V_+$ demostra que χ és un morfisme de grups. □

5.2 Construint $X^{p,q}$

Siguin p i q dos primers senars diferents. Al capítol 3 hem definit un conjunt S_p de p + 1 quaternions distingits de norma p. Considerem ara la reducció mòdul q:

$$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$$

Per la proposició 3.0.10 existeixen enters x, y tals que $x^2 + y^2 + 1 \equiv 0(mod.\, q)$. A més, per la proposició 3.0.9, qualsevol elecció de x i y determina un isomorfisme

$$\psi_q : \mathbb{H}(\mathbb{F}_{\text{ii}}) \to M_2(\mathbb{F}_q)$$

on recordem que $M_2(K)$ denota les matrius 2x2 amb coeficients a K, i que compleix les següents propietats:

a) $N(\alpha) = \det \psi_q(\alpha)$ per $\alpha \in \mathbb{H}(\mathbb{F}_q)$;

b) Si $\alpha \in \mathbb{H}(\mathbb{F}_q)$ és real (és a dir, si $\alpha = \bar{\alpha}$), aleshores $\psi_q(\alpha)$ és una matriu escalar.

Per $\alpha \in S_p$ observem que $\psi_q(\tau_q(\alpha))$ pertany al grup $GL_2(q)$ dels invertibles de $M_2(\mathbb{F}_q)$), ja que $N(\alpha) = p \neq q$. També tenim que $\psi_q(\tau_q(\alpha\bar{\alpha})) = \psi_q(\tau_q(\bar{\alpha}\alpha))$ és una matriu escalar diferent de zero a $GL_2(q)$. Ara prenem el morfisme

$$\varphi : \mathrm{GL}_2(q) \to PGL_2(q)$$

I definim

$$S_{p,q} = (\varphi \circ \psi_q \circ \tau_q)(S_p)$$

Que és un subconjunt simètric de $PGL_2(q)$.

Lema 5.2.1. *Si q és prou gran respecte a p (posem $q > 2\sqrt{p}$), aleshores $|S_{p,q}| = p + 1$.*

Demostració: Siguin $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ i $\beta = b_0 + b_1 i + b_2 j + b_3 k$ dos elements diferents de S_p, aleshores, per algun $i \in 0, 1, 2, 3$ tenim que $a_i \neq b_i$. Com α i β pertanyen a S_p sabem que $N(\alpha) = N(\beta) = p$, i per tant $a_j, b_j \in (-\sqrt{p}, \sqrt{p})$ per tot $j \in 0, 1, 2, 3$. Aleshores si $q > 2\sqrt{p}$ tenim que $a_i \equiv b_i \pmod q$ i $\tau_q(\alpha) \neq \tau_q(\beta)$. Ara definim $A = (\psi_q \circ \tau_q)(\alpha)$ y $B = (\psi_q \circ \tau_q)(\beta)$, de manera que $A \neq B$ a $\mathrm{GL}_2(q)$. Suposem per contradicció que $\varphi_A = \varphi_B$ a $PGL_2(q)$, aleshores existeix $\lambda \in \mathbb{F}_q^{\times}$ tal que $\lambda \neq 1$ i $A = \lambda B$. Prenent determinants obtenim que $p = detA = \lambda^2 detB = \lambda^2 p$, i d'aquí es dedueix que $\lambda^2 = 1$ o $\lambda = -1$. A partir de $A = -B$ obtenim que $\alpha \equiv -\beta(mod.q)$, és a dir,$\alpha_j \equiv -\beta_j(mod.q)$ per cada $j \in 0, 1, 2, 3$. Com $q > 2\sqrt{p}$ deduim que $a_j = -b_j$, i per tant $\alpha = -\beta$. Per suposició tenim que $a_0, b_0 \geq 0$, cosa que implica que $a_0 = b_0 = 0$ i, per tant, $\beta = \bar{\alpha}$, però això entra en contradicció amb la definició de S_p ja que si $\alpha \in S_p$ té $a_0 = 0$ aleshores necessàriament $\bar{\alpha} \notin S_p$. □

Un cop demostrat aquest lema definirem els grafs $X^{p,q}$ de la següent manera:

Si p és un quadrat mòdul q, és a dir, $(\frac{p}{q}) = 1$ aleshores $S_{p,q}$ es troba inclòs a $PSL_2(q)$. Per tant, definim $X^{p,q}$ com el graf de Cayley de $PSL_2(q)$ respecte de $S_{p,q}$:

$$X^{p,q} = \mathcal{G}(PSL_2(q), S_{p,q})$$

Per contra, si p no és un quadrat mòdul q, és a dir, $(\frac{p}{q}) = -1$, aleshores $S_{p,q}$ es troba inclós a $PGL_2Q - PSL_2(q)$. Per tant, definim $X^{p,q}$ com el graf de Cayley de $PGL_2(q)$ respecte de $S_{p,q}$:

$$X^{p,q} = \mathcal{G}(PGL_2(q), S_{p,q})$$

Teorema 5.2.2. [1, *Theorem* 4.2.2, *pg.* 114] *Siguin p,q dos primers senars diferents tals que* $q > 2\sqrt{p}$. *Els grafs* $X^{p,q}$ *són (p+1)-regulars, connexos i de Ramanujan. A més:*

a) $Si(\frac{p}{q}) = 1$ *aleshores* $X^{p,q}$ *és un graf no bipartit amb* $\frac{q(q^2-1)}{2}$ *vèrtexs i satisfà que* $g(X^{p,q}) \geq 2\log_p(q)$.

b) $Si(\frac{p}{q}) = -1$ *aleshores* $X^{p,q}$ *és un graf bipartit amb* $q(q^2-1)$ *vèrtexs i satisfà que* $g(X^{p,q}) \geq 4\log_p(q) - \log_p(4)$.

Aquest teorema s'atribueix a Lubotzky i una demostració detallada es pot trobar a [7], el que és del nostre interès i que provarem tot seguit és el fet que $X^{p,q}$ siguin grafs connexos, o, el que és equivalent (proposició 5.1.3c)), que $S_{p,q}$ genera tant $PSL_2(q)$ com $PGL_2(q)$.

5.3 Connexió dels grafs $X^{p,q}$

Abans de provar el resultat desitjat, hem de definir una sèrie d'elements que necessitarem per facilitar la demostració. Amb ells, introduirem una nova família de grafs (p+1)-regulars $Y^{p,q}$ que resultaran ser isomorfs als $X^{p,q}$.

Comencem amb un primer senar p. Al capítol 3 vam definir el subconjunt Λ' de $\mathbb{H}(\mathbb{Z})$ com

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod 2 \,\text{o}\, \alpha \equiv i+j+k \pmod 2, N(\alpha) \,\text{és una potència de p}\}.$$

A Λ' definim la següent relació d'equivalència: $\alpha \sim \beta$ si existeixen $m, n \in \mathbb{N}$ tals que $p^m\alpha = \pm p^n\beta$. Denotem per $[\alpha]$ la classe d'equivalència d'$\alpha \in \Lambda'$ i per $\Lambda = \Lambda'/\sim$ el conjunt de classes d'equivalència, amb aplicació de pas al quocient $Q : \Lambda' \to \Lambda$ tal que $Q(\alpha) = [\alpha]$

Recordem el conjunt S_p de p+1 quaternions distingits definit al capítol 3. Per definició $S_p \subset \Lambda'$.

Proposició 5.3.1. *a)* Λ *és un grup.*

b) El graf de Cayley $\mathcal{G}(\Lambda, Q(S_p))$ *és l'arbre (p+1)-regular.*

Demostració: La demostració d'aquesta proposició es pot trobar a la següent referència [1, Proposition 4.3.1, pg. 115]. □

Com hem fet a la secció anterior, considerem la reducció mòdul q donada per

$$\tau_q : H(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q);$$

que envia Λ' al grup $\mathbb{H}(\mathbb{F}_q)^\times$, que són els elements invertibles de $\mathbb{H}(\mathbb{F}_q)$. Sigui Z_p el següent subgrup d'$\mathbb{H}(\mathbb{F}_q)^\times$:

$$Z_q = \{\alpha \in \mathbb{H}(\mathbb{F}_q)^\times : \alpha = \bar{\alpha}\}.$$

Siguin $\alpha, \beta \in \Lambda'$: si $\alpha \sim \beta$, aleshores $\tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q$. Això vol dir que $\tau_q : \Lambda' \to \mathbb{H}(\mathbb{F}_q)^\times$ cau a un grup de morfismes ben definit

$$\Pi_q : \Lambda \to \mathbb{H}(\mathbb{F}_q)^\times / Z_q.$$

Denotem el nucli de Π_q per $\Lambda(q)$ i identifiquem la imatge de Π_q amb el grup quocient $\Lambda/\Lambda(q)$. Definim $T_{p,q} = (\Pi_q \circ Q)(S_p)$.

Com hem fet a la secció anterior, si q és prou gran respecte de p, definim el graf $Y^{p,q}$ com el graf de Cayley de $\Lambda/\Lambda(q)$ respecte de $T_{p,q}$:

$$Y^{p,q} = \mathcal{G}(\Lambda/\Lambda(q), T_{p,q})$$

Com Λ està generat per $Q(S_p)$ (proposició 5.3.1), es dedueix de la proposició 5.1.3 que per $q > 2\sqrt{p}$ el graf $Y^{p,q}$ és (p+1)-regular i connex.

Observem que l'isomorfisme $\psi_q : \mathbb{H}(\mathbb{F}_q)^\times \to \mathrm{GL}_2(q)$ envia Z_q al subgrup de matrius escalars a $GL_2(q)$, que, per la seva banda, és el nucli de $\varphi : GL_2(q) \to PGL_2(q)$. Per tant, ψ_q passa a l'isomorfisme

$$\beta : \mathbb{H}(\mathbb{F}_q)^\times / Z_q \to PGL_2(q).$$

Això ens permet comparar, a partir d'un diagrama commutatiu, les construccions de $X^{p,q}$ i $Y^{p,q}$:

$$\begin{array}{ccccc}
S_p \subset \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & \xrightarrow{\psi_q} & \mathrm{GL}_2(q) \\
\downarrow Q & & \downarrow & & \downarrow \varphi \\
\Lambda & \xrightarrow[\Pi_q]{} & \mathbb{H}(\mathbb{F}_q)^\times / Z_q & \xrightarrow[\beta]{} & \mathrm{PGL}_2(q)
\end{array}$$

A diferència del $X^{p,q}$, sabem que $Y^{p,q}$ és connex per definició, per contra, no tenim identificat el grup $\Lambda/\Lambda(q)$ del qual prové. Sí que sabem, però, que, com $\beta(T_{p,q} = S_{p,q}$ aleshores $Y^{p,q}$ és una component connexa de $X^{p,q}$. Eventualment, podrem demostrar que, per $q > p^8$, $X^{p,q}$ és connex i, per tant, isomorf a $Y^{p,q}$. Abans, hem d'identificar el subgrup $\Lambda(q)$.

Lema 5.3.2. $\Lambda(q) = \{[\alpha] \in \Lambda : \alpha = a_0 + a_1 i + a_2 j + a_3 k,\ q | a_1, a_2, a_3\}$.

Demostració:

$$\begin{aligned}
[\alpha] \in \Lambda(q) &\iff \tau_q(\alpha) \in Z_q \\
&\iff q \text{no divideix} a_0 \text{i} q | a_1, a_2, a_3 \\
&\iff q | a_1, a_2, a_3,
\end{aligned}$$

On l'equivalència entre la segona i la tercera línia surt del fet que $N(\alpha)$ és una potència de p i $p \neq q$. $\square$.

La següent proposició ens dona una cota inferior de la circumferència de $Y^{p,q}$.

Proposició 5.3.3. $g(Y^{p,q}) \geq 2\log_p q$. *Si* $\left(\frac{p}{q}\right) = -1$ *aleshores tenim la següent desigualtat* $g(Y^{p,q}) \geq 4\log_p q - \log_p 4$

Demostració: Es pot veure la demostració detallada d'aquesta proposició a [1,Proposition 4.3.3, pg. 118]. □

Observació 5.3.4. Sabem que per $p \geq 5$ es compleix

$$g(Y^{p,q}) \leq 2 + 2\log_p |Y^{p,q}|;$$

Per tant, per la proposició 5.3.3

$$|Y^{p,q}| \geq \frac{q}{p}.$$

A més, si $\left(\frac{p}{q}\right) = -1$

$$|Y^{p,q}| \geq \frac{q^2}{2p}.$$

Per tant, veiem que $|Y^{p,q}| = |\Lambda/\Lambda(q)|$ creix com a mínim de forma lineal respecte a q.

Ara passem al resultat principal de la secció:

Teorema 5.3.5. [1, *Theorem* 4.3.5, *pg.* 119] *Suposem* $p \geq 5$. *Per* $q > p^8$, *el graf* $X^{p,q}$ *és connex.*

Demostració: Per la proposició 5.1.3c) per demostrar que $X^{p,q}$ és connex hem de demostrar que $S_{p,q}$ genera $PSL_2(q)$ si $(\frac{p}{q}) = 1$ i $PGL_2(q)$ si $(\frac{p}{q}) = -1$. Recordem l'isomorfisme $\beta : \mathbb{H}(\mathbb{F}_q)^\times/Z_q \to PGL_2(q)$. Com $\beta(T_{p,q} = S_{p,q}$ és equivalent a demostrar

$$\beta(\Lambda/\Lambda(q)) = \begin{cases} \mathrm{PSL}_2(q) & \text{si } \left(\frac{p}{q}\right) = 1; \\ \mathrm{PGL}_2(q) & \text{si } \left(\frac{p}{q}\right) = -1 \end{cases}$$

En el segon cas, ja hem vist anteriorment que $S_{p,q} \subset PGL_2(q) - PSL_2(q)$. Donat $H_{p,q} = PSL_2(q) \cap \beta(\Lambda/\Lambda(q))$. Només resta provar que en ambdós casos,

$$H_{p,q} = PSL_2(q).$$

Pel teorema 4.0.6 això es dedueix de dos fets: $|H_{p,q} > 60$ i $H_{p,q}$ no és metabelià.

Per provar que $|H_{p,q} > 60$ observem que, com $q > p^8$ i $p \geq 5$, gràcies a l'observació 5.3.4, veiem que $|\Lambda/\Lambda(q)| \geq \frac{q}{p} > 120$, i per tant $|H_{p,q} > 60$.

Per veure que $H_{p,q}$ no és metabelià hem de veure que existeixen $g_1, g_2, g_3, g_4 \in H_{p,q}$ tals que $[[g_!, g_2], [g_3, g_4]] \neq 1$.

Estudiem els dos casos possibles:

a) Si $\left(\frac{p}{q}\right) = 1$ aleshores podem escollir els g_i d'entre els elements de $S_{p,q}$ de la següent forma: escollim g_1 un element qualsevol de $S_{p,q}$ i escollim g_2 de forma que sigui diferent de $g_1^{\pm 1}$. Tot seguit escollim $g_3 = g_1$ i $g_4 \notin g_1^{\pm 1}, g_2^{\pm 1}$. D'aquesta forma, $[[g_!, g_2], [g_3, g_4]]$ és una paraula reduïda de mida 16 sobre $S_{p,q}$. Per la proposició 5.3.3 la circumferència de $Y^{p,q}$ satisfà

$$g(Y^{p,q}) \geq 2 \log_p q > 16$$

i, per tant, qualsevol paraula reduïda de mida 16 sobre $S_{p,q}$ ha de ser diferent de 1 a $H_{p,q}$, ja que això produiria un cicle de mida com a molt 16 a $Y^{p,q}$.

b) Si $\left(\frac{p}{q}\right) = -1$ escollim $h_1, h_2, h_3 \in S_{p,q}$ de la següent forma: Sigui h_1 qualsevol element de $S_{p,q}$, sigui h_2 diferent de $h_1^{\pm 1}$ i $h_3 \notin h_1^{\pm 1}, h_2^{\pm 1}$. Aleshores definim $g_1 = h_1 h_3$, $g_2 = h_2 h_3$, $g_3 = h_1 h_2$, *i* $g_4 = h_3 h_2$ i ja tenim els elements de $H_{p,q}$. Llavors $[g_1, g_2] = h_1 h_3 h_2 h_1^{-1} h_3^{-1} h_2^{-1}$ i $[g_3, g_4] = h_1 h_2 h_3 h_1^{-1} h_2^{-1} h_3^{-1}$. Aleshores, $[[g_1, g_2], [g_3, g_4]]$ és una paraula reduïda de mida 24 a $S_{p,q}$. Per la proposició 5.3.3 sabem que

$$g(Y^{p,q}) \geq 4 \log_p q - \log_p 4 > 24$$

I argumentem anàlogament al cas a). □

Per resumir el que realment implica pels grafs $X^{p,q}$ tenim el següent corol·lari.

Corołari 5.3.6. *Suposem $q > p^8$. Els grafs $X^{p,q}$ són (p+1)-regulars i connexos. A més:*

a) Si $\left(\frac{p}{q}\right) = 1$ aleshores $X^{p,q}$ no és bipartit i té

$$g(X^{p,q}) \geq \frac{2}{3} \log_p |X^{p,q}|$$

b) Si $\left(\frac{p}{q}\right) = -1$ aleshores $X^{p,q}$ és bipartit i té

$$g(X^{p,q}) \geq \frac{4}{3} \log_p |X^{p,q}| - \log_p 4$$

Demostració: Que és connex ja ha quedat demostrat amb el teorema anterior. Les aproximacions de la circumferència fan servir resultats que no tractarem al treball, però si és de l'interès del lector, pot trobar els detalls a [1,Corollary 4.3.6, pg. 120]. □

5.4 Demostració de què $X^{p,q}$ son *expanders*.

Un cop vist que els $X^{p,q}$ són connexos, o el que és equivalent, que $S_{p,q}$ genera $PSL_2(q)$ si $(\frac{p}{q}) = 1$ i $PGL_2(q)$ si $(\frac{p}{q}) = -1$, resta provar el darrer resultat: que fixat un primer senar p, la família $X^{p,q}$ és una família d'*expanders*.

Denotem per n el nombre de vèrtexs de $X^{p,q}$ i l'espectre de la seva matriu d'adjacència com $\mu_0 = p + 1 > \mu_1 \geq \mu_2 \geq \ldots \geq \mu_{n-1}$.

Definició 5.4.1. *Definim els* ***polinomis de Txebixev del segon tipus*** *expressant* $\frac{\sin(m+1)\theta}{\sin\theta}$ *com un polinomi de grau m en* $\cos\theta$*:*

$$U_m(\cos\theta = \frac{\sin(m+1)\theta}{\sin\theta}, \quad (m \in \mathbb{N})$$

Per exemple, $U_0(X) = 1$, $U_1(x) = 2x$, $U_2(x) = 4x^2 - 1, \ldots$.

A partir de relacions trigonomètriques es pot veure que els polinomis satisfan la següent relació de recurrència:

$$U_{m+1}(x) = 2xU_m(x) - U_{m-1}(x).$$

Denotem per f_m el nombre de camins de mida m sense marxa enrere que comencen i acaben a 1 a $X^{p,q}$. Per la proposició 5.1.3a), sabem que $X^{p,q}$ és vèrtex-transitiu, tenim la següent fórmula de la traça, que es desenvolupa a [1,Corollary 1.4.7, pg. 25], i per $X^{p,q}$, (p+1)-regular i vèrtex-transitiu, tenim

$$\sum_{0\leq r\leq \frac{m}{2}} f_{m-2r} = \frac{p^{\frac{m}{2}}}{n} \sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{p}}\right),$$

per cada $m \in \mathbb{N}$.

El primer que volem és transformar el costat esquerre de la fórmula, per aquest motiu, introduïm la forma quadràtica en 4 variables:

$$Q(x_0, x_1, x_2, x_3) = x_0^2 + q^2(x_1^2 + x_2^2 + x_3^2)$$

i per $m \geq 1$ definim

$$\begin{aligned} s_Q(p^m) = |\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 : Q(x_0, x_1, x_2, x_3) = pm, \text{tals que o bé} \\ x_0 \text{ senar i } x_1, x_2, x_3 \text{ parells, o } x_0 \text{ parell i } x_1, x_2, x_3 \text{ senars}\}| \end{aligned}$$

Observació 5.4.2. Suposem que o bé m és parell o $p \equiv 1(mod.\ 4)$. Al reduir mòdul 4 veiem que a la definició anterior totes les 4-tuples (x_0, x_1, x_2, x_3) tenen x_0 senar i x_1, x_2, x_3 parells. Definim la forma quadràtica:

$$Q'(x_0, x_1, x_2, x_3) = x_0^2 + 4q^2(x_1^2 + x_2^2 + x_3^2)$$

i aleshores $s_Q(p^m)$ és el nombre exacte de representacions enteres de p^m per la forma quadràtica Q'.

Ara agafem un p general.

Lema 5.4.3. *Per* $m \in \mathbb{N} : s_Q(p^m) = 2\sum_{0\leq r\leq \frac{m}{2}} f_{m-2r}$.

Demostració: Pel teorema 5.3.5 identifiquem $X^{p,q}$ amb $Y^{p,q}$. Siguin $x_0 = 1, x_!, \ldots, x_{l-1}, x_l = 1$ els vèrtexs d'un camí de longitud l sense marxa enrere que

comença i acaba a $1 \in Y^{p,q}$. Anàlogament a com es fa a la demostració de la proposició 5.3.3, que es pot veure a [1], podem trobar $t_1, \ldots, t_l \in T_{p,q}$, tals que $x_i = t_1 t_2 \ldots t_i \, (1 \leq i \leq l)$. Escrivim $t_i = \Pi_q[\alpha_i]$ per un únic $\alpha_i \in S_p (i = 1, \ldots, l)$. Aleshores $[\alpha_1][\alpha_2] \ldots [\alpha_l]$ és una paraula reduïda de mida l a Λ, ja que prové d'un camí sense marxa enrere. I com $\Pi_q([\alpha_1][\alpha_2] \ldots [\alpha_l]) = x_l = 1$, podem veure que $[\alpha_1][\alpha_2] \ldots [\alpha_l]$ pertany a $\Lambda(q)$. Això demostra que f_l és el nombre de paraules reduide de mida l a Λ, que pertanyen a $\Lambda(q)$.

Sigui $(x_0, x_1, x_2, x_3) \in \mathbb{Z}$ que contribueix a $s_Q(p^m)$ de manera que $Q(x_0, x_1, x_2, x_3) = p^m$ i que les congruències mòdul 2 estiguin satisfetes. Sigui α el quaternió $\alpha = x_0 + q(x_1 i + x_2 j + x_3 k)$. α pertany a Λ' i, pel lema 5.3.2, la seva classe d'equivalència pertany a $\Lambda(q)$. D'aqui obtenim la igualtat

$$s_Q(p^m) = |\{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda' : N(\alpha) = pm, \, q \mid a_1, a_2, a_3\}|$$

Suposem que α contribueix a la banda dreta de l'equació anterior. Pel corol·lari 3.0.14 α té una factorització única $\alpha = \pm p^l w_{m-2l}$, on w_{m-2l} és una paraula reduïda de mida $m - 2l$ sobre S_p. La classe d'equivalència $[\alpha]$ és, per tant, una paraula reduïda de mida $m - 2l$ a Λ, que, a més, pertany a $\Lambda(q)$. Recíprocament, a partir d'una paraula reduïda w de mida $m - 2l$ a $\Lambda(q)$, la fórmula $\alpha = \pm p^l w$ genera dos quaternions com els anteriors. Això demostra que

$$|\{\alpha \in \Lambda' : N(\alpha) = pm, [\alpha] \in \Lambda(q)\}| = 2 \sum_{o \leq r \leq \frac{m}{2}} f_{m-2r},$$

que finalitza la demostració. □

Aleshores, la fórmula de la traça per $X^{p,q}$ passa a ser, per tot $m \in \mathbb{N}$:

$$s_Q(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m \left(\frac{\mu_j}{2\sqrt{p}} \right).$$

En aquest punt, definim el següent subconjunt $\Theta_p \subset \mathbb{C}$:

$$\Theta_p = [i \log \sqrt{p}, 0] \cup [0, \pi] \cup [\pi, \pi + i \log \sqrt{p}.$$

Recordem que el sinus i el cosinus d'un nombre complex $z \in \mathbb{C}$ es defineixen com:

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \frac{z^6}{6!} + \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n}}{(2n)!} = \frac{e^{iz} + e^{-iz}}{2}$$

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!} = \frac{e^{iz} - e^{-iz}}{2i}$$

Es pot comprovar que el canvi de variable $z \to 2\sqrt{p} \cos z$ és una bijecció entre Θ_p i $[-(p+1), p+1]$i, en particular, envia $[0, \pi]$ a $[-2\sqrt{p}, 2\sqrt{p}]$. Per $j = 0, 1, \ldots, n-1$ sigui $\theta_j \in \Theta_p$ l'únic element de Θ_p tal que $\mu_j = 2\sqrt{p} \cos \theta_j$. En particular, $\theta_0 = i \log \sqrt{p}$ i, si $\left(\frac{p}{q}\right) = -1$:

$$\theta_{n-1} = \pi + i \log \sqrt{p} \quad \text{(pel corol·lari 5.3.6).}$$

Per definició del polinomi de Txebixev U_m, tenim que

$$s_Q(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} \frac{\sin(m+1)\theta_j}{\sin\theta_j}$$

Es pot demostrar que $X^{p,q}$ és de Ramanujan si provem que, llevat de $\theta_0 = i\log\sqrt{p}$ i possiblement $\theta_{n-1} = \pi + i\log\sqrt{p}$, la resta de θ_j's viuen a $\mathbb{R}$. Malauradament, aquesta demostració s'escapa de les eines de les quals disposem en aquest treball, però es pot llegir a [7]. Nosaltres, en canvi, provarem que per q prou gran, la part imaginària dels θ_j està acotada per una constant que només depèn de p, i amb això demostrarem que els $X^{p,q}$ formen una família d'*expanders*.

El següent resultat ens donarà informació sobre la multiplicitat dels valors propis de $X^{p,q}$, ja que a la fórmula de la traça els θ_j's surten repetits segons les respectives multiplicitats.

Proposició 5.4.4. *Sigui μ un valor propi no trivial de $X^{p,q}$ (és a dir, $|\mu| \neq p+1$). Denotem la seva multiplicitat per $M(\mu)$. Aleshores $M(\mu) \geq \frac{q-1}{2}$.*

Demostració: Sigui V_μ l'espai propi corresponent a μ. Es pot veure que l'espai vectorial V_μ és un espai de representació del grup subjacent a $X^{p,q}$. Com aquest grup sempre conté al $PSL_2(q)$, V_μ és un espai de representació de $PSL_2(q)$. Del teorema 4.0.13 es dedueix que qualsevol representació no trivial de $PSL_2(q)$ té grau com a mínim $\frac{q-1}{2}$. El que volem provar és que, si $|\mu| \neq p+1$, aleshores la representació de $PSL_2(q)$ a V_μ és no trivial. Ho demostrarem pel contra recíproc, assumint que la representació de $PSL_2(q)$ a V_μ és trivial. Hi ha dos casos:

a) Si $\left(\frac{p}{q}\right) = 1$ aleshores totes les funcions de V_μ són constants i, per tant, $\mu = p+1$.

b) Si $\left(\frac{p}{q}\right) = -1$, aleshores una funció $f \in V_\mu$ diferent de zero ha de ser constant a cadascuna de les dues classes laterals de $PSL_(q)$ a $PGL_2(q)$, és a dir:

$$f = \begin{cases} a_+ & \text{a}PSL_2(q) \\ a_- & \text{a}PGL_2(q) - PSL_2(q). \end{cases}$$

Observem que f és una funció pròpia de la matriu d'adjacència de $X^{p,q}$ i llavors ens trobem amb el següent sistema:

$$\begin{cases} \mu a_- = (p+1)a_+ \\ \mu a_+ = (p+1)a_- \end{cases}$$

Aplicant que f és diferent de zero, obtenim que $\mu^2 = (p+1)^2$, per tant, $|\mu| = p+1$, com volíem demostrar. □

Finalment, enunciarem i demostrarem el resultat més important del capítol.

Teorema 5.4.5. [1, *Theorem* 4.4.4, *pg.* 125] *Fixem* ϵ *complint* $0 < \epsilon < \frac{1}{6}$. *Per* q *prou gran, cada valor propi no trivial* μ *de* $X^{p,q}$ *satisfà*

$$|\mu| \leq p^{\frac{5}{6}+\epsilon} + p^{\frac{1}{6}-\epsilon}$$

En particular, els $X^{p,q}$*'s són una família d'expanders.*

Demostració: Prenem com a punt de partida l'expressió que hem deduït abans per la fòrmula de la traça de $X^{p,q}$:

$$s_Q(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} \frac{\sin(m+1)\theta_j}{\sin\theta_j},$$

per tot $m \in \mathbb{N}$. $\mu_j = 2\sqrt{p}\cos\theta_j$. Si μ_j no pertany a l'interval de Ramanujan $[-2\sqrt{p}, 2\sqrt{p}]$ escrivim:

$$\begin{cases} \theta_j = i\psi_j & \text{si} 2\sqrt{p} < \mu_j \leq p+1, \\ \theta_j = \pi + i\psi_j & \text{si} -(p+1) \leq \mu_j < -2\sqrt{p}, \end{cases}$$

on $0 < \psi_j \leq \log\sqrt{p}$ en els dos casos.

A partir d'aquest punt, suposarem que m és parell. Recordem que definim el sinus hiperbòlic i el cosinus hiperbòlic d'un nombre complez z com:

$$\sinh z = \frac{e^z - e^{-z}}{2} = i\sin(-iz)$$

$$\cosh z = \frac{e^z + e^{-z}}{2} = \cos(-iz)$$

Com m és parell, tenim, per $\mu_j \notin [-2\sqrt{p}, 2\sqrt{p}]$

$$\frac{\sin(m+1)\theta_j}{\sin\theta_j} = \frac{\sin i(m+1)\psi_j}{\sin i\psi_j} = \frac{\sinh(m+1)\psi_j}{\sinh\psi_j} \geq 0$$

Aleshores, per un valor propi no trivial fixat $\mu_k \notin [-2\sqrt{p}, 2\sqrt{p}]$,

$$s_Q(p^m) = \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh\psi_k} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j:\mu_j \neq \mu_k} \frac{\sin(m+1)\theta_j}{\sin\theta_j}$$

$$\geq \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh\psi_k} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j:|\mu_j| \leq 2\sqrt{p}} \frac{\sin(m+1)\theta_j}{\sin\theta_j}$$

Es pot comprovar que, per θ real, es compleix que $\left|\frac{\sin(m+1)\theta}{\sin\theta}\right| \leq m+1$, cosa que implica que

$$s_Q(p^m) \geq \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh\psi_k} - 2p^{\frac{m}{2}}(m+1).$$

Ara volem estimar el valor de $s_Q(p^m)$. De l'observació 5.4.2 i al ser m parell, tenim que $s_Q(p^m)$ és el nombre de solucions enteres de $x_0^2 + 4q^2(x_1^2 + x_2^2 + x_3^2) = p^m$.

Primer estudiarem les possibles eleccions de x_0. Tenim que $|x_0| \leq p^{\frac{m}{2}}$ i a més $x_0^2 \equiv p^m \pmod{q^2}$, per tant, $x_0^2 \equiv \pm p^{\frac{m}{2}} \pmod{q^2}$.

Com x_0 i p són els dos senars, realment tenim $x_0^2 \equiv \pm p^{\frac{m}{2}} \pmod{2q^2}$.

Això dona, com a màxim dues possibilitats per x_0 (calculades de $\frac{p^{\frac{m}{2}}}{q^2} + 1$. Un cop fixem x_0 haurem de trobar les solucions enteres de

$$x_1^2 + x_2^2 + x_3^2 = \frac{p^m - x_0^2}{4q^2}$$

Amb la notació del capítol 3, hi ha $r_3\left(\frac{p^m - x_0^2}{4q^2}\right)$ possibilitats. Del corolari 3.0.4 tenim:

$$r_3\left(\frac{p^m - x_0^2}{4q^2}\right) = \mathcal{O}_\epsilon\left(\left(\frac{p^m}{q^2}\right)^{\frac{1}{2}+\epsilon}\right)$$

per cada $\epsilon > 0$. Aleshores

$$\begin{aligned} s_Q(p^m) &= \mathcal{O}_\epsilon\left[\frac{p^{\frac{m}{2}+\epsilon m}}{q^{1+2\epsilon}}\left(\frac{p^{\frac{m}{2}}}{q^2} + 1\right)\right] \\ &= \mathcal{O}_\epsilon\left[\frac{p^{m(1+\epsilon)}}{q^{3+2\epsilon}} + \frac{p^{\frac{m}{2}(1+2\epsilon)}}{q^{1+2\epsilon}}\right] \\ &= \mathcal{O}_\epsilon\left[\frac{p^{m(1+\epsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\epsilon}}{q}\right]. \end{aligned}$$

Llavors, per alguna constant $C_\epsilon > 0$, la desigualtat és

$$\frac{M(\mu_k)}{n} \cdot p^{\frac{m}{2}} \cdot \frac{\sinh(m+1)\psi_k}{\sinh\psi_k} \leq C_\epsilon\left[\frac{p^{m(1+\epsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\epsilon)}}{q}\right] + p^{\frac{m}{2}}(m+1).$$

Cancel·lant $p^{\frac{m}{2}}$ i fent servir que $n \leq q^3$ (proposició 4.0.1) obtenim que:

$$M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} \leq C_\epsilon\left[p^{m(\frac{1}{2}+\epsilon)} + q^2 p^{m\epsilon}\right] + q^3(m+1).$$

Suposem que escollim m de forma que $p^{\frac{m}{2}} \leq q^3$. Aleshores

$$M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} \leq C_\epsilon[q^{3+6\epsilon} + q^{2+6\epsilon}] + q^3(1 + 6\log_p q).$$

Com $\sinh\psi_k \leq \sinh\log\sqrt{p}$ obtenim que

$$M(\mu_k)\sinh(m+1)\psi_k = \mathcal{O}_\epsilon[q^{3+6\epsilon}].$$

Ara agafem m com l'enter parell més gran tal que $p^{\frac{m}{2}} \leq q^3$. Per q prou gran tenim que

$$\sinh(m+1)\psi_k \geq \frac{e^{(m+1)\psi_k}}{3} \geq \frac{e^{(-1+6\log_p q)\psi_k}}{3} \geq \frac{p^{-\frac{1}{2}}}{3} e^{6\log_p q \cdot \psi_k},$$

.

A la darrera desigualtat anterior hem fet servir $\psi_k \leq \log\sqrt{p}$. Aleshores

$$M(\mu_k) = \mathcal{O}_\epsilon\left(q^{3+6\epsilon-\frac{6\psi_k}{\log p}}\right).$$

Però com μ_k és un valor propi no trivial, tenim que

$$M(\mu_k) \geq \frac{q-1}{2}$$

a conseqüència de la proposició 5.4.4. Llavors, per q prou gran, tenim

$$3 + 6\epsilon - \frac{6\psi_k}{\log p} \geq 1 \text{i també} \psi_k \leq \left(\frac{1}{3} + \epsilon\right)\log p.$$

Aleshores, com o bé $\theta_k = i\psi_k$ o bé $\theta_k = \pi + i\psi_k$ i $\mu_k = 2\sqrt{p}\cos\theta_k$ llavors obtenim

$$|\mu_k| = 2\sqrt{p}|\cos(i\psi_k)| = 2\sqrt{p}\cosh\psi_k \leq p^{\frac{5}{6}+\epsilon} + p^{\frac{1}{6}-\epsilon},$$

per q prou gran, i obtenim el resultat desitjat. □

Per tant, hem aconseguit el que volíem: una construcció explícita d'una família d'*expander graphs* i la prova de què, efectivament, es tracta d'una família d'*expanders*. Al següent apartat agafarem un cas particular d'aquesta família que hem construït per mostrar una de les moltes aplicacions dels *expander graphs* al món de la informàtica.

Capítol 6

L'aplicació a GNN

Finalment, aquesta secció anirà dedicada a l'exemple d'aplicació a la informàtica que he volgut tractar pels *expander graphs*. Aquests tenen utilitat en diversos camps, com els codis de correcció d'errors, el disseny d'algorismes o, com el nostre cas, la propagació d'informació a través de xarxes neuronals. Si el lector està interessat en més aplicacions, algunes d'elles surten explicades a [2].

En particular, el nostre exemple és un algorisme per propagar informació a través de xarxes neuronals de graf (d'aquí en endavant farem servir GNN, de l'anglès *Graph Neural Network*, per abreviar). Cal destacar que l'objectiu principal del treball no era dissenyar un algorisme sinò estudiar una construcció d'*expander graphs* i mostrar com es pot aplicar. Per tant, he fet servir un algorisme descrit a l'article *Expander Graph Propagation* [3], al qual també he trobat les referències per implementar la GNN i els *datasets* corresponents, i jo m'he dedicat a implementar la construcció dels *expanders* i els he integrat.

6.1 L'algorisme

En primer lloc, explicaré l'algorisme que he volgut implementar, el qual està descrit i detallat a [3]. Aquest algorisme es basa en un cas particular dels grafs que hem descrit en aquest treball, i són grafs de Cayley que fan servir $SL(2, \mathbb{Z}_\ltimes)$ com a grup i com a conjunt de generadors el següent:

$$S_n = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

On els membres de la família varien per diferents valors de n. Per determinar el nombre de vèrtexs del graf n-èssim es fa servir la següent fòrmula:

$$|V(Cay(SL(2, \mathbb{Z}_\ltimes); S_n))| = n^3 \prod_{p|n \,:\, p\, primer} \left(1 - \frac{1}{p^2}\right).$$

En particular, el nombre de nodes del graf n-èssim és de l'ordre de n^3.
Un cop establerts aquests detalls, l'algorisme proposat a [3] és el següent:

Algorithm 1: Expander graph propagation (EGP) forward pass

Inputs : Node features $\mathbf{X} \in \mathbb{R}^{|V| \times d}$, Adjacency matrix $\mathbf{A} \in \mathbb{R}^{|V| \times |V|}$
Output : Node embeddings $\mathbf{H}$

// Choose the smallest Cayley graph from our family that has number of nodes equal to, or greater than, $|V|$
$n \leftarrow \text{argmin}_{m \in \mathbb{N}} |V(\text{Cay}(\text{SL}(2, \mathbb{Z}_m); S_m))| \geqslant |V|$; // We can use Equation 10 to determine n

$G^{\text{Cay}(n)} \leftarrow \text{Cay}(\text{SL}(2, \mathbb{Z}_n); S_n)$

$\mathbf{A}^{\text{Cay}(n)}_{uv} \leftarrow \begin{cases} 1 & (u, v) \in E(G^{\text{Cay}(n)}) \\ 0 & \text{otherwise} \end{cases}$; // Populate adjacency matrix of the Cayley graph

$\mathbf{H}^{(0)} \leftarrow \mathbf{X}$; // Initialise GNN inputs

for $t \in \{1, \ldots, T\}$ **do**
  if $t \mod 2 = 0$ **then**
    $\mathbf{H}^{(t)} \leftarrow \text{GNN}^{(t)}(\mathbf{H}^{(t-1)}, \mathbf{A})$; // GNN layer over input graph; e.g. Equation 15
  end
  else
    $\mathbf{H}^{(t)} \leftarrow \text{GNN}^{\text{Cay}(t)}\left(\mathbf{H}^{(t-1)}, \mathbf{A}^{\text{Cay}(n)}_{1:|V|,1:|V|}\right)$; // GNN layer over Cayley graph; e.g. Eq. 15
  end
end

return $\mathbf{H}^{(T)}$; // Return final embeddings for downstream use

El comentarem amb més detall:

Els inputs serien els detalls dels vèrtexs del graf de la GNN base i la seva matriu d'adjacència. Volem retornar els *node embeddings* per realitzar l'aprenentatge sobre la xarxa neuronal.

En primer lloc, fem servir la fórmula descrita abans per calcular el valor de n a partir del qual construirem l'*expander*. Volem el valor mínim per tal d'agafar el graf de Cayley més petit que té nombre de vèrtexs major o igual que el nombre de vèrtexs del graf de la GNN base.

Notem que en la majoria dels casos no tindrem els mateixos vèrtexs a un graf i l'altre, cosa que resulta problemàtica perquè per aplicar l'algorisme que volem cal que siguin els mateixos. En aquest cas, la solució proposada a l'article [3] és fer un truncament dels vèrtexs sobrants (més en particular, de les línies de la matriu d'adjacència sobrants) per tal que s'ajustin. Al mateix article es destaca que no és la solució òptima, però ha donat resultats prou bons mentre no es trobi una millor.

Seguidament, amb la n calculada realitzem la construcció de l'*expander* i també la seva matriu d'adjacència, que com sabem pel capítol 2, al ser el graf simple serà una matriu de zeros i uns.

Un cop tenim la nova matriu d'adjacència, es fa un *ping-pong* en el que en les iteracions parelles es fa servir la matriu d'adjacència el graf de la GNN base per fer els *embeddings* i en les iteracions senars es fa servir la de l'*expander*.

La idea darrere d'aquest algorisme és que fem servir la GNN perquè està muntada tenint en compte les dades, i fem servir l'*expander* perquè, tot i no tenir a priori res a veure amb les dades, gràcies a les propietats de connexió ens permet arribar a més

profunditat. Per tant, el que s'espera aconseguir és un millor rendiment del procés d'aprenentatge i que això porti a un millor resultat en el procés de l'avaluació.

6.2 La meva implementació

En aquesta secció descriuré els detalls de la meva implementació. El codi sencer és massa pesat perquè inclou com a base la implementació de la GNN i els *datasets* fets servits a l'article [3]. Si és d'interès del lector, la GNN està basada en la descrita a [15] i tant els *datasets* com el repositori base són de [16]. El meu repositori es pot trobar a `https://github.com/GuillermoMariscal/ExpanderGraphs-TFG`.

De tot el codi, m'he centrat a fer les proves sobre el *dataset* **mol**, que és el més petit i requeria menys temps d'execució de l'algorisme. El meu codi es troba a la carpeta **examples/graphproppred/mol** i els meus fitxers són els anomenats **Cayley, OnlyExpander i ExpanderGraphPropagation**.

El codi base fa servir les llibreries de **PyTorch** per gestionar la GNN, mentre que per la meva implementació he fet servir les llibreries **NumPy, primePy i networkx**.

La primera funció que he implementat és **compute n**, que, donat el nombre de vèrtexs dessitjat, calcula el valor de n necessari. El codi és el següent:

```
def compute_n(n_vertices):
    argmin = -1
    count = 2
    while(argmin < n_vertices):
        prod = 1
        primes_list = primes.between(2,count+1)
        primes_list.append(2)
        for p in primes_list:
            if count % p == 0:
                prod = prod * (1 - 1/(p**2))
        argmin = count**3 * prod
        count += 1
    return count
```

Realment és bastant clar, itera sobre els valors de n des de 2 fins que trobi un tal que la fórmula descrita abans retorni un valor major o igual que el nombre de vèrtexs. Com a apunt a destacar, a la llista de primers hem d'afegir el 2, ja que la llibreria **primePy** té un error i no el considera a l'hora de construir la llista de primers.

Un cop tenim el valor de n, el passem a la funció **cayley graph**, de la qual no posaré imatge per ser massa extensa, però comentaré que es basa en el fet que els *expanders* són connexos, i construeix el graf començant per la identitat i operant els elements de S_n, afegint els nous nodes que s'obtenen a una llista de nodes pendents

de visitar i finalitzant quan no en queda cap pendent. En visitar un node el que fem és operar el seu element corresponent amb els elements de S_n per obtenir nous nodes, sempre tenint en compte que si s'arriba a un node ja visitat, no l'hem de tornar a visitar (per això també portem el recompte de nodes visitats). La matriu d'adjacència del graf l'obtindrem amb la funció específica de la llibreria **networkx** que la genera.

Finalment, tenim una classe CayleyConv que replica la classe GINConv del fitxer **conv**, però afegint la matriu d'adjacència que volem al paràmetre on s'aplica aquesta:

```
G = cayley_graph(self.n_value)
adj_matrix = get_ad_matrix(G)
adj_tensor = torch.tensor(adj_matrix.toarray(), dtype=torch.int)
self.edge_index = adj_tensor.nonzero(as_tuple=False).t()
```

Finalment, els fitxers **OnlyExpander i ExpanderGraphPropagation** són còpies del fitxer **main pyg**, però que canvien la part on s'aplica el model per fer l'aprenentatge, sent únicament amb el **CayleyConv** al primer (per fer proves només amb l'**expander**) i el *ping-pong* descrit a l'algorisme en el cas del segon:

```
for epoch in range(1, args.epochs + 1):
    if epoch % 2 == 0:
        model = model2
    else:
        model = model1
```

Ambdós fitxers tenen funció main per poder-se executar independentment

Per acabar, he fet unes petites proves sobre el *dataset* mol amb els tres fitxers i aquests són els resultats obtinguts:

GIN	Expander	GIN + EGP
0.7564 ± 0.0121	0.8234 ± 0.0424	0,7734 ± 0.0648

Taula 6.1: Proves de la implementació amb el dataset mol.

Només amb la GIN ja hem obtingut un resultat molt semblant al que obtenen a l'article. Pel que fa a l'execució només amb l'*expander*, el resultat és sospitosament alt, faria falta estudiar més a fons el motiu d'aquesta desviació. Pel que fa al resultat obtingut amb la *expander graph propagation*, veiem que obtenim un resultat lleugerament millor que només amb la GIN, però no ho milloren tant com el que s'obté a l'article. No he aconseguit trobar disponible la implementació realitzada pels autors, ja que m'hagués agradat tenir-la per comparar-la amb la meva, però no ha estat possible. Queda com a repte pel futur veure com millorar la meva implementació per fer-la òptima i eficaç.

Capítol 7

Conclusions

Aquest treball ha començat amb un objectiu clar: estudiar una de les construccions explícites que hi ha de famílies d'*expander graphs* i mostrar una de les múltiples formes que té d'aplicar-se al món de la informàtica. Al llarg del camí hem parlat d'Àlgebra Lineal, Teoria de Nombres, Teoria de Grups i, com no podria ser d'altra forma, Teoria de Grafs, tot branques de les matemàtiques que havia estudiat de forma independent al llarg del grau i que ara he tingut l'oportunitat de veure actuar conjuntament.

La introducció actua com a preliminar per posar al lector en context del treball, dona definicions que en molts casos ja seran conegudes, però no per aquest motiu s'han d'ignorar, a més, es dona la definició del concepte troncal del treball: el de família d'*expander graphs*.

Al capítol 2 hem vist com obtenir informació d'un graf donat a partir de la seva matriu d'adjacència i eines d'Àlgebra Lineal, i, el que és més important, enuncia i demostra la relació entre la constant isoperimètrica d'un graf i els valors propis de la seva matriu d'adjacència, cosa que resulta molt útil per comprovar si una família de grafs són *expanders* sense les complicacions que podria portar haver de fer servir la definició.

Els capítols 3 i 4 han estat dedicats a donar les eines de Teoria de Nombres i Teoria de Grups necessàries per poder definir posteriorment la família de grafs que volem. Hem fet servir resultats de Legendre, Jacobi i la llei de reciprocitat quadràtica per acabar definint un conjunt de quaternions distingits de norma p i també un isomorfisme per associar els quaternions amb l'àlgebra de matrius 2x2. Al capítol 4 hem definit i vist resultats sobre els grups PGL_2q i $PSL_2(q)$, que són la base dels grafs que volem definir.

Finalment, al capítol 5 hem definit els grafs $X^{p,q}$ i demostrat els dos resultats més importants del treball: que són connexos i que són *expanders*. Amb això hem après una construcció relativament senzilla de definir, però no tant de demostrar, d'una família d'*expander graphs*.

Pel que fa a l'aplicació informàtica, hem replicat, de manera molt rudimentària, l'algorisme plantejat a [3], veient una petita aplicació dels *expanders* al món de les GNN.

Com a conclusió personal em trobo, més enllà dels conceptes apresos, la satisfacció de veure com els dos graus que he estudiat de forma simultània, però sense veure gairebé lligats, van realment molt agafats de la mà, i els conceptes matemàtics que a priori es veuen abstractes realment es poden aplicar a un àmbit molt concret, com és el desenvolupament d'algorismes informàtics.

Finalment, considero que la meva implementació és molt rudimentària i segurament hi ha moltes possibles millores, sobretot en el sentit d'optimització. També seria un bon següent punt d'estudi mirar com actua aquest algorisme sobre altres *datasets* o aplicant-lo sobre altres xarxes neuronals com a base. M'hauria agradat també trobar la implementació de l'algorisme proposat a [3], per poder comparar-la amb la meva.

Bibliografia

[1] Davidoff, G.; Sarnak, P.; Valette, A.: *Elementary Number Theory, Group Theory, and Ramanujan Graphs.* New York : Cambridge University Press, cop, 2003.

[2] Hoory, S.; Linial, N.; Wigderson, A.: *Expander Graphs and their Applications.*BULLETIN (New Series) OF THE AMERICAN MATHEMATICAL SOCIETY Volume 43, Number 4, Pages 439–561, October 2006.

[3] Deac, A.; Lackenby, M.; Velickovic, P.: *Expander Graph Propagation.* https://arxiv.org/abs/2210.02997, 2022.

[4] Pinsker, M. S.: *On the Complexity of a Concentrator.* Academy of Sciences, Moscow, 1973.

[5] Alon, N.; Milman, V.: *λ1, isoperimetric inequalities for graphs, and superconcentrators.* Journal of Combinatorial Theory, Series B, Volume 38, 73-88, 1985.

[6] Dodziuk, J.: *Difference equations, isoperimetric inequality and transcience of certain random walks.* Transactions of the American Mathematical Society, Volume 284, Number 2, 787-794, 1984.

[7] Lubotzky, A.; Phillips, R.; Sarnak, P.: *Ramanujan Graps, Combinatorica 8*, 261-277, 1988.

[8] Li, W.C.W; Solé, P.: *Spectra of regular graphs and hypergraphs and orthogonal polynomials, Eur. J. Comb.*, 17(5), 461-477, 1996.

[9] Aigner, M.; Ziegler, M.: *Proofs from The Book*, Sprienger-Verlag, Berlin/New York, 1998.

[10] Hardy, G. H.; Wright, E. M.: *An introduction to the theory of numbers*, 5th ed., Clarendon Press, Oxford, 1979.

[11] Dirichlet, P.G.L: *Sur l'equationt*$^2 + u^2 + v^2 + w^2 = 4m$, *J. Math. pures et appliquées*, 1, 210-214, 1856.

[12] Dickson, L.E.: *Arithmetic of quaternions, Proc London Math. Soc.*, 20, 225-232, 1922.

[13] Nilli, A.:*On the second eigenvalue of a graph, Discrete Math*, 91, 207-210, 1991.

[14] Margulis, G.A.: *Explicit construction of concentrators, Problems Inform. Transmission*, 9, 325-332, 1973.

[15] Keyulu, X.; Weihua, H.; Leskovec, J.; Jegelka, S.: *How powerful are graph neural networks?*, arXiv preprint arXiv:1810.00826, 2018.

[16] Weihua H.; Fey, M.; Zitnik, M.; Dong, Y.; Ren, H.; Liu, B.; Catasta, M.;Leskovec, J.: *Open graph benchmark: Datasets for machine learning on graphs. Advances in neural information processing systems*, 33:22118-22133, 2020

[17] Huppert, B.: *Endliche Gruppen I, Grundlehren der Math. Wiss.*, 134, Springer-Verlag, Berlin/New York, 1979.

[18] Frobenius, G.: *Über Gruppencharaktere*, Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, 985-1021, 1896.

[19] Weihua, H.; Fey, M.; Zitnik, M.; Dong, Y.; Ren, H.; Liu, B.; Catasta, M.; Leskovec, J.: *OGB-LSC: A Large-Scale Challenge for Machine Learning on Graphs*, arXiv preprint arXiv:2103.09430, 2021.

[20] Kowalski, E.: *An introduction to expander graphs*, Cours Spécialisés, vol. 26, Société Mathématique de France, Paris, 2019.