Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas
Posgrado en Ciencias Matemáticas

Un estudio algebraico de las familias de grafos expanders y de los códigos expanders

Tesis

Que para obtener el grado de

Maestra en Ciencias Matemáticas

Presenta:

Aleyda Toledano Villegas

Director de tesis

Dr. Carlos Alberto López Andrade

PUEBLA, PUE Diciembre 2023

DR. SEVERINO MUÑOZ AGUIRRE
SECRETARIO DE INVESTIGACIÓN Y
ESTUDIOS DE POSGRADO, FCFM-BUAP
P R E S E N T E:

Por este medio le informo que la C:

ALEYDA TOLEDANO VILLEGAS

estudiante de la Maestría en Ciencias (Matemáticas), ha cumplido con las indicaciones que el Jurado le señaló en el Coloquio que se realizó el día 24 de noviembre de 2023, con la tesis titulada:

Un estudio algebraico de las familias de grafos expanders y de los códigos expanders

Por lo que se le autoriza a proceder con los trámites y realizar el examen de grado en la fecha que se le asigne.

A T E N T A M E N T E.
H. Puebla de Z. a 27 de noviembre de 2023

DR. RAÚL ESCOBEDO CONDE
COORDINADOR DEL POSGRADO
EN MATEMÁTICAS.

D*REC/mtrv

Facultad
de Ciencias
Físico Matemáticas

Av. San Claudio y 18 sur, edif. FM1
Ciudad Universitaria, Col. San
Manuel, Puebla, Pue. C.P. 72570
(222) 229 55 00 Ext. 7550 y 7552

Con cariño para mi familia,
gracias por su apoyo incondicional.

Agradecimientos

En primer lugar quiero agradecer a mis padres, Guadalupe y Aarón Rodolfo, por apoyarme en todos mis estudios, quiero que sepan que valoró todo el trabajo y esfuerzo que hicieron por mi y que la persona que soy ahora es gracias a ustedes.

A mis hermanos Arantxa y Aarón, por siempre cuidarme, quererme y escucharme. Gracias por motivarme a seguir adelante, por hacerme ver mis logros y celebrar cada uno de ellos, pero sobre todo por nunca dejarme sola, siempre han estado para mí y yo siempre estaré para ustedes.

A mi novio Luis Fernando, por su paciencia, confianza y amor. Gracias por llegar a mi vida a quererme de la forma más bonita. Coincidir contigo, es lo mejor que me ha pasado. Te quiero mucho.

A mis mascotas Cookie, Taemin y Cachetes por acompañarme en mis sesiones de estudio, en particular Taemin por tomar teoría de grafos conmigo, en el fondo sé que eres un gato matemático.

A mi asesor de tesis el Dr. Carlos Alberto López Andrade por creer en mí y aceptarme como su tesista. Gracias por dedicar su tiempo y esfuerzo en la elaboración de este trabajo y por su enorme paciencia ante mis problemas de lenguaje y espacialidad, pero sobretodo gracias por impulsarme a seguir mis sueños.

A mis sinodales el Dr. Iván Fernando Vilchis Montalvo, el Dr. Carlos Guillén Galván, el Dr. Henry Ricardo Chimal Dzul y la Dra. Sonia Navarro Flores, por tomarse el tiempo de revisar esta tesis, gracias.

Al Consejo Nacional de Humanidades, Ciencia y Tecnología (CONAHCYT) por el apoyo económico que recibí a través del Programa Nacional de Posgrados de Calidad (PNPC) para poder realizar mis estudios de maestría.

A mis amigos de licenciatura, compañeros de maestría y a mis alumnos del verano 2022, por todos los buenos momentos que compartimos, sin duda dejaron una huella en mí.

Y por último quiero agradecer a la vida por permitirme estar sana y siempre rodearme de personas maravillosas, aún tengo mucho que aprender, pero por el momento solo me queda decir: muchas gracias.

Introducción

Las familias de grafos expanders son familias de grafos que cumplen con ser altamente conectados pero contener pocas aristas. Esta característica tan particular los convierte en herramientas útiles para la teoría de la información, de hecho gracias a su buena aplicación en la construcción de redes de comunicación es que en la década de los 70′s las familias de grafos expanders fueron definidas por L. A. Bassalygo y M. S. Pinsker [11]. Si bien Pinsker probó su existencia de manera probabilística, fue hasta 1973 que Margulis [53] dio la primera construcción explicita de familias de grafos expanders. Esta construcción motivó el estudio de estas familias, obteniendo nuevas construcciones basadas en el estudio de constantes relacionadas a la conectividad del grafo, como lo es el segundo valor propio más grande asociado al grafo, y en nuevas aplicaciones en la teoría de la información, como la construcción de familias de códigos detectores-correctores de errores asintóticamente buenos.

Si bien las familias de grafos expanders son ampliamente estudiadas desde el punto de vista probabilístico y combinatorio, esta tesis tiene como objetivo principal estudiar a las familias de grafos expanders desde un punto de vista algebraico con el fin de obtener ejemplos explícitos de estas familias para la construcción de códigos detectores-correctores de errores. Este estudio se enfocará principalmente en los valores propios asociados al grafo y en las representaciones de grupos, donde los elementos de tales grupos fungirán como los vértices de grafos de Cayley. Por lo que será necesario revisar un poco de la teoría de grafos, análisis matemático, representaciones de grupos y para la construcción de códigos expanders algunos conceptos de la teoría de códigos. Esta tesis esta dividida en cuatro capítulos, los cuales describimos a continuación.

El capítulo 1 contiene el material preliminar para el resto de la tesis, este material incluye un resumen de los conceptos básicos de la teoría de grafos, grafos de Cayley, cubiertas de un grafo, teoría de representaciones de grupos y el espacio de Hilbert L^2.

En el capitulo 2 se define lo que es una familia de grafos expanders mediante cinco constantes, la constante isoperimétrica, la constante de expansión de vértices, la brecha espectral, la constante de expansión espectral y la constante de Kazhdan. Tomaremos como base la definición mediante la constante isoperimé-

trica y a partir de ella se probarán las demás. Un punto muy importante que debemos dejar claro a partir de este capítulo es el abuso del lenguaje, al referirnos a un grafo como expander, lo correcto es decir un grafo con cierta cantidad α de constante de expansión, esta constante puede ser cualquiera de las cinco ya mencionadas y con base en a la que se tome, se puede señalar que un grafo tiene mejor expansión si su constante es más grande o en algunos casos si es más pequeña. Si bien este abuso viene desde la literatura, nosotros trataremos de evitarlo, aunque en algunos casos será imposible. Por ello recomendamos al lector estar atento a los siguientes términos, cuando ponemos la palabra *expanders* nos referimos al plural, es decir, una familia de grafos expanders y cuando ponemos *expander* nos referimos al singular, es decir, un grafo con una cierta constante de expansión.

En el capítulo 3 mostramos un resumen de las primeras construcciones de las familias de grafos expanders, entre ellas esta la de Margulis en la que se ocupa la propiedad (T). Si bien esta propiedad es un concepto más de la topología algebraica, nosotros damos una introducción de esta propiedad mediante la constante de Kazhdan y posteriormente desarrollamos la construcción que da Lubotzky [47] con base a esta propiedad. También estudiamos la relación que existe entre las familias de Ramanujan y las familias de grafos expanders, de donde obtenemos un ejemplo explicito de familias de grafos expanders. Al revisar estas construcciones nos topamos con resultados que nos indican cuando una familia de grafos de Cayley no forman una familia de grafos expanders, los cuales sirven para darnos una noción de por donde no buscar familias de grafos expanders. Los resultados ya mencionados son el principio de no expansión de cocientes, en donde nosotros tenemos la aportación de dar su prueba mediante el segundo valor propio más grande asociado al grafo, y que los grupos abelianos finitos no forman una familia de grafos expanders.

Finalmente en el capítulo 4 hacemos la conexión entre las familias de grafos expanders y los códigos detectores-correctores de errores mediante los códigos expanders, los cuales pertenecen a la clase de los códigos LDPC, por lo que primero daremos una ligera introducción a la teoría de códigos, para ser más específicos, a los códigos lineales binarios. Posteriormente definimos los códigos expanders y como aportación mostramos ejemplos explícitos de códigos expanders mediante el uso de grafos con buena constante de expansión, por medio de estos ejemplos se refleja la importancia de la expansión para estos códigos. Por último cerramos el capítulo mostrando un ejemplo de una familia de códigos expanders.

Índice general

Capítulo 1
Preliminares

En este capítulo introducimos los conceptos de espacio de Banach L^2, de teoría de grafos y de representaciones de grupos que serán de utilidad para los siguientes capítulos.

1.1. Espacio L^2

En esta sección daremos algunos conceptos relacionados al espacio vectorial $L^2(X)$ con X un conjunto finito.

Definición 1.1.1 Sea X un conjunto finito, definimos el $\mathbb{C}-$espacio vectorial $L^2(X)$ como sigue

$$L^2(X) = \{f : X \to \mathbb{C}\}$$

donde para cada $f, g \in L^2(X)$ y $\alpha \in \mathbb{C}$,

$$(f+g)(x) := f(x) + g(x) \qquad (\alpha f)(x) := \alpha f(x)$$

cuyo producto interno y norma están dadas por

$$\langle f, g\rangle_2 = \sum_{x\in X} f(x)\overline{g(x)} \qquad \text{y} \qquad \|f\|_2 = \sqrt{\langle f, f\rangle_2} = \sqrt{\sum_{x\in X} |f(x)|^2}.$$

Definición 1.1.2 Sea $a \in X$, definimos la función $\delta_a \colon X \to \mathbb{C}$ como sigue

$$\delta_a(x) = \begin{cases} 1 & \text{si } \ x = a \\ 0 & \text{si } \ x \neq a. \end{cases}$$

El conjunto $\mathcal{B} = \{\delta_a : a \in X\}$ es un conjunto ortonormal de elementos de $L^2(X)$. Además para cada $f \in L^2(X)$ tenemos que $f = \sum_{a\in X} f(a)\delta_a$. Así que $\mathcal{B}$ es una base ortonormal de $L^2(X)$.

Sea $c \in \mathbb{C}$, denotaremos por f_c a la función de $L^2(X)$ tal que $f_c(x) = c$ para todo $x \in X$.

Definición 1.1.3 Sea $f_1 \in L^2(X)$, definimos los siguientes $\mathbb{C}$- espacios vectoriales

$$\begin{aligned} L^2_1(X) &= \{f \in L^2(X) | \langle f, f_1 \rangle_2 = 0\} \\ &= \{f \in L^2(X) | \sum_{x \in X} f(x) = 0\}, \end{aligned}$$

$$L^2(X, \mathbb{R}) = \{f \colon X \to \mathbb{R}\}$$

y

$$\begin{aligned} L^2_1(X, \mathbb{R}) &= \{f \in L^2(X, \mathbb{R}) | \langle f, f_1 \rangle_2 = 0\} \\ &= \{f \in L^2(X, \mathbb{R}) | \sum_{x \in X} f(x) = 0\} \end{aligned}$$

1.2. Teoría de grafos

Los textos revisados para el desarrollo de esta sección fueron [24], [14], [63] y [38].

Definición 1.2.1 Sea V un conjunto, se entiende por un *grafo* a cualquier pareja ordenada $X = (V, E)$ donde $E \subseteq [V]^2 = \{A \subseteq V \mid |A| = 2\}$. El conjunto V es el conjunto de *vértices o nodos* de X y el conjunto E es el conjunto de *aristas* de X.

La manera de representar un grafo es dibujar un punto para cada vértice y unir dos de estos puntos con una línea si los dos vértices correspondientes forman una arista, la forma en la que se dibujan estos puntos y líneas es irrelevante, lo importante es mostrar cuales vértices forman una arista y cuales no.

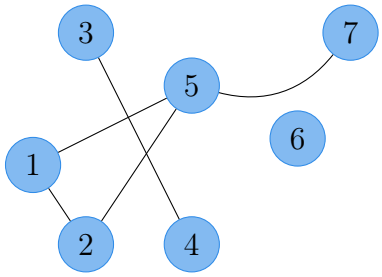


Figura 1.1: Grafo con conjunto de vértices $V = \{1, \ldots, 7\}$ y conjunto de aristas $E = \{\{1, 2\}, \{1, 5\}, \{2, 5\}, \{3, 4\}, \{5, 7\}\}$.

Observación 1.2.2 A un grafo $X = (V, E)$ se le conoce como *grafo dirigido* o *digrafo* cuando nos interesa la dirección de sus aristas. En un grafo dirigido las aristas son parejas ordenadas de vértices, es decir, $e = (a, b)$, con $a, b \in V$, es la arista con vértice inicial a y con vértice final b.

Definición 1.2.3 Sea X un grafo, decimos que X es un *grafo finito* si el número de vértices de X es finito. El número de vértices de X se le conoce como el *orden* de X, el cual se denota por $|X|$ y al número de aristas de X se le denota por $\|X\|$.

Definición 1.2.4 Sea $X = (V, E)$ un grafo.

- Se dice que $v \in V$ es *incidente* con $e \in E$, si $v \in e$.
- Si $\{v, w\} \in E$ se dice que v y w son vértices *adyacentes* o *vecinos*.
- Si $v \in V$ se definen los siguientes conjuntos.

  El conjunto de vecinos de v

  $$N_X(v) = \{w \in V : \{v, w\} \in E\}.$$

  El conjunto de aristas incidentes en v

  $$E_X(v) = \{e \in E : v \in e\}.$$

- Si $v \in V$ es adyacente a sí mismo, decimos que $e = \{v, v\}$ es un *bucle* o *lazo.*
- Si $v \in V$, el *grado o valencia* de v es el número de aristas incidentes en v, es decir, $|E_X(v)|$ y se denota por $d_X(v)$.

Observación 1.2.5

- Para cada $v \in V$, $|N_X(v)| = |E_X(v)|$.
- Cada bucle cuenta como dos aristas.
- Si $v \in V$ es aislado, entonces $d_X(v) = 0$.
- Si todos los vértices de X tienen el mismo grado d, entonces decimos que X es un *grafo d-regular*.

Observación 1.2.6 En la Definición 1.2.1 consideramos a E como un conjunto, sin embargo hay grafos donde dos vértices son adyacentes más de una vez, así que su arista aparece más de una vez en E, es decir, E es un multiconjunto. A este tipo de aristas se les denomina *aristas múltiples*.

Observación 1.2.7 En el caso de un grafo dirigido $X = (V, E)$, tenemos que cada vértice v tiene un grado de salida, es decir, el número de aristas que salen de v, y un grado de entrada, es decir, el número de aristas que entran a v. Si para cada $v \in V$, se cumple que v tiene como grado de salida y grado de entrada d aristas entonces decimos que X es un grafo dirigido $d-$regular.

Definición 1.2.8 Decimos que X es un *grafo simple* si no tiene bucles o aristas múltiples.

En el desarrollo de este trabajo, se estarán empleando grafos finitos simples no dirigidos a menos que se especifique lo contrario.

Definición 1.2.9 Sean $X = (V, E)$ y $Y = (V', E')$ grafos y sea ψ una función de V a V', decimos que ψ es un *homomorfismo de grafos* si para cada $\{v, w\} \in E$ se cumple que $\{\psi(v), \psi(w)\} \in E'$, es decir, ψ preserva la adyacencia de vértices.

Observación 1.2.10 En algunos textos, el homomorfismo de grafos se maneja como un par de funciones $\psi_V \colon V \to V'$ y $\psi_E \colon E \to E'$ donde cada vez que $e \in E$ tiene como vértices incidentes a $v, w \in V$ y $\psi_E(e)$ tiene como vértices de incidencia a $v', w' \in V'$, entonces $\psi_V(\{v, w\}) = \{v', w'\}$.

Definición 1.2.11 Sean $X = (V, E)$ y $Y = (V', E')$ grafos, si $\psi \colon V \to V'$ es biyectiva y para cada $v, w \in V$, $\{v, w\} \in E$ si y solo si $\{\psi(v), \psi(w)\} \in E'$, decimos que ψ es un *isomorfismo de grafos* de X a Y, entonces X y Y son *grafos isomorfos* y lo denotamos por $X \cong Y$.

Definición 1.2.12 Se dice que un grafo $X = (V, E)$ es un *grafo completo* si para cada $v, w \in V$ con $v \neq w$ tenemos que $\{v, w\} \in E$. Si el grafo tiene n vértices se escribe K^n en lugar de X.

En la Figura 1.2 se exhibe el grafo completo de 8 vértices K^8.

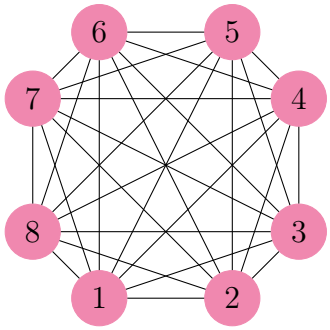


Figura 1.2: K^8.

Definición 1.2.13 Un *camino* es un grafo $P = (V, E)$ de la forma

$$V = \{v_1, v_2, \ldots, v_n\}, \quad E = \Big\{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}\Big\}$$

donde todos los v_i con $i \in \{1, \ldots, n\}$ son distintos. En este caso se dice que los vértices v_1 y v_n están *conectados o ligados* por P y son llamados los *extremos* del camino.

El número de aristas en un camino P es la *longitud* de P y se denota por $\|P\|$. Si P tiene longitud k, denotamos al camino por P^k en lugar de P, si $k = 0$ tenemos que $P^0 = K^1$.

Definición 1.2.14 Un *ciclo* $C = (V, E)$ es un grafo de la forma

$$V = \{v_1, v_2, \ldots, v_n\}, \quad E = \Big\{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}, \{v_n, v_1\}\Big\}$$

donde todos los v_i con $i \in \{1, \ldots, n\}$ son distintos.

Si P es un camino como en la Definición 1.2.13, tenemos que $P + \{x_1, x_n\}$ es un ciclo. El número de aristas (o vértices) de un ciclo C es la longitud de C. Decimos que C es un $k-$ciclo si C tiene longitud k y lo denotamos por C^k.

En la Figura 1.3 exhibimos el ciclo C^8.

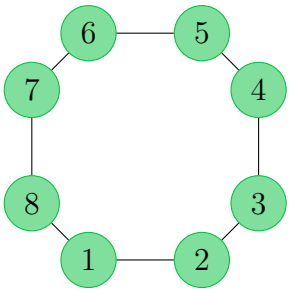


Figura 1.3: C^8.

Definición 1.2.15 La *cintura* de un grafo X es la longitud del ciclo más corto contenido en X y se denota por $g(X)$. En caso de que X no contenga ciclos, se dice que $g(X) = \infty$.

Definición 1.2.16 Un grafo $X = (V, E)$ es *conexo* si para cada $x, y \in V$ existe un camino que conecta a x con y.

Cuando estamos trabajando con un grafo que tiene muchos vértices, resulta complicado estudiar sus propiedades, una herramienta muy útil para agilizar este estudio es encontrar un grafo con menor número de vértices que conserve la conectividad de los vértices del grafo más grande. Esta herramienta es conocida como cubierta y se define a continuación.

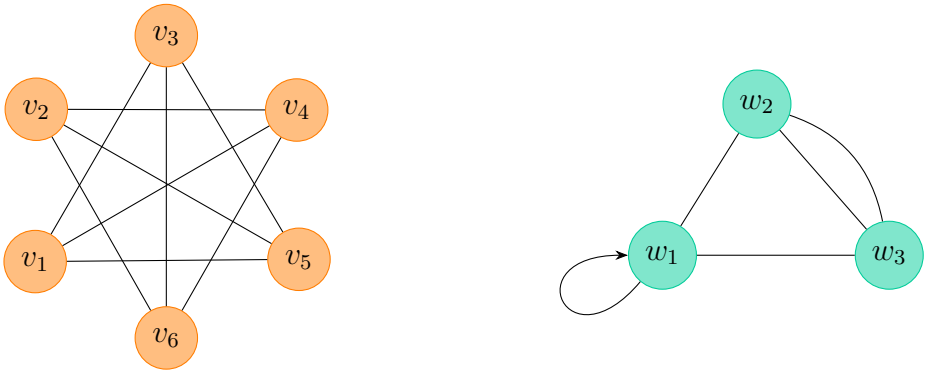
Definición 1.2.17 ([45], Definición 2.2) Sean $X = (V, E), Y = (V', E')$ grafos y ϕ un homomorfismo de X a Y.

- Si v es un vértice de X decimos que ϕ es biyectiva en v si el mapeo inducido por ϕ en E_v, $\phi_{E_v} : E_v \to E_{\phi(v)}$ es biyectiva, donde E_v es el conjunto de las aristas incidentes en v y $E_{\phi(v)}$ es el conjunto de las aristas incidentes en $\phi(v)$.

- Si para cada vértice v de X ϕ es biyectiva en v, entonces decimos que ϕ es localmente biyectiva.
- Si ϕ es localmente biyectiva y $\phi : V \to V'$ es sobreyectiva, entonces ϕ es una cubierta de X a Y por lo que decimos que X cubre a Y.

Observación 1.2.18 No debemos confundir isomorfismo de grafos con una cubierta, ya que en una cubierta se pide que $\phi : V \to V'$ sea solo sobreyectiva. De hecho los isomorfismos son los ejemplos más sencillos de cubiertas.

Ejemplo 1.2.19 Consideremos los grafos X y Y que se muestran en la Figura 1.4.



(a) $X = (V, E)$. (b) $Y = (V', E')$.

Figura 1.4

El homomorfismo $\phi\colon X \to Y$ donde $\phi(v_1) = \phi(v_4) = w_1$, $\phi(v_2) = \phi(v_3) = w_2$ y $\phi(v_5) = \phi(v_6) = w_3$ es una cubierta de X a Y.

Observación 1.2.20 De cierta manera una cubierta es como comprimir un grafo grande a un grafo chico, no debemos dejarnos llevar por la noción que nos da el nombre de cubierta en el contexto cotidiano, recordemos que la cubierta en grafos va de un grafo grande a uno más chico, no al revés.

Proposición 1.2.21 Sean $X = (V, E), Y = (V', E')$ grafos tales que X cubre a Y entonces X es $d-$regular si y solo si Y es $d-$regular.

Demostración.

Si X es $d-$regular, entonces para cada $v \in V$, $|E_v| = d$. Como X cubre a Y, existe una cubierta ϕ de X a Y, así que $\phi_{E_v}\colon E_v \to E_{\phi(v)}$ es biyectiva. Entonces $|E_{\phi(v)}| = |E_v| = d$ para cada $v \in V$. Dado que $\phi\colon V \to V'$ es sobreyectiva tenemos que para cada $v' \in V'$ existe $v \in V$ tal que $\phi(v) = v'$, entonces $|E_{v'}| = |E_{\phi(v)}| = |E_v| = d$, es decir, $|E_{v'}| = d$ para cada $v' \in V'$. Por lo tanto, Y es $d-$regular. Ahora si Y es $d-$regular, entonces para cada $w \in V'$, $|E_w| = d$. Dado que X cubre a Y, existe una cubierta ϕ de X a Y. Entonces existe $v \in V$ tal que $w = \phi(v)$, como $\phi_{E_v}\colon E_v \to E_{\phi(v)}$ es biyectiva tenemos que $d = |E_w| = |E_{\phi(v)}| = |E_v|$, es decir, $|E_v| = d$. Por lo tanto, X es $d-$regular. ■

Lema 1.2.22 Sean $X = (V, E), Y = (V', E')$ grafos tales que X cubre a Y y X es conexo, entonces Y es conexo.

Demostración.

Sean $w_1, w_2 \in V'$ y ϕ una cubierta de X a Y, entonces por la sobreyectividad de $\phi\colon V \to V'$ existen $v_1, v_2 \in V$ tales que $\phi(v_1) = w_1$ y $\phi(v_2) = w_2$. Como X es conexo, existe un camino $P = \{e_1, \ldots, e_r\}$ que conecta a v_1 y v_2, entonces por ser ϕ un homomorfismo de grafos tenemos que $P' = \{\phi(e_1), \ldots, \phi(e_r)\}$ es un camino que conecta a w_1 y w_2. Por lo tanto, Y es conexo. ■

Definición 1.2.23 Sea $r \geq 2$ un entero. Un grafo $X = (V, E)$ es llamado $r-$partito si V admite una partición de r clases tales que cada arista tiene sus extremos en diferentes clases; los vértices en la misma clase de la partición no deben ser adyacentes.

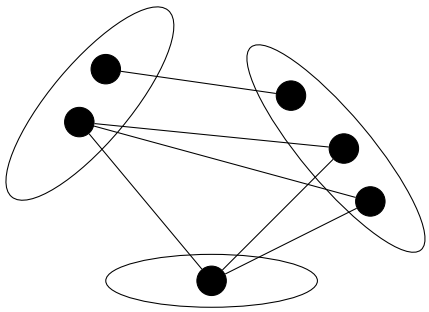


Figura 1.5: Grafo 3−partito.

Definición 1.2.24 Un grafo $X = (V, E)$ es *bipartito* si V puede ser divido en dos conjuntos V_1, V_2 tales que $V_1 \cup V_2 = V$ y $V_1 \cap V_2 = \emptyset$, de manera que cada arista de X es incidente a un vértice en V_1 y a un vértice en V_2. Podemos denotar a un grafo bipartito como $X = (V_1 \cup V_2, E)$.

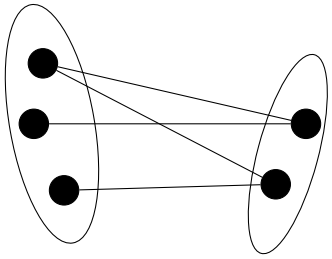


Figura 1.6: Grafo bipartito.

En las Figuras 1.5 1.6 se exhiben un grafo 3−partito y un grafo bipartito, respectivamente.

Definición 1.2.25 Sea $X = (V_1 \cup V_2, E)$ un grafo bipartito. Si todos los vértices en V_1 tienen el mismo grado d_{V_1}, y todos los vértices en V_2 tienen el mismo grado d_{V_2}, donde $d_{V_1} \neq d_{V_2}$, decimos que X es un *grafo bipartito* $(d_{V_1}, d_{V_2})-$*regular*.

Observación 1.2.26 Sea $X = (V_1 \cup V_2, E)$ un grafo bipartito regular con grados d_{V_1} y d_{V_2} de sus correspondientes conjuntos de vértices. Si $d_{V_1} = d_{V_2} = d$ decimos que X es un grafo bipartito d-regular.

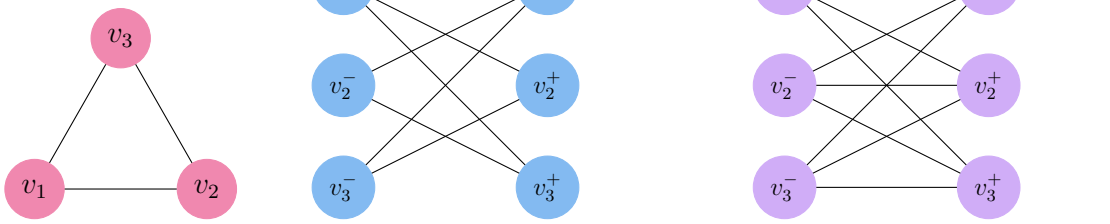
Si tenemos un grafo simple, es posible construir un grafo bipartito a partir de este, a través de una cubierta doble.

Definición 1.2.27 Sea $X = (V, E)$ un grafo, la *cubierta doble* de X es el grafo bipartito X' con conjunto de vértices $V_- \cup V_+$ tal que V_- y V_+ son copias de V, donde un vértice en V_- y un vértice en V_+ son adyacentes solo si los vértices correspondientes en V son adyacentes en X.

Observación 1.2.28 No se debe confundir la cubierta doble con aplicar dos veces la definición de cubierta, dado que esta última no precisamente genera un grafo bipartito.

Definición 1.2.29 ([3]) Sea $X = (V, E)$ un grafo con $V = \{v_1, v_2, \ldots, v_n\}$, la *cubierta doble extendida* de X es el grafo bipartito $Y = (V^- \cup V^+, E')$, donde $V^- = \{v_1^-, v_2^-, \ldots, v_n^-\}$, $V^+ = \{v_1^+, v_2^+, \ldots, v_n^+\}$ y $v_i = v_i^- = v_i^+$ para cada $i \in \{1, \ldots, n\}$, en cual $\{v_i^-, v_i^+\} \in E'$ y $\{v_i^-, v_j^+\} \in E'$ si y solo si $\{v_i, v_j\} \in E$.

Ejemplo 1.2.30 Tomemos al grafo K^3, su cubierta doble es un grafo bipartito 2-regular, mientras que su cubierta doble extendida es un grafo bipartito 3-regular.



(a) K^3 (b) Cubierta doble de K^3 (c) Cubierta doble extendida de K^3

1.2.1. Operador y matriz de adyacencia

Definición 1.2.31 Sea $X = (V, E)$ un grafo simple con $V = \{v_1, v_2, \ldots, v_n\}$. La *matriz de adyacencia* de X es la matriz $A = (a_{ij})$, donde

$$a_{ij} = \begin{cases} 1 & \text{si } \{v_i, v_j\} \in E \\ 0 & \text{de otro modo.} \end{cases}$$

Observación 1.2.32 La matriz de adyacencia de un grafo simple es una matriz simétrica, pues cada arista que une v_i con v_j también une a v_j con v_i.

Observación 1.2.33 Si $X = (V \cup U, E)$ es un grafo bipartito con $V = \{v_1, \ldots, v_n\}$ y $U = \{u_1, \ldots, u_m\}$, la matriz de adyacencia de X es de la forma

$$\begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix},$$

en la cual $B = (b_{ij})$ es una matriz de tamaño $n \times m$, donde

$$b_{ij} = \begin{cases} 1 & \text{si } \{v_i, u_j\} \in E \\ 0 & \text{de otro modo.} \end{cases}$$

Como esta matriz es la que nos da la información de adyacencia entre los vértices de las particiones, B recibe el nombre de *matriz de biadyacencia.* [7]

Definición 1.2.34 Sea $X = (V, E)$ un grafo. En el espacio vectorial $L^2(V)$ (ver Definición 1.1.1) definimos la siguiente función.

$$\begin{aligned} \mathscr{A} \colon L^2(V) &\longrightarrow L^2(V) \\ f &\longmapsto \mathcal{A}(f), \end{aligned}$$

donde

$$\begin{aligned} \mathscr{A}(f) \colon V &\longrightarrow \mathbb{C} \\ v &\longmapsto \sum_{w \in N_X(v)} f(w). \end{aligned}$$

Proposición 1.2.35 Sea $X = (V, E)$ un grafo, $\mathscr{A}$ es un operador lineal sobre $L^2(V)$.

Demostración.

Sean $f, g \in L^2(V)$ y $\alpha \in \mathbb{C}$. Entonces

$$\begin{aligned} \mathscr{A}(\alpha f + g)(v) = \sum_{w \in N_X(v)} (\alpha f + g)(w) &= \sum_{w \in N_X(v)} \alpha f(w) + g(w) \\ &= \sum_{w \in N_X(v)} \alpha f(w) + \sum_{w \in N_X(v)} g(w) \\ &= \alpha \sum_{w \in N_X(v)} f(w) + \sum_{w \in N_X(v)} g(w) \\ &= \alpha \mathscr{A}(f)(v) + \mathscr{A}(g)(v) \\ &= (\alpha \mathscr{A}(f) + \mathscr{A}(g))(v), \end{aligned}$$

es decir, $\mathscr{A}(\alpha f + g)(v) = (\alpha \mathscr{A}(f) + \mathscr{A}(g))(v)$, para cada $v \in V$. Por lo tanto, $\mathscr{A}$ es un operador $\mathbb{C}$-lineal. ■

Teorema 1.2.36 Sea $X = (V, E)$ un grafo, A su matriz de adyacencia y $\mathcal{B}$ la base usual de $L^2(V)$, entonces $[\mathscr{A}]_{\mathcal{B}} = A$.

Demostración.

Sean $V = \{v_1, \ldots, v_n\}$ y $\mathcal{B} = \{\delta_{v_1}, \ldots, \delta_{v_n}\}$. Entonces

$$[\mathscr{A}]_{\mathcal{B}} = \begin{bmatrix} [\mathscr{A}(\delta_{v_1})]_{\mathcal{B}} & [\mathscr{A}(\delta_{v_2})]_{\mathcal{B}} & \ldots & [\mathscr{A}(\delta_{v_n})]_{\mathcal{B}} \end{bmatrix}.$$

Sea $v \in V$ y sea $i \in \{1, \ldots, n\}$, como $\mathscr{A}(\delta_{v_i})(v) = \sum_{w \in N_X(v)} \delta_{v_i}(w)$ tenemos los siguientes casos.

Si $v_i \notin N_X(v)$ entonces para cada $w \in N_X(v)$, $w \neq v_i$, así que

$$\sum_{w \in N_X(v)} \delta_{v_i}(w) = \sum_{w \in N_X(v)} 0 = 0,$$

es decir, $\mathscr{A}(\delta_{v_i})(v) = 0$.

Si $v_i \in N_X(v)$ entonces

$$\sum_{w \in N_X(v)} \delta_{v_i}(w) = \delta_{v_i}(v_i) + \sum_{\substack{w \in N_X(v) \\ w \neq v_i}} \delta_{v_i}(w) = 1 + 0 = 1,$$

es decir, $\mathscr{A}(\delta_{v_i})(v) = 1$.

Entonces

$$\begin{aligned} \mathscr{A}(\delta_{v_i})(v) &= \begin{cases} 1 & \text{si } \ v \in N_X(v_i) \\ 0 & \text{si } \ v \notin N_X(v_i) \end{cases} \\ &= 1_{N_X(v_i)}(v), \end{aligned}$$

es decir $\mathscr{A}(\delta_{v_i})(v) = 1_{N_X(v_i)}(v)$ para cada $v \in V$, así que $\mathscr{A}(\delta_{v_i}) = 1_{N_X(v_i)}$ para cada $i \in \{1, \ldots, n\}$. Dado que $\mathcal{B}$ es una base ortonormal de $L^2(V)$ y $\mathscr{A}(\delta_{v_i}) \in L^2(V)$ tenemos que $\mathscr{A}(\delta_{v_i}) = \sum_{a \in V} \mathscr{A}(\delta_{v_i})(a)\delta_a$, entonces $\mathscr{A}(\delta_{v_i}) = \sum_{a \in V} \mathscr{A}(\delta_{v_i})(a)\delta_a = \sum_{a \in V} 1_{N_X(v_i)}(a)\delta_a$, así que para cada $i \in \{1, \ldots, n\}$

$$\mathscr{A}(\delta_{v_i}) = 1_{N_X(v_i)}(v_1)\delta_{v_1} + \cdots + 1_{N_X(v_i)}(v_n)\delta_{v_n}.$$

Entonces

$$[\mathscr{A}]_{\mathcal{B}} = \begin{bmatrix} 1_{N_X(v_1)}(v_1) & 1_{N_X(v_2)}(v_1) & \ldots & 1_{N_X(v_n)}(v_1) \\ 1_{N_X(v_1)}(v_2) & 1_{N_X(v_2)}(v_2) & \ldots & 1_{N_X(v_n)}(v_2) \\ \vdots & \vdots & \ddots & \vdots \\ 1_{N_X(v_1)}(v_n) & 1_{N_X(v_2)}(v_n) & \ldots & 1_{N_X(v_n)}(v_n) \end{bmatrix}.$$

Por lo tanto, $[\mathscr{A}]_{\mathcal{B}} = \left(1_{N_X(v_j)}(v_i)\right) = A$. ■

Observación 1.2.37 $\mathscr{A}$ es llamado el *operador de adyacencia del grafo* X u *operador de Hecke.*

Corolario 1.2.38 Sea $X = (V, E)$ un grafo y $\mathscr{A}$ su operador de adyacencia, entonces $\mathscr{A}$ es un operador autoadjunto.

Demostración.

Por el Teorema 1.2.36 la representación matricial del operador $\mathscr{A}$ en la base usual de $L^2(V)$ es la matriz de adyacencia del grafo, la cual es simétrica y por consiguiente autoadjunta. Por lo tanto, $\mathscr{A}$ es un operador autoadjunto. ■

Definición 1.2.39 Sea $X = (V, E)$ un grafo y $\mathscr{A}$ su operador de adyacencia, el *espectro de* X es el conjunto de valores propios de $\mathscr{A}$ y es denotado por $Spec(X)$.

Proposición 1.2.40 Sea $X = (V, E)$ un grafo entonces $Spec(X) \subseteq \mathbb{R}$.

Demostración.

Sea $\lambda \in Spec(X)$,entonces existe $f \in L^2(V) \setminus \{0\}$ tal que $\mathscr{A}(f) = \lambda f$. Como $\mathscr{A}$ es un operador autoadjunto tenemos que $\langle \mathscr{A}(f), f\rangle_2 = \langle f, \mathscr{A}(f)\rangle_2$ entonces $\langle \lambda f, f\rangle_2 = \langle f, \lambda f\rangle_2$, así que $\lambda\langle f, f\rangle_2 = \overline{\lambda}\langle f, f\rangle_2$. Como $\langle f, f\rangle_2 \neq 0$ tenemos que $\lambda = \overline{\lambda}$, así que $\lambda \in \mathbb{R}$. Por lo tanto, $Spec(X) \subseteq \mathbb{R}$.

■

Observación 1.2.41 Si el espectro consiste en distintos valores propios tales que $\lambda_1 > \lambda_2 > \ldots > \lambda_r$ con multiplicidades $m_1, m_2, \ldots, m_r$ respectivamente, podemos denotar al espectro de X como sigue:

$$Spec(X) = \begin{pmatrix} \lambda_r & \ldots & \lambda_2 & \lambda_1 \\ m_r & \ldots & m_2 & m_1 \end{pmatrix}.$$

Teorema 1.2.42 Sea $X = (V, E)$ un grafo $d-$regular entonces

1) $d \in Spec(X)$,

2) si $\lambda \in Spec(X)$ entonces $|\lambda| \leq d$.

Demostración.

1) Sea $f_c \in L^2(V)$ tal que $f_c(v) = c$ para toda $v \in V$ con $c \in \mathbb{C} \setminus \{0\}$ fijo. Entonces

$$\mathscr{A}(f_c)(v) = \sum_{w \in N_X(v)} f_c(w) = \sum_{w \in N_X(v)} c = d \cdot c = d \cdot f_c(v),$$

es decir, $\mathscr{A}(f_c)(v) = d \cdot f_c(v)$ para cada $v \in V$. Entonces $f_c \in L^2(V) \setminus \{0\}$ es tal que $\mathscr{A}(f_c) = d \cdot f_c$. Por lo tanto, $d \in Spec(X)$.

2) Sea $\lambda \in Spec(X)$, existe $f \in L^2(V) \setminus \{0\}$ tal que $\mathscr{A}(f) = \lambda f$. Sea $v_0 \in V$ tal que $|f(v_0)| = \max_{v \in V} |f(v)|$ donde $|f(v_0)| > 0$ ya que $f \neq 0$. Luego

$$|\lambda|\,|f(v_0)| = |\lambda f(v_0)| = |\mathscr{A}(f)(v_0)| = \left| \sum_{w \in N_X(v_0)} f(w) \right| \leq \sum_{w \in N_X(v_0)} |f(w)|$$
$$\leq \sum_{w \in N_X(v_0)} |f(v_0)| = d\,|f(v_0)|,$$

es decir, $|\lambda|\,|f(v_0)| \leq d\,|f(v_0)|$. Entonces $|\lambda| \leq d$.

■

Teorema 1.2.43 Sea $X = (V_1 \cup V_2, E)$ un grafo bipartito, para cada $\lambda \in Spec(X)$ se cumple que $-\lambda \in Spec(X)$.

Demostración.

Sea $\lambda \in Spec(X)$, existe $f \in L^2(V_1 \cup V_2) \setminus \{0\}$ tal que $\mathscr{A}(f) = \lambda f$. Definimos la función $\widetilde{f}\colon V_1 \cup V_2 \to \mathbb{C}$ como sigue

$$\widetilde{f}(v) = \begin{cases} f(v) & \text{si } \ v \in V_1 \\ -f(v) & \text{si } \ v \in V_2. \end{cases}$$

Sea $v \in V_1$, si $w \in N_X(v)$ tenemos que $\{v, w\} \in E$, más aún por ser X bipartito $w \in V_2$, así que $N_X(v) \subseteq V_2$. Entonces

$$\begin{aligned} \mathscr{A}(\widetilde{f})(v) &= \sum_{w \in N_X(v)} \widetilde{f}(w) = \sum_{w \in N_X(v)} -f(w) = -\sum_{w \in N_X(v)} f(w) = -\mathscr{A}(f)(v) \\ &= -\lambda f(v) \\ &= -\lambda \widetilde{f}(v), \end{aligned}$$

es decir, $\mathscr{A}(\widetilde{f})(v) = -\lambda \widetilde{f}(v)$ para cada $v \in V_1$.

Sea $v \in V_2$, si $w \in N_X(v)$ tenemos que $\{v, w\} \in E$, más aún por ser X bipartito $w \in V_1$, así que $N_X(v) \subseteq V_1$. Entonces

$$\mathscr{A}(\widetilde{f})(v) = \sum_{w \in N_X(v)} \widetilde{f}(w) = \sum_{w \in N_X(v)} f(w) = \mathscr{A}(f)(v) = \lambda f(v) = \lambda(-\widetilde{f}(v)),$$

es decir, $\mathscr{A}(\widetilde{f})(v) = -\lambda \widetilde{f}(v)$ para cada $v \in V_2$. Así que para todo $v \in V_1 \cup V_2$, $\mathscr{A}(\widetilde{f})(v) = -\lambda \widetilde{f}(v)$, de ahí que $\mathscr{A}(\widetilde{f}) = -\lambda \widetilde{f}$. Por lo tanto, $-\lambda \in Spec(X)$. ■

Además de la matriz de adyacencia, existe otra matriz que nos muestra la relación de incidencia que tienen los vértices de un grafo con sus aristas.

Definición 1.2.44 Sea $X = (V, E)$ un grafo simple con $V = \{v_1, \ldots, v_n\}$ y $E = \{e_1, \ldots, e_s\}$. La matriz de incidencia de X es la matriz $M = (m_{ij})$, donde

$$m_{ij} = \begin{cases} 1 & \text{si } v_i \in e_j \\ 0 & \text{de otro modo.} \end{cases}$$

1.2.2. Grafos de Cayley

Definición 1.2.45 Sea G un grupo y $S \subseteq G$, se dice que S es un conjunto generador de G, si $G = \langle S \rangle$. Si además para cada $x \in S$ tenemos que $s^{-1} \in S$ ($-s \in S$ si G es un grupo aditivo), decimos que S es un conjunto simétrico de generadores de G.

Definición 1.2.46 Sea G un grupo finito y S un conjunto simétrico de generadores de G. Se define el conjunto $E = \{\{x, y\} \in [G]^2 \mid xy^{-1} \in S\}$. Y a partir de E se define el grafo $Cay(G, S) := (G, E)$ llamado *grafo de Cayley* con conjunto de vértices G.

Observación 1.2.47 Si G es un grupo aditivo $E = \{\{x, y\} \in [G]^2 \mid x - y \in S\}$.

Proposición 1.2.48 Sea $Cay(G, S)$ un grafo de Cayley entonces

$$E = \{\ \{x, sx\} \mid s \in S \text{ y } x \in G\}.$$

Demostración.

Sean $x \in G$, $s \in S$ y $E' = \{\ \{x, sx\} \mid s \in S \text{ y } x \in G\}$. Probemos que $E' = E$. Sea $\{x, y\} \in E$ tenemos que $xy^{-1} \in S$ entonces $xy^{-1} = s'$ para algún $s' \in S$ así que $sx = y$ con $s = (s')^{-1} \in S$ de ahí que $\{x, y\} = \{x, sx\} \in E'$. Por consiguiente $E \subseteq E'$. Ahora sea $\{x, sx\} \in E'$ tenemos que $x(sx)^{-1} = xx^{-1}s^{-1} = s^{-1} \in S$, así que $\{x, sx\} \in E$ entonces $E' \subseteq E$. Por lo tanto, $E = \{\{x, sx\} | s \in S \text{ y } x \in G\}$. ■

Observación 1.2.49 Si pedimos que S no contenga al neutro del grupo entonces los elementos de E son subconjuntos de G con dos elementos distintos, es decir $Cay(G, S)$ no tendrá bucles.

Corolario 1.2.50 Sea $Cay(G, S)$ un grafo de Cayley y $x \in G$. Entonces

$$N_{Cay(G,S)}(x) = \{sx \mid s \in S\}.$$

Demostración.

Sea $x \in G$, consideremos $N = \{sx \mid s \in S\}$. Probemos que $N_{Cay(G,S)}(x) = N$. Sea $y \in N_{Cay(G,S)}(x)$ tenemos que $\{x, y\} \in E$, así que $xy^{-1} = s'$ para algún $s' \in S$ entonces $y = sx$ con $s = (s')^{-1} \in S$, de ahí que $y \in N$ y por consiguiente $N_{Cay(G,S)}(x) \subseteq N$. Luego sea $y \in N$ tenemos que $y = s_0 x$ para algún $s_0 \in S$ entonces $y^{-1} = x^{-1}s_0^{-1}$ de ahí que $xy^{-1} = s_0^{-1} \in S$, es decir, $xy^{-1} \in S$ entonces $\{x, y\} \in E$ y por consiguiente $y \in N_{Cay(G,S)}(x)$ así que $N \subseteq N_{Cay(G,S)}(x)$. Por lo tanto, $N_{Cay(G,S)}(x) = \{sx \mid s \in S\}$. ■

Observación 1.2.51 Sea $f \in L^2(G)$ y $x \in G$,. Si $y \in N_{Cay(G,S)}(x)$ entonces $xy^{-1} = s$ para algún $s \in S$, así que y puede reescribirse como $y = s^{-1}x$.Entonces el operador de adyacencia del grafo $Cay(G, S)$ es

$$\mathscr{A}(f)(x) = \sum_{y \in N_{Cay(G,S)}(x)} f(y) = \sum_{s \in S} f(s^{-1}x).$$

Teorema 1.2.52 Sea $Cay(G, S)$ un grafo de Cayley, entonces:

1) $Cay(G, S)$ es $|S|-$regular.

2) $Cay(G, S)$ es conexo.

Demostración.

1) Sea $x \in G$ definimos la función $f\colon S \longrightarrow N_{Cay(G,S)}(x)$ tal que $f(s) = sx$. Sean $s_1, s_2 \in S$ tales que $f(s_1) = f(s_2)$ entonces $s_1x = s_2x$ así que $s_1 = s_2$, por lo que, f es inyectiva. Ahora bien, si $y \in N_{Cay(G,S)}(x)$ tenemos que $y = sx$ para alguna $s \in S$, de ahí que para toda $y \in N_{Cay(G,S)}(x)$ existe $s \in S$ tal que $f(s) = y$. Entonces f es sobreyectiva y por consiguiente, biyectiva. Así que para cada $x \in G$, $|N_{Cay(G,S)}(x)| = |S|$, entonces cada vértice de G tiene grado $|S|$. Por lo tanto, $Cay(G, S)$ es un grafo $|S|-$regular.

2) Sea $x \in G$, tenemos que $x = s_1s_2 \dots s_r$ con $s_i \in S$, $i \in \{1, \dots, r\}$ y $r \in \mathbb{N}$. Sea 1 el elemento neutro del grupo, tenemos que $1(s_r)^{-1} = s_r^{-1} \in S$, así que $e_1 = \{1, s_r\} \in E$, luego

$$(s_r)(s_{r-1} \cdot s_r)^{-1} = s_{r-1}^{-1} \in S,$$

por lo que $e_2 = \{s_r, s_{r-1}s_r\} \in E$

$$(s_{r-1}s_r)(s_{r-2} \cdot s_{r-1}s_r)^{-1} = s_{r-2}^{-1} \in S.$$

entonces $e_3 = \{s_{r-1}s_r, s_{r-2}s_{r-1}s_r\} \in E$.

Siguiendo este proceso, tenemos que

$$s_2 \dots s_{r-1}s_r(s_1 \cdot s_2 \dots s_{r-1}s_r)^{-1} = s_1^{-1} \in S,$$

por lo que $\{s_2 \dots s_{r-1}s_r, s_1 \cdot s_2 \dots s_{r-1}s_r\} \in E$, es decir, $e_r = \{s_2 \dots s_{r-1}s_r, x\} \in E$. Entonces $\{e_1, e_2, \dots, e_r\}$ es un camino que une a x con 1. Así que, para cada cada $x \in G$ existe un camino que une a x con 1. Sean $x_1, x_2 \in G$ existen P_1 y P_2 caminos que unen a x_1 con 1 y 1 con x_2 respectivamente, entonces $P_1 + P_2$ es un camino que une a x_1 con x_2. Por lo tanto, $Cay(G, S)$ es conexo.

■

Ejemplo 1.2.53 Para el grupo aditivo $\mathbb{Z}/m\mathbb{Z}$ tenemos que $Cay(\mathbb{Z}/m\mathbb{Z}, \{1, m-1\})$ es el grafo ciclo C^m y $Cay(\mathbb{Z}/m\mathbb{Z}, \{1, \ldots, m-1\})$ es el grafo completo K^m. En la Figura 1.8 exhibimos el grafo de Cayley $Cay(\mathbb{Z}/4\mathbb{Z}, \{1, 3\})$, el cual es el grafo ciclo C^4 y en la Figura 1.9 exhibimos el grafo de Cayley $Cay(\mathbb{Z}/4\mathbb{Z}, \{1, 2, 3\})$, el cual es el grafo completo K^4.

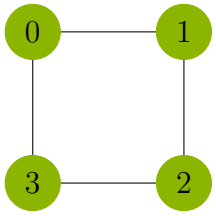


Figura 1.8: $Cay(\mathbb{Z}/4\mathbb{Z}, \{1, 3\})$.

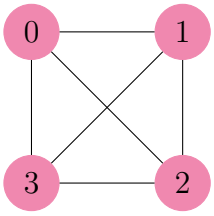


Figura 1.9: $Cay(\mathbb{Z}/4\mathbb{Z}, \{1, 2, 3\})$.

Ejemplo 1.2.54 Consideremos al grupo $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ y sea $S = \{(12), (23), (123), (132)\}$ un conjunto simétrico de generadores de S_3. Construyamos el grafo de Cayley $Cay(S_3, S)$. Recordemos que en los grafos de Cayley las aristas tienen la siguiente forma $\{x, sx\}$ con $x \in S_3$ y $s \in S$. En la Figura 1.10 exhibimos el grafo de Cayley $Cay(S_3, \{(12), (23), (123), (132)\})$.

Vértice	Vecinos			
x	$(12)x$	$(23)x$	$(123)x$	$(132)x$
(1)	(12)	(23)	(123)	(132)
(12)	(1)	(132)	(13)	(23)
(13)	(132)	(123)	(23)	(12)
(23)	(123)	(1)	(12)	(13)
(123)	(23)	(13)	(132)	(1)
(132)	(13)	(12)	(1)	(123)

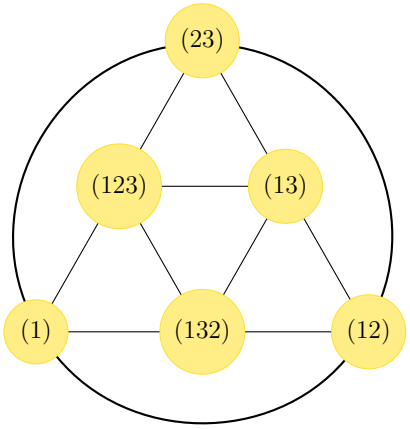


Figura 1.10: $Cay(S_3, \{(12), (23), (123), (132)\})$.

1.3. Representaciones y caracteres de grupos

En esta sección mencionaremos algunos conceptos y resultados relacionados a la teoría de representaciones y caracteres de grupos. Los textos que se consultaron son [60], [45] y [40].

Definición 1.3.1 Sea V un espacio vectorial de dimensión finita. El *grupo lineal general* de V denotado por $GL(V)$ es el grupo de todas las transformaciones lineales invertibles de V sobre sí mismo.

Definición 1.3.2 Sea G un grupo finito. Una *representación* de dimensión finita de G sobre $\mathbb{C}$ es el par (V, ρ) donde V un $\mathbb{C}-$espacio vectorial de dimensión finita y ρ un homomorfismo del grupo G a $GL(V)$. Definimos el *grado* de ρ como la dimensión de V como $\mathbb{C}-$espacio vectorial.

Observación 1.3.3 En ocasiones haremos un abuso de notación al referirnos a la representación mediante V, esto lo haremos cuando ρ ya es conocido, de igual manera a veces nos referiremos a la representación como ρ cuando el espacio vectorial V ya es conocido.

Observación 1.3.4 Tenemos que $\rho\colon G \to GL(V)$ induce una acción de G en V dada por $g \cdot v = \rho(g)(v)$, entonces para todo $g, h \in G$, $v, w \in V$ y $\alpha \in \mathbb{C}$ se cumple que:

1) $\rho(g)v \in V$.

2) $\rho(gh)v = (\rho(g) \circ \rho(h))v$.

3) Si e_G es la identidad de G, entonces $\rho(e_G)v = v$.

4) $\rho(g)\ (\alpha v) = \alpha(\rho(g)v)$.

5) $\rho(g)(v + w) = \rho(g)v + \rho(g)w$.

Definición 1.3.5 Sea (V, ρ) una representación de un grupo G y sea $\langle \cdot, \cdot \rangle$ un producto interno en V. Si para todo $g \in G$, $v, w \in V$

$$\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle$$

decimos que (V, ρ) es una *representación unitaria* con respecto a $\langle \cdot, \cdot \rangle$.

Observación 1.3.6 Si consideramos que ρ define una acción en G sobre V como en la Observación 1.3.4, entonces decimos que $\langle \cdot, \cdot \rangle$ es $G-$*invariante* si para todo $g \in G$ y $v, w \in V$ se cumple que $\langle g \cdot v, g \cdot w \rangle = \langle v, w \rangle$.

Lema 1.3.7 Sea (V, ρ) una representación para un grupo finito G. Entonces existe un producto interno $G-$invariante en V.

Demostración.

Sea $\mathcal{B} = \{v_1, \ldots, v_n\}$ una base de V, definamos la función $\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{C}$ como sigue, para cada $v, w \in V$ tenemos que $v = \sum_{i=1}^{n} \alpha_i v_i$ y $w = \sum_{i=1}^{n} \beta_i v_i$ para algunos $\alpha_i, \beta_i \in \mathbb{C}$ con $i \in \{1, \ldots, n\}$, entonces $\langle v, w \rangle = \sum_{i=1}^{n} \alpha_i \overline{\beta_i}$. Probemos que $\langle \cdot, \cdot \rangle$ es un producto interno sobre V. Sean $v, w, u \in V$ como arriba, $u = \sum_{i=1}^{n} \gamma_i v_i$ y sea $\mu \in \mathbb{C}$. Entonces

1) $\langle v + w, u \rangle = \sum_{i=1}^{n} (\alpha_i + \beta_i)\overline{\gamma_i} = \sum_{i=1}^{n} \alpha_i \overline{\gamma_i} + \sum_{i=1}^{n} \beta_i \overline{\gamma_i} = \langle v, u \rangle + \langle w, u \rangle.$

2) $\langle \mu v, w \rangle = \sum_{i=1}^{n} \mu \alpha_i \overline{\beta_i} = \mu \sum_{i=1}^{n} \alpha_i \overline{\beta_i} = \langle v, w \rangle.$

3) $\langle v, w \rangle = \sum_{i=1}^{n} \alpha_i \overline{\beta_i} = \sum_{i=1}^{n} \overline{\overline{\alpha_i}\, \beta_i} = \overline{\sum_{i=1}^{n} \overline{\alpha_i}\, \beta_i} = \overline{\sum_{i=1}^{n} \beta_i \overline{\alpha_i}} = \overline{\langle w, v \rangle}.$

4) $\langle v, v \rangle = \sum_{i=1}^{n} \alpha_i \overline{\alpha_i} = \sum_{i=1}^{n} |\alpha_i|^2 \geq 0.$

5) $\langle v, v \rangle = 0 \iff \sum_{i=1}^{n} |\alpha_i|^2 = 0 \iff \alpha_i = 0$ para cada $i \in \{1, \ldots, n\} \iff v = 0.$

Por lo tanto, $\langle \cdot, \cdot \rangle$ es un producto interno sobre V.

Sea

$$\begin{aligned} \langle \cdot, \cdot \rangle' \colon V \times V &\longrightarrow \mathbb{C} \\ (v, w) &\longmapsto \sum_{x \in G} \langle \rho(x)v, \rho(x)w \rangle. \end{aligned}$$

Probemos que $\langle \cdot, \cdot \rangle'$ es un producto interno sobre V. Sean $v, w, u \in V$ y sea $\mu \in \mathbb{C}$. Entonces

1)

$$\begin{aligned} \langle v + w, u \rangle' &= \sum_{x \in G} \langle \rho(x)(v + w), \rho(x)u \rangle \\ &= \sum_{x \in G} \langle \rho(x)(v) + \rho(x)(w), \rho(x)u \rangle \\ &= \sum_{x \in G} \langle \rho(x)v, \rho(x)u \rangle + \langle \rho(x)w, \rho(x)u \rangle \\ &= \sum_{x \in G} \langle \rho(x)v, \rho(x)u \rangle + \sum_{x \in G} \langle \rho(x)v, \rho(x)u \rangle \\ &= \langle v, u \rangle' + \langle w, u \rangle'. \end{aligned}$$

2)
$$\begin{aligned}\langle \mu v, w\rangle' = \sum_{x\in G}\langle \rho(x)(\mu v), \rho(x)w\rangle &= \sum_{x\in G}\langle \mu\rho(x)(v), \rho(x)w\rangle \\ &= \sum_{x\in G}\mu\langle \rho(x)v, \rho(x)w\rangle \\ &= \mu\sum_{x\in G}\langle \rho(x)v, \rho(x)w\rangle \\ &= \mu\langle v, w\rangle'.\end{aligned}$$

3)
$$\begin{aligned}\langle v, w\rangle' = \sum_{x\in G}\langle \rho(x)v, \rho(x)w\rangle = \sum_{x\in G}\overline{\langle \rho(x)w, \rho(x)v\rangle} &= \overline{\sum_{x\in G}\langle \rho(x)w, \rho(x)v\rangle} \\ &= \overline{\langle w, v\rangle'}.\end{aligned}$$

4) Para cada $x \in G$ tenemos que $\rho(x)v \in V$, así que $0 \leq \langle \rho(x)v, \rho(x)v\rangle$, entonces $0 \leq \sum_{x\in G}\langle \rho(x)v, \rho(x)v\rangle = \langle v, v\rangle'$.

5)
$$\begin{aligned}\langle v, v\rangle' = 0 \iff \sum_{x\in G}\langle \rho(x)v, \rho(x)v\rangle = 0 &\iff \langle \rho(x)v, \rho(x)v\rangle = 0 \\ &\iff \rho(x)v = 0 \\ &\iff v = 0.\end{aligned}$$

Entonces $\langle \cdot, \cdot\rangle'$ es un producto interno sobre V. Por último verifiquemos que con este producto interno ρ es una representación unitaria. Sean $v, w \in V$ y sea $a \in G$. Entonces

$$\begin{aligned}\langle \rho(a)v, \rho(a)w\rangle' = \sum_{x\in G}\langle \rho(x)\rho(a)v, \rho(x)\rho(a)w\rangle &= \sum_{x\in G}\langle \rho(xa)v, \rho(xa)w\rangle \\ &= \sum_{y=xa\in G}\langle \rho(y)v, \rho(y)w\rangle \\ &= \langle v, w\rangle',\end{aligned}$$

es decir, $\langle \rho(a)v, \rho(a)w\rangle' = \langle v, w\rangle'$. Por lo tanto, $\langle \cdot, \cdot\rangle'$ es un producto interno $G-$invariante sobre V. ■

Definición 1.3.8 El grupo lineal general, denotado por $GL(n, \mathbb{C})$ es el grupo de las matrices invertibles de tamaño $n \times n$ con coeficientes en $\mathbb{C}$.

Definición 1.3.9 Sea G un grupo finito de orden n. Una *representación matricial* de G es un homomorfismo $\pi\colon G \longrightarrow GL(n, \mathbb{C})$. El *grado* de π es n.

Definición 1.3.10 Sea G un grupo y π una representación matricial de G, decimos que π es una *representación matricial unitaria* si para cada $g \in G$ tenemos que $\overline{\pi(g)}^t\pi(g) = I_{n\times n}$, es decir, si para cada $g \in G$, $\pi(g)$ es una matriz unitaria.

Observación 1.3.11 Sea G un grupo, podemos ir y venir entre las dos definiciones de representaciones de la siguiente manera. Sea $\pi\colon G \to GL(n,\mathbb{C})$ una representación matricial de G de grado n, entonces la función $\rho\colon G \to GL(\mathbb{C}^n)$ definida por $\rho(g)(v) = \pi(g)v$ para cada $g \in G$ y $v \in \mathbb{C}^n$, es una transformación lineal, entonces $(\mathbb{C}^n, \rho)$ es una representación de G de grado n. Ahora si (V,ρ) es una representación de G de grado n y $\mathcal{B}$ es una base para V, entonces la función $\pi\colon G \to G(n,\mathbb{C})$ definida por $\pi(g) = [\rho(g)]_{\mathcal{B}}$ es una representación matricial de G de grado n.

Definición 1.3.12 Sean (V,ρ) y (W,ϕ) representaciones de un grupo finito G y sea θ una función de V a W.

- Si para cada $g \in G$ y $v \in V$, $\theta(\rho(g)v) = \phi(g)\theta(v)$, decimos que θ es $G-$*invariante*.
- Si θ es una transformación lineal y es $G-$invariante, decimos que θ es un $G-$*homomorfismo*.
- Si θ es un $G-$isomorfismo, es decir, un isomorfismo de espacios vectoriales que es $G-$invariante, decimos que (V,ρ) y (W,ϕ) son equivalentes y lo denotamos por $\rho \cong \phi$ o bien $V \cong W$.

Definición 1.3.13 Sean $\pi\colon G \longrightarrow GL(n,\mathbb{C})$ y $\sigma\colon G \longrightarrow GL(m,\mathbb{C})$ dos representaciones matriciales de un grupo finito G. Si $n = m$ y si existe $T \in GL(n,\mathbb{C})$ tal que para cada $g \in G$

$$T\sigma(g)T^{-1} = \pi(g),$$

decimos que π es *equivalente* a σ y lo denotamos por $\pi \cong \sigma$.

Proposición 1.3.14 Sean (V,ρ) y (W,ϕ) dos representaciones de un grupo finito G y sea $\psi\colon V \to W$ un G-isomorfismo. Si $\langle\cdot,\cdot\rangle$ es un producto interno G-invariante sobre W, entonces

$$\begin{aligned}\langle\cdot,\cdot\rangle''\colon V\times V &\longrightarrow \mathbb{C}\\ (v,w) &\longmapsto \langle\psi(v),\psi(w)\rangle\end{aligned}$$

es un producto interno sobre V.

Demostración.

Sean $u, v, w \in V$ y $\alpha \in \mathbb{C}$

1)

$$\begin{aligned}\langle u+v, w\rangle'' = \langle\psi(u+v),\psi(w)\rangle &= \langle\psi(u)+\psi(v),\psi(w)\rangle\\ &= \langle\psi(u),\psi(w)\rangle + \langle\psi(v),\psi(w)\rangle\\ &= \langle u,w\rangle'' + \langle v,w\rangle''.\end{aligned}$$

2)
$$\langle \alpha v, w\rangle'' = \langle \psi(\alpha v), \psi(w)\rangle = \langle \alpha\psi(v), \psi(w)\rangle = \alpha\langle \psi(v), \psi(w)\rangle = \alpha\langle v, w\rangle''.$$

3)
$$\langle v, w\rangle'' = \langle \psi(v), \psi(w)\rangle = \overline{\langle \psi(w), \psi(v)\rangle} = \overline{\langle w, v\rangle''}.$$

4)
$$\langle v, v\rangle'' = \langle \psi(v), \psi(v)\rangle \geq 0.$$

5) $\langle v, v\rangle'' = 0 \iff \langle \psi(v), \psi(v)\rangle = 0 \iff \psi(v) = 0 \iff v = 0.$

Por lo tanto, $\langle \cdot, \cdot\rangle''$ es un producto interno sobre V. ■

Proposición 1.3.15 Si G es un grupo finito toda representación de G es equivalente a una representación unitaria. (c.f [60])

Definición 1.3.16 Sea (V, ρ) una representación de un grupo finito G y sea W un subespacio de V si para cada $g \in G$ y $w \in W$ se satisface que $\rho(g)(w) \in W$, decimos que W es un *subespacio $G-$invariante* de V.

Observación 1.3.17 $\{0\}$ y V son llamados los subespacios $G-$invariantes triviales de V.

Proposición 1.3.18 Sean (V, ρ) y (W, ϕ) representaciones de un grupo finito G, si $\theta\colon V \to W$ es un $G-$homomorfismo, entonces $ker\ \theta$ es un subespacio $G-$invariante de V y $Im\ \theta$ es un subespacio $G-$invariante de W.

Demostración.

Como θ es un $G-$homomorfismo tenemos que θ es un transformación lineal de V en W, luego $ker\ \theta$ es un subespacio vectorial de V y $Im\ \theta$ es un subespacio vectorial de W. Sea $v \in ker\ \theta$ y $g \in G$, entonces $\theta(\rho(g)v) = \phi(g)\theta(v) = \phi(g)0_W = 0_W$, así $\rho(g)v \in ker\ \theta$, por consiguiente $ker\ \theta$ es un subespacio $G-$invariante de V. Por otro lado, sea $w \in Im\ \theta$ tenemos que $w = \theta(v)$ para algún $v \in V$, así que $\phi(g)w = \phi(g)\theta(v) = \theta(\rho(g)v)$, como $\rho(g)v \in V$ tenemos que $\phi(g)w \in Im\ \theta$. Por lo tanto, $Im\ \theta$ es un subespacio $G-$invariante de W. ■

Definición 1.3.19 Sea (V, ρ) una representación de un grupo finito G, decimos que (V, ρ) es una representación irreducible de G si V es irreducible, es decir, si V no contiene ningún subespacio W $G-$invariante no trivial. De lo contrario, decimos que (V, ρ) es una representación reducible.

Observación 1.3.20 Para un grupo finito G, tenemos que $\widehat{G}$ denota al conjunto completo de representaciones unitarias irreducibles de G no equivalentes. [60]

Proposición 1.3.21 Sea V una representación irreducible de un grupo finito G y sean $\langle \cdot, \cdot\rangle$, $\langle \cdot, \cdot\rangle'$ dos productos internos $G-$invariantes sobre V. Entonces, para todo $v, w \in V$
$$\langle v, w\rangle' = C\langle v, w\rangle$$
para algún número real positivo C. (c.f [45])

Definición 1.3.22 Sea (V, ρ) una representación de un grupo finito G y W un subespacio $G-$invariante de V, si $\rho_W \colon G \longrightarrow GL(W)$ tal que $\rho_W(g) = \rho(g)|_W$ para cada $g \in G$, decimos que (W, ρ_W) es una *subrepresentación* de (V, ρ).

Observación 1.3.23 Sea (V, ρ) una representación de un grupo finito G y sean W, U subespacios $G-$invariantes de V tales que $V = W \oplus U$. Para cada $v \in V$ tenemos que $v = w + u$ para algunos $w \in W$ y $u \in U$ determinados de forma única. Entonces para cada $g \in G$

$$\rho(g)(v) = \rho(g)(w + u) = \rho(g)(w) + \rho(g)(u) = \rho_W(g)(w) + \rho_U(g)(u)$$

donde $\rho_W = \rho|_W$ y $\rho_U = \rho|_U$. Por lo tanto, ρ es la suma directa de ρ_W y ρ_U y lo denotamos por $\rho = \rho_W \oplus \rho_U$.

Teorema 1.3.24 (Teorema de Maschke) Sea (V, ρ) una representación unitaria de un grupo finito G, con producto interno $\langle \cdot, \cdot \rangle$ $G-$invariante. Entonces existen subespacios $G-$invariantes irreducibles $V_1, \ldots, V_n$ de V tales que V es igual a la suma directa ortogonal $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$. (c.f [45])

Teorema 1.3.25 (Lema de Schur) Sean $(V, \rho), (W, \phi)$ representaciones irreducibles de un grupo G.

1) Si $\theta \colon V \to W$ es un $G-$homomorfismo. Entonces θ es un $G-$isomorfismo o $\theta(v) = 0_W$ para toda $v \in V$.

2) Si $\theta \colon V \to V$ es un $G-$isomorfismo entonces θ es un múltiplo escalar del endomorfismo identidad 1_V.

Demostración.

1) Por la Proposición 1.3.18 $ker\ \theta$ es un subespacio $G-$invariante de V y $Im\ \theta$ es un subespacio $G-$invariante de W. Supongamos que $\theta(v) \neq 0_W$ para algún $v \in V \setminus \{0_V\}$, así que $Im\ \theta \neq \{0_W\}$ entonces $Im\ \theta = W$ ya que (W, ϕ) es una representación irreducible. Además, como (V, ρ) también es irreducible tenemos que $ker\ \theta = \{0_w\}$ o $ker\ \theta = V$ pero $Im\ \theta = W$, luego $ker\ \theta \neq V$, de ahí que $ker\ \theta = \{0_V\}$. Por consiguiente $ker\ \theta = \{0_V\}$ y $Im\ \theta = W$, es decir, θ es biyectiva. Por lo tanto, θ es un isomorfismo.

2) Como θ es un $G-$isomorfismo entonces es un endomorfismo de V que tiene un valor propio $\lambda \in \mathbb{C}$ así que $\theta(v) = \lambda v$ para algún $v \in V \setminus \{0\}$ por lo que $(\theta - \lambda 1_v)(v) = 0$ entonces $ker(\theta - \lambda 1_v) \neq \{0\}$ y por la Proposición 1.3.18 $ker(\theta - \lambda 1_v)$ es un subespacio $G-$invariante de V entonces $ker(\theta - \lambda 1_v) = V$ ya que V es irreducible. Luego para cada $v \in V$ tenemos que $(\theta - \lambda 1_v)(v) = 0$ de ahí que $\theta(v) = \lambda v$ para cada $v \in V$. Por lo tanto, $\theta = \lambda 1_v$.

■

Proposición 1.3.26 Sea (V, ρ) una representación de un grupo finito G y sea $V = U_1 \oplus U_2 \oplus \cdots \oplus U_s$ una suma directa de subespacios $G-$invariantes irreducibles de V. Si W es cualquier subespacio $G-$invariante irreducible de V, entonces $W \cong U_i$ para algún $i \in \{1, \ldots, s\}$.

Demostración.

Sea $w \in W \setminus \{0\}$, como $W \subseteq V$ tenemos que $w \in V$ así que $w = u_1 + \cdots + u_s$ para vectores únicos $u_i \in U_i$ con $i \in \{1, \ldots, s\}$. Definimos la función

$$\begin{aligned} \pi_i \colon W &\longrightarrow U_i \\ w &\longmapsto u_i \end{aligned}$$

para aquellos $i \in \{1, \ldots, n\}$ tales que $u_i \neq 0$, es decir, $\pi_i \neq 0$. Está claro que π_i es una transformación lineal. Probemos que es $G-$invariante. Sea $w \in W$ y $g \in G$, tenemos que para únicos $u_i \in U_i$ con $i \in \{1, \ldots, n\}$, $w = u_1 + u_2 + \cdots + u_n$, entonces

$$\begin{aligned} \pi_i(\rho_W(g)w) = \pi_i(\rho(g)w) &= \pi_i(\rho(g)(u_1 + u_2 + \cdots + u_n)) \\ &= \pi_i(\rho(g)(u_1) + \rho(g)(u_2) + \cdots + \rho(g)(u_n)) = \rho(g)(u_i) \\ &= \rho_{U_i}(g)(u_i) \\ &= \rho_{U_i}(g)(\pi_i(w)). \end{aligned}$$

Por lo tanto, para cada $w \in W$, $\pi_i(\rho_W(g)w) = \rho_{U_i}(g)(\pi_i(w))$. Como W y U_i son irreducibles y además π_i es un $G-$homomorfismo distinto de cero, el Lema de Schur 1.3.25 implica que π_i es un $G-$isomorfismo, de ahí que $W \cong U_i$ para algún $i \in \{1, \ldots, n\}$ ■

Definición 1.3.27 Sea (V, ρ) una representación de un grupo finito G y sea $\mathcal{B}$ una base de V. El *caracter* de (V, ρ) es la función

$$\begin{aligned} \chi : G &\longrightarrow \mathbb{C} \\ g &\longmapsto tr[\rho(g)]_{\mathcal{B}} \end{aligned}$$

donde tr es la función traza matricial.

Lema 1.3.28 El caracter de (V, ρ) no depende de la base $\mathcal{B}$.

Demostración.

Sean $\mathcal{B}$ y $\mathcal{B}'$ bases de V, entonces para alguna matriz invertible T se verifica que, para todo $g \in G$,

$$[\rho(g)]_{\mathcal{B}'} = T^{-1}[\rho(g)]_{\mathcal{B}}T.$$

Como para cada $A \in M(n, \mathbb{C})$, $tr(T^{-1}AT) = trA$, entonces $tr[\rho(g)]_{\mathcal{B}'} = tr[\rho(g)]_{\mathcal{B}}$. ■

Definición 1.3.29 Sea $G = \{g_1, \ldots, g_n\}$ un grupo finito, el *álgebra de grupo* $\mathbb{C}G$ es un espacio vectorial sobre $\mathbb{C}$ de dimensión $|G| = n$, donde sus elementos son de la forma $\lambda_1 g_1 + \lambda_2 g_2 + \cdots + \lambda_n g_n$ con $\lambda_i \in \mathbb{C}$, $i \in \{1, \ldots, n\}$, es decir,

$$\mathbb{C}G = \left\{ \sum_{i=1}^{n} \lambda_i g_i | \lambda_i \in \mathbb{C},\ i \in \{1, \ldots, n\} \right\}.$$

Observación 1.3.30 Como cada $\lambda_i \in \mathbb{C}$, podemos formar una función $f : G \to \mathbb{C}$ tal que $f(g_i) = \lambda_i$, por lo que podemos identificar los elementos de $\mathbb{C}G$ con funciones de $L^2(G)$, es decir, se puede identificar el álgebra de grupo $\mathbb{C}G$ con el espacio $L^2(G)$.

Definición 1.3.31 Sea G un grupo finito, la *representación regular* de G es la pareja $(L^2(G), L)$ donde L se define como

$$\begin{aligned} L : G &\longrightarrow GL(L^2(G)) \\ a &\longmapsto L(a) \end{aligned}$$

donde

$$[L(a)(f)](x) = f(a^{-1}x)$$

para todo $f \in L^2(G)$ y $a, x \in G$. L es conocida como la *representación regular izquierda* de G.

Observación 1.3.32 Algunos textos como [40] manejan a $\mathbb{C}G$ como la representación regular de G.

El siguiente Lema muestra que la representación regular izquierda contiene todas las representaciones unitarias irreducibles dentro de ella.

Lema 1.3.33 (La representación regular izquierda es la madre de todas las representaciones) Sea G un grupo finito con elemento neutro e_G y sea L su representación regular izquierda. Entonces

a) El caracter de L es

$$\chi_L(g) = \begin{cases} |G| & \text{si } g = e_G \\ 0 & \text{en otro caso.} \end{cases}$$

b) Cada representación irreducible $\rho \in \widehat{G}$ esta contenida en L con multiplicidad d_ρ, donde d_ρ es el grado de ρ. Esto es, si $\widehat{G} = \{\rho_1, \ldots \rho_r\}$, entonces L es isomorfo a la suma directa de las copias de todos los ρ_j

$$L \cong d_{\rho_1}\rho_1 \oplus \cdots \oplus d_{\rho_r}\rho_r.$$

c) Si d_ρ es el grado de ρ,

$$\sum_{\rho \in \widehat{G}} d_\rho^2 = |G|.$$

Demostración.

Solo probaremos a). La demostración de b) y c) se encuentran en el Lema 2 de [60].

a) Si $G = \{g_1, g_2, \ldots, g_n\}$, entonces $\mathcal{B} = \{\delta_{g_1}, \ldots, \delta_{g_n}\}$ es una base de $L^2(G)$. Sea $g \in G$

$$[L(g)]_{\mathcal{B}} = \left([L(g)\delta_{g_1}]_{\mathcal{B}} \,\middle|\, [L(g)\delta_{g_2}]_{\mathcal{B}} \,\middle|\, \ldots \,\middle|\, [L(g)\delta_{g_n}]_{\mathcal{B}} \right).$$

Luego, si $x \in G$ para $i \in \{1, \ldots, n\}$ tenemos que

$$\begin{aligned}
[L(g)(\delta_{g_i})](x) = \delta_{g_i}(g^{-1}x) &= \begin{cases} 1 & \text{si } g^{-1}x = g_i, \\ 0 & \text{en otro caso} \end{cases} \\
&= \begin{cases} 1 & \text{si } x = gg_i, \\ 0 & \text{en otro caso} \end{cases} \\
&= \delta_{gg_i}(x)
\end{aligned}$$

De ahí que, para cada $x \in G$, $[L(g)(\delta_{g_i})](x) = \delta_{gg_i}(x)$ y por lo tanto, $L(g)(\delta_{g_i}) = \delta_{gg_i}$ para cada $i \in \{1, \ldots, n\}$. Notemos que $\delta_{gg_i} = \delta_{g_i}$ sí y sólo si $g = e_G$. Entonces la entrada diagonal en la g_i-ésima columna de la matriz $[L(g)]_{\mathcal{B}}$ es distinta de cero si y solo si $\delta_{gg_i} = \delta_{g_i}$ si y solo si $g = e_G$, por consiguiente,

$$\chi_L = tr[L(g)]_{\mathcal{B}} = \sum_{i=1}^{n} \delta_{gg_i}(g_i) = \begin{cases} n & \text{si } g = e_G, \\ 0 & \text{en otro caso.} \end{cases}$$

■

Corolario 1.3.34 Sea G un grupo finito y sea $\widehat{G} = \{V_1 \ldots . V_n\}$ el conjunto de representaciones irreducibles no isomorfas de G donde V_1 es la representación trivial de G, si $d_i = dim(V_i)$, entonces $L_1^2(G) \cong d_2V_2 \oplus \ldots \oplus d_nV_n$.

Demostración.

Sea $\mathbb{C}f_1 = \{\alpha f_1 |\ \alpha \in \mathbb{C}\}$ el conjunto de las funciones constantes de $L^2(G)$ y sea $L_1^2(G) = \{f \in L^2(G) |\ \langle f, f_1\rangle_2 = 0\}$. Probemos que $L_1^2(G) = \mathbb{C}f_1^{\perp}$. Sea $f \in L_1^2(G)$ y $\alpha \in \mathbb{C}$ tenemos que $\langle f, \alpha f_1\rangle_2 = \overline{\alpha}\langle f, f_1\rangle_2 = 0$, por lo que $L_1^2(G) \subseteq \mathbb{C}f_1^{\perp}$. Luego, sea $g \in \mathbb{C}f_1^{\perp}$ tenemos que $\langle g, \alpha f_1\rangle_2 = 0$ para cada $\alpha \in \mathbb{C}$, si $\alpha \neq 0$, se cumple que $0 = \langle g, \alpha f_1\rangle_2 = \overline{\alpha}\langle g, f_1\rangle_2$, es decir,$\langle g, f_1\rangle_2 = 0$, por lo que $\mathbb{C}f_1^{\perp} \subseteq L_1^2(G)$. Entonces $L_1^2(G) = \mathbb{C}f_1^{\perp}$, así que $L^2(G) = \mathbb{C}f_1 \oplus L_1^2(G)$. Sean $f \in \mathbb{C}f_1$ y $g, x \in G$, $[L(g)(f)](x) = f(g^{-1}x) = f(x)$ ya que f es una función constante, entonces a $\mathbb{C}f_1$ le corresponde la representación trivial y es invariante bajo la acción de la representación regular izquierda. Luego por el Lema 1.3.33 b), $L_1^2(G)$ debe descomponerse en las restantes representaciones que están contenidas en $L^2(G)$. ■

1.3.1. Teoría de representaciones de grupos abelianos finitos

Proposición 1.3.35 Si G es un grupo abeliano finito entonces toda representación (V, ρ) irreducible tiene dimensión 1.

Demostración.
Sea $x \in G$, definimos

$$\begin{aligned} \tau_x \colon V &\longrightarrow V \\ v &\longmapsto \rho(x)v. \end{aligned}$$

Probemos que τ_x es un $G-$homomorfismo. Recordemos que ρ induce una acción sobre V que satisface las propiedades ya enunciadas en la Observación 1.3.4 las cuales serán utilizadas en la prueba. Sean $u, v \in V$, $g \in G$ y $\alpha \in \mathbb{C}$ tenemos que

$$\tau_x(\rho(g)v) = \rho(x)\rho(g)v = \rho(x+g)v = \rho(g+x)v = \rho(g)\rho(x)v = \rho(g)\tau_x(v)$$

y

$$\tau_x(\alpha u+v) = \rho(x)(\alpha u+v) = \rho(x)(\alpha u)+\rho(x)v = \alpha(\rho(x)(u))+\rho(x)v = \alpha\tau_x(u)+\tau_x(v),$$

es decir, $\tau_x(\rho(g)v) = \rho(g)\tau_x(v)$ para cada $v \in V$ y para cada $g \in G$ y $\tau_x(\alpha u + v) = \alpha\tau_x(u) + \tau_x(v)$ para cada $u, v \in V$ y para cada $\alpha \in \mathbb{C}$. Así que τ_x es un transformación lineal $G-$invariante, por lo tanto, τ_x es un $G-$homomorfismo. Dado que G es un grupo abeliano existe $-x \in G$ tal que $x + (-x) = e_G$, entonces para cada $v \in V$,

$$\tau_x \circ \tau_{-x}(v) = \tau_x(\tau_{-x}(v)) = \tau_x(\rho(-x)(v)) = \rho(x)\rho(-x)v = \rho(e_G)v = v = Id(v)$$

y

$$\tau_{-x} \circ \tau_x(v) = \tau_{-x}(\tau_x(v)) = \tau_{-x}(\rho(x)(v)) = \rho(-x)\rho(x)v = \rho(e_G)v = v = Id(v),$$

es decir, $\tau_x \circ \tau_{-x}(v) = Id(v) = \tau_{-x} \circ \tau_x(v)$, así que τ_x es invertible para cada $x \in G$ y por consiguiente τ_x es $G-$isomorfismo. Luego, por el Lema de Schur 1.3.25 tenemos que $\tau_x = \lambda_x 1_V$ para algún $\lambda_x \in \mathbb{C}$, así que $\rho(x)v = \lambda_x v$ para cada $v \in V$.

Sea U un subespacio de V con $U \neq \{0\}$, como para cada $g \in G$ y $u \in U$ $\rho(g)u = \lambda_g u \in U$, es decir, $\rho(g)u \in U$ tenemos que U es un subespacio $G-$invariante de V, pero V es irreducible así que $V = U$, dado que $U \neq \{0\}$ existe $u_0 \in U$, luego $span\{u_0\}$ es un subespacio de U, más aún como $\rho(g)\lambda u_0 = \lambda_g \lambda u_0 \in span\{u_0\}$ para cada $\lambda u_0 \in span\{u_0\}$ y $g \in G$ tenemos que $span\{u_0\}$ es un subespacio $G-$invariante de V, así que $span\{u_0\} = U = V$ por ser V irreducible. Por lo tanto, V tiene dimensión 1. ■

Proposición 1.3.36 Sea $m \in \mathbb{Z}$ con $m \geq 2$. Entonces el conjunto de las representaciones irreducibles de $\mathbb{Z}/m\mathbb{Z}$ es

$$\{\phi_a | a \in \{0, 1, \ldots, m-1\}\}$$

donde

$$\begin{aligned} \phi_a \colon \mathbb{Z}/m\mathbb{Z} &\longrightarrow GL(1, \mathbb{C}) \\ \overline{k} &\longmapsto [\exp(\tfrac{2\pi i a k}{m})]. \end{aligned}$$

Demostración.

Sea $\phi \colon \mathbb{Z}/m\mathbb{Z} \to GL(n, \mathbb{C})$ una representación matricial irreducible de $\mathbb{Z}/m\mathbb{Z}$, por la Proposición 1.3.35 $n = 1$, entonces para $\overline{1} \in \mathbb{Z}/m\mathbb{Z}$ existe $\lambda_{\overline{1}} \in \mathbb{C}$ tal que $\phi(\overline{1}) = \lambda_{\overline{1}}$. Como $\overline{1}$ tiene orden m tenemos que

$$[1] = \phi\left(m\overline{1}\right) = \phi\left(\overline{1}\right)^m = [\lambda_{\overline{1}}]^m = [\lambda_{\overline{1}}^m],$$

es decir, $\lambda_{\overline{1}}^m = 1$, así que $\lambda_{\overline{1}}$ es una raíz $m-$ésima de la unidad por consiguiente existe $a \in \{0, 1, \ldots, n-1\}$ tal que $\lambda_{\overline{1}} = \exp(\frac{2\pi i a}{m})$, así que $\phi(\overline{1}) = \exp(\frac{2\pi i a}{m})$ con $a \in \{0, 1, \ldots, m-1\}$. Sea $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$ tenemos que

$$\phi(\overline{k}) = \phi(k\overline{1}) = \phi(\overline{1})^k = (\exp(\tfrac{2\pi i a}{m}))^k = \exp(\tfrac{2\pi i a k}{m}),$$

es decir, $\phi(\overline{k}) = \exp(\frac{2\pi i a k}{m})$. Notemos que ϕ no depende de la elección del representante ya que si $k_1, k_2 \in \mathbb{Z}$ tales que $k_1 \equiv k_2 \mod m$ tenemos que $k_1 = k_2 + ml$ para algún $l \in \mathbb{Z}$. Entonces

$$\begin{aligned} \phi(\overline{k_1}) = \exp(\tfrac{2\pi i a k_1}{m}) = \exp(\tfrac{2\pi i a (k_2 + ml)}{m}) &= \exp(\tfrac{2\pi i a k_2}{m}) \exp(2\pi i a l) \\ &= \exp(\tfrac{2\pi i a k_2}{m}) \\ &= \phi(\overline{k_2}). \end{aligned}$$

Por lo tanto, ϕ es una representación irreducible de grado 1 donde $\phi(\overline{k}) = \exp(\frac{2\pi i a k}{m})$.

Recíprocamente, cualquier función de la forma

$$\begin{aligned} \phi_a \colon \mathbb{Z}/m\mathbb{Z} &\longrightarrow GL(1, \mathbb{C}) \\ \overline{k} &\longmapsto [\exp(\tfrac{2\pi i a k}{m})] \end{aligned}$$

con $a \in \{0, 1, \ldots, m-1\}$, es una representación matricial de $\mathbb{Z}/m\mathbb{Z}$ ya que para cada $\overline{k}_1, \overline{k}_2 \in \mathbb{Z}/m\mathbb{Z}$ tenemos que

$$\phi_a(\overline{k}_1 + \overline{k}_2) = [\exp(\tfrac{2\pi i a (k_1 + k_2)}{m})] = [\exp(\tfrac{2\pi i a k_1}{m})][\exp(\tfrac{2\pi i a k_2}{m})] = \phi_a(\overline{k}_1)\phi_a(\overline{k}_2).$$

Por último, veamos que las representaciones no son equivalentes. Sean $a, b \in \{0, 1, \ldots, m-1\}$ supongamos que $\phi_a \cong \phi_b$ entonces existe $\alpha \in \mathbb{C} \setminus \{0\}$ tal que para cada $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$

$$[\alpha]\phi_a(\overline{k})[\alpha]^{-1} = \phi_b(\overline{k}),$$

como el producto en $\mathbb{C}$ es conmutativo tenemos que $\phi_a(\overline{k}) = \phi_b(\overline{k})$ entonces $\exp(\frac{2\pi iak}{m}) = \exp(\frac{2\pi ibk}{m})$ de ahí que $a = b$. Entonces si $\phi_a \cong \phi_b$ se cumple que $a = b$ con $a, b \in \{0, 1, \ldots, m-1\}$. Por lo tanto, el conjunto de todas las representaciones irreducibles de $\mathbb{Z}/m\mathbb{Z}$ es $\{\phi_a | a \in \{0, 1, \ldots, m-1\}\}$.

■

Corolario 1.3.37 Sea $a \in \{0, \ldots, m-1\}$ y sea $\rho_a \colon \mathbb{Z}/m\mathbb{Z} \to GL(\mathbb{C})$ dada por $\rho_a(\overline{k})z = \exp(\frac{2\pi iak}{m})z$ para cada $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$ y $z \in \mathbb{C}$, entonces $\rho_0, \rho_1, \ldots \rho_{m-1}$ son todas la representaciones irreducibles de $\mathbb{Z}/m\mathbb{Z}$.

Recordemos que el Teorema Fundamental de los Grupos Abelianos Finitos nos dice que un grupo abeliano finito es el producto directo de grupos cíclicos y como todo grupo cíclico es isomorfo a algún grupo de la forma $\mathbb{Z}/m\mathbb{Z}$ entonces un grupo abeliano finito es isomorfo a un producto de la forma $\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$, así que si encontramos las representaciones de grupos de la forma $\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ obtendremos las representaciones de cualquier grupo abeliano finito.

Proposición 1.3.38 Sea G un grupo abeliano finito que está dado por $\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$. Entonces el conjunto de las representaciones matriciales irreducibles de G es

$$\{\phi_a | a = (a_1, a_2, \ldots, a_r)\}$$

donde

$$\begin{aligned}\phi_a(\overline{g_1}, \ldots, \overline{g_r}) &= \left[\exp(\tfrac{2\pi ia_1g_1}{m_1}) \ \exp(\tfrac{2\pi ia_2g_2}{m_2}) \ \ldots \ \exp(\tfrac{2\pi ia_rg_r}{m_r})\right] \\ &= [\exp(i\theta)]\end{aligned}$$

con $\theta = \frac{2\pi a_1g_1}{m_1} + \frac{2\pi a_2g_2}{m_2} + \cdots + \frac{2\pi a_rg_r}{m_r}$.

Demostración.

Sea $\phi \colon G \to GL(n, \mathbb{C})$ una representación matricial irreducible de G, por la Proposición 1.3.35 $n = 1$. Sea $e_j = (0, \ldots, 0, \overline{1}, 0, \ldots, 0)$ donde $\overline{1}$ está en la $j-$ésima posición con $j \in \{1, \ldots, r\}$. Como todo elemento de G se puede escribir como una combinación lineal de los e_j tenemos que ϕ estará determinada por los valores que tome en cada e_j, luego para cada e_j existe $\lambda_j \in \mathbb{C}$ tal que $\phi(e_j) = [\lambda_j]$ y como e_j tiene orden m_j tenemos que λ_j es una raíz m_j-ésima de la unidad, es decir, $\phi(e_j) = [\exp(\frac{2\pi ia_j}{m_j})]$ con $a_j \in \{0, 1, \ldots, m_j - 1\}$ para cada $j \in \{1, \ldots, r\}$. Entonces si nos tomamos a $g = (\overline{g_1}, \ldots, \overline{g_r}) \in G$ tenemos que

$$\begin{aligned}\phi(\ (\overline{g_1}, \ldots, \overline{g_r})\ ) = \phi(\ g_1e_1 + \cdots + g_re_r\ ) &= \phi(g_1e_1) \ldots \phi(g_re_r) \\ &= \phi(e_1)^{g_1} \ldots \phi(e_r)^{g_r} \\ &= [\exp(\tfrac{2\pi ia_1}{m_1})]^{g_1} \ldots [\exp(\tfrac{2\pi ia_r}{m_r})]^{g_r} \\ &= [\exp(\tfrac{2\pi ia_1g_1}{m_1}) \ldots \exp(\tfrac{2\pi ia_rg_r}{m_r})].\end{aligned}$$

El que ϕ no dependa del representante se sigue de la misma forma que en la demostración de 1.3.36.

Recíprocamente cualquier función de la forma

$$\begin{aligned}\phi_a\colon G &\longrightarrow GL(1,\mathbb{C})\\ \overline{k} &\longmapsto [\exp(\tfrac{2\pi i a_1 g_1}{m_1})\dots\exp(\tfrac{2\pi i a_r g_r}{m_r})]\end{aligned}$$

con $a=(a_1,a_2,\dots,a_r)$ donde $a_j\in\{0,1,\dots,m_j-1\}$ para cada $j\in\{1,\dots,r\}$, es una representación matricial de G ya que para cada $(g_1,g_2,\dots,g_r),(h_1,h_2,\dots,h_r)\in G$ tenemos que

$$\begin{aligned}&\phi_a((g_1,g_2,\dots,g_r)+(h_1,h_2,\dots,h_r))\\ &=\phi_a((g_1+h_1,\dots,g_r+h_r))\\ &=[\exp(\tfrac{2\pi i a_1(g_1+h_1)}{m_1})\dots\exp(\tfrac{2\pi i a_r(g_r+h_r)}{m_r})]\\ &=[\exp(\tfrac{2\pi i a_1 g_1}{m_1})\dots\exp(\tfrac{2\pi i a_r g_r}{m_r})][\exp(\tfrac{2\pi i a_1 h_1}{m_1})\dots\exp(\tfrac{2\pi i a_r g_r}{m_r})]\\ &=\phi_a((g_1,g_2,\dots,g_r))\phi_a((h_1,h_2,\dots,h_r)).\end{aligned}$$

Por último, el que las representaciones no sean equivalentes se sigue de manera similar a lo realizado en la demostración de 1.3.36.

■

Corolario 1.3.39 Sea G un grupo abeliano finito que esta dado por $\frac{\mathbb{Z}}{m_1\mathbb{Z}}\times\frac{\mathbb{Z}}{m_2\mathbb{Z}}\times\dots\times\frac{\mathbb{Z}}{m_r\mathbb{Z}}$. Entonces el conjunto de las representaciones irreducibles de G es

$$\{\rho_a\colon G\mapsto GL(\mathbb{C})|a=(a_1,a_2,\dots,a_r)\}$$

donde

$$\rho_a(\overline{g_1},\dots,\overline{g_r})z=\exp(i\theta)z$$

con $\theta=\frac{2\pi a_1 g_1}{m_1}+\frac{2\pi a_2 g_2}{m_2}+\dots+\frac{2\pi a_r g_r}{m_r}$, para cada $(\overline{g_1},\dots,\overline{g_r})\in G$ y $z\in\mathbb{C}$.

Capítulo 2
Familias de grafos expanders

Las familias de grafos expanders son sucesiones de grafos regulares con la característica de que al tomar un subconjunto de vértices, no muy grande, este tiene muchos vecinos distintos. Está característica de conectividad puede ser medida mediante distintas constantes.

En este capítulo abordaremos la definición de una familia de grafos expander mediante la constante isoperimétrica, la constante de expansión de vértices, la brecha espectral, la constante de expansión espectral y la constante de Kazhdan.

2.1. Constante isoperimétrica

Definición 2.1.1 Sea $X = (V, E)$ un grafo y $F \subset V$, la *frontera de aristas* de F, denotada por $E(F, V \setminus F)$, es el conjunto de aristas que tienen un extremo en F y otro extremo en $V \setminus F$.

Ejemplo 2.1.2 En el grafo de la Figura 2.1, el conjunto F consiste en todos los vértices blancos y su frontera de aristas son todas las lineas punteadas. Ahora si analizamos el complemento de F, es decir, los vértices negros, tenemos que los elementos de su frontera de aristas vuelven a ser las líneas punteadas. En otra palabras tenemos que $E(F, V \setminus F) = E(V \setminus F, F)$.

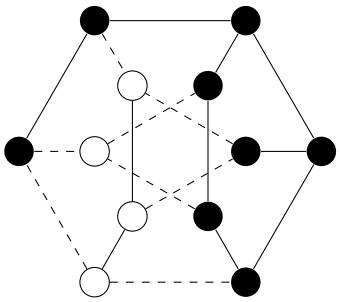


Figura 2.1

Definición 2.1.3 Sea $X = (V, E)$ un grafo, la *constante isoperimétrica* de X se define como:

$$h(X) = \text{mín}\left\{\frac{|E\ (F,\ V \setminus F)|}{|F|} : F \subset V \text{ y } |F| \leq \frac{|V|}{2}\right\}.$$

Observaciones 2.1.4

- Sea $F \subset V$ con $|F| \leq 2$ tenemos que $|E(F, V \setminus F)| \geq h(X)|F|$, es decir, el tamaño de la frontera de aristas de F es al menos $h(X)$ veces el tamaño de F. Entonces cuando $h(X)$ es grande, cada conjunto F con no más de la mitad de los vértices de X tendrá muchos vecinos distintos en relación con su tamaño.
- En el Ejemplo 2.1.2, vimos que $E(F, V \setminus F) = E(V \setminus F, F)$ para cada $F \subset V$, entonces la definición de la constante isoperimétrica puede darse en términos más generales

$$h(X) = \text{mín}\left\{\frac{|E(F, V \setminus F)|}{\text{mín}\{|F|, |V \setminus F|\}} : F \subset V\right\}.$$

- La constante isoperimétrica también es conocida como constante de expansión de aristas, conductancia o constante de Cheeger (este último particularmente cuando se enfatizan las conexiones geométricas). [45]

Ejemplo 2.1.5 Consideremos el grafo ciclo C^4, si $F \subset V$ tal que $|F| \leq \frac{|V|}{2}$, entonces $|F| = 1$ o $|F| = 2$.

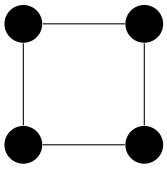
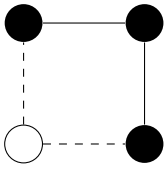
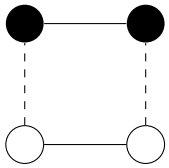


Figura 2.2: C^4.

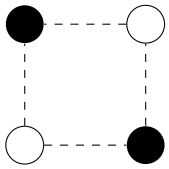
Si F consta de un sólo vértice, entonces $|E(F, V \setminus F)| = 2$ y $\dfrac{|E(F, V \setminus F)|}{|F|} = 2$.



Si F consta de dos vértices que son adyacentes mediante una arista, tenemos que $|E(F, V \setminus F)| = 2$ y $\dfrac{|E(F, V \setminus F)|}{|F|} = 1$.



Por último, si F consta de dos vértices que no son adyacentes, se sigue que $|E(F, V \setminus F)| = 4$ y $\dfrac{|E(F, V \setminus F)|}{|F|} = 2$.



Entonces el mínimo valor que puede tomar $\frac{|E(F,V\setminus F)|}{|F|}$ es 1. Por lo tanto, $h(C^4) = 1$.

Ejemplo 2.1.6 Analizaremos la constante isoperimétrica de los grafos completos. Sea F un subconjunto de vértices con no más de la mitad de vértices del grafo. Para K^3, F solo puede tener un elemento, entonces $\frac{|E(F,V\setminus F)|}{|F|} = |E(F, V \setminus F)| = 2$. Por lo tanto, $h(K^3) = 2$.

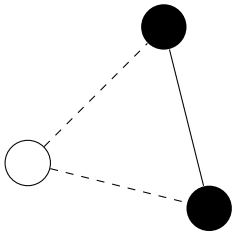
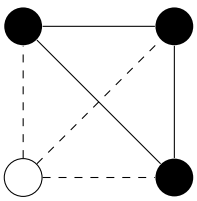
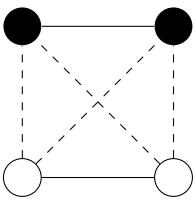


Figura 2.3: K^3.

Para K^4, F puede tener uno o dos vértices, pero a diferencia de C^4, en K^4 estos dos vértices siempre son adyacentes, así que $\frac{|E(F,V\setminus F)|}{|F|}$ es 3 o 2, como se muestra en la Figura 2.4. Por lo tanto, $h(K^4) = 2$.



(a) $\frac{|E(F,V\setminus F)|}{|F|} = 3$



(b) $\frac{|E(F,V\setminus F)|}{|F|} = 2$

Figura 2.4: K^4.

Ahora pasemos al caso general. Sea K^n un grafo completo con conjunto de vértices V. Si $F \subset V$ con no más de la mitad de vértices de V, entonces $|F| \leq \frac{n}{2}$ si n es par, pero si n es impar F puede tener a lo más $\frac{n-1}{2}$ vértices.

Luego

$$\frac{|E(F, V \setminus F)|}{|F|} = \frac{|V \setminus F|\,|F|}{|F|} = |V \setminus F| = n - |F|.$$

Si n es par

$$\frac{|E(F, V \setminus F)|}{|F|} = n - |F| \geq n - \frac{n}{2} = \frac{n}{2}.$$

Pero, si n es impar

$$\frac{|E(F, V \setminus F)|}{|F|} = n - |F| \geq n - \left(\frac{n-1}{2}\right) = \frac{n+1}{2},$$

es decir, para cada $F \subset V$ con no más de la mitad de vértices, tenemos que

$$\frac{|E(F, V \setminus F)|}{|F|} \geq \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ \frac{n+1}{2} & \text{si } n \text{ es impar.} \end{cases}$$

Por lo tanto,

$$h(K^n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ \frac{n+1}{2} & \text{si } n \text{ es impar.} \end{cases}$$

En el caso de grafos regulares, es posible acotar el valor de su constante isoperimétrica.

Proposición 2.1.7 Sea $X = (V, E)$ un grafo $d-$regular, entonces $0 \leq h(X) \leq d$.

Demostración.

Por definición $h(X)$ es el mínimo del cociente de dos cardinalidades, por lo que $h(X) \geq 0$. Luego, sea $v \in V$ tenemos que $|E(\{v\}, V \setminus \{v\})| = |E_X(v)| = d$, ya que X es un grafo $d-$regular entonces $h(X) \leq \frac{|E(\{v\}, V \setminus \{v\})|}{|\{v\}|} = d$. ■

Proposición 2.1.8 Sea $X = (V, E)$ un grafo, $h(X) = 0$ si y solo si X es un grafo no conexo.

Demostración.

Si $h(X) = 0$ entonces existe $F_0 \subset V$ con $|F_0| \leq \frac{|V|}{2}$ tal que $\frac{|E(F_0, V \setminus F_0)|}{|F_0|} = 0$ por lo que $|E(F_0, V \setminus F_0)| = 0$ así que para los vértices de F_0 no existen aristas que los unan con los vértices de $V \setminus F_0$, por lo tanto, X es un grafo no conexo. Recíprocamente, si X es un grafo no conexo, entonces existen $v_1, v_2 \in V$ tales que ningún camino los conecta. Sea $F = \{v \in V : v_1 \text{ y } v \text{ son los extremos de algún camino}\}$. Si $F = \emptyset$, entonces v_1 es un vértice aislado, por lo tanto, $E(\{v_1\}, V \setminus \{v_1\}) = \emptyset$, así que

$$0 = \frac{|E(\{v_1\}, V \setminus \{v_1\})|}{|\{v_1\}|} \geq h(X),$$

es decir, $0 \geq h(X)$. Ahora si $F \neq \emptyset$, supongamos que $E(F, V \setminus F) \neq \emptyset$. Sea $e \in E(F, V \setminus F)$, tenemos que existen $u \in F$ y $w \in V \setminus F$ tales que $e = \{u, w\}$, como $u \in F$ existe un camino P con extremos v_1 y u, entonces $P + e$ es un camino que une a v_1 con w, por consiguiente $w \in F$ pero esto contradice el hecho de que $w \in V \setminus F$, por consiguiente $E(F, V \setminus F) = \emptyset$. Entonces

$$0 = \frac{|E(F, V \setminus F)|}{\text{mín}\{|F|, |V \setminus F|\}} \geq h(X),$$

es decir, $0 \geq h(X)$ y por la Proposición 2.1.7. $0 \leq h(X)$. Entonces, $h(X) = 0$. ■

En una familia de grafos expanders debemos de procurar que a medida de que los vértices crezcan, las constantes isoperimétricas no se acerquen a cero ya que esto nos indicaría que los grafos son no conexos, para evitar esto pediremos que las constantes de expansión estén acotadas lejos de cero.

Definición 2.1.9 Sea (a_n) una sucesión de números reales distintos de cero, decimos que (a_n) está acotada lejos de cero si existe $\varepsilon > 0$ tal que para todo $n \in \mathbb{N}$, $a_n \geq \varepsilon$.

Definición 2.1.10 Sea (X_n) una sucesión de grafos $d-$regulares tal que $|X_n| \to \infty$ cuando $n \to \infty$. Decimos que (X_n) es una familia de grafos expanders, si la sucesión $h((X_n))$ está acotada lejos de cero.

2.2. Constante de expansión de vértices

La constante de expansión de vértices como su nombre lo dice, es una constante que nos permitirá conocer la conectividad de un grafo mediante el estudio de los vértices conectados a un subconjunto de vértices, esta constante da paso a la definición más popular de grafo expander.

Definición 2.2.1 Sea $X = (V, E)$ un grafo $d-$regular con $|V| = n$ y $c > 0$. X es un $(n, d, c)-$expander si para cada $A \subset V$ con $|A| \leq \frac{n}{2}$ se cumple que

$$|\partial(A)| \geq c\left(1 - \frac{|A|}{n}\right)|A|$$

donde ∂A es el conjunto de vértices en $V \setminus A$ que son adyacentes a algún vértice de A, ∂A se suele llamar la *frontera de vértices* de A y la constante c es llamada la *constante de expansión de vértices* .

Observación 2.2.2 La constante de expansión de vértices c de un grafo $X = (V, E)$ se puede ver como

$$c = \text{mín}\left\{\frac{|\partial A|}{|A|\left(1 - \frac{|A|}{|V|}\right)} : A \subset V \text{ y } |A| \leq \frac{|V|}{2}\right\}.$$

En la sección anterior estudiamos la frontera de aristas y aquí definimos la frontera de vértices, si bien ambas nos dan información sobre los vecinos de un subconjunto de vértices, no necesariamente tienen la misma cantidad de elementos.

Lema 2.2.3 Sea $X = (V, E)$ un grafo y $A \subset V$ con $A \neq \emptyset$. Entonces $|\partial A| \leq |E(A, V \setminus A)|$.

Demostración.

Si no existen vértices en $V \setminus A$ que estén conectados mediante una arista con algún vértice de A, tenemos que $E(A, V \setminus A) = \emptyset$ y $\partial A = \emptyset$. Por lo tanto, se satisface que $|\partial A| \leq |E(A, V \setminus A)|$. Supongamos que existen vértices de $V \setminus A$ que están conectados mediante una arista a algún vértice de A. Sea

$$\begin{aligned} f \colon E(A, V \setminus A) &\longrightarrow \partial A \\ \{a, v\} &\longmapsto v. \end{aligned}$$

Dado que para cada $v \in \partial A$, existe algún $a \in A$ tal que $\{a, v\} \in E$, tenemos que $\{a, v\} \in E(A, V \setminus A)$ tal que $f(\{a, v\}) = v$, así que f es sobreyectiva. Por lo tanto, $|\partial A| \leq |E(A, V \setminus A)|$. ■

Observación 2.2.4 En el lema anterior f no necesariamente es inyectiva ya que dos vértices en A puede que sean adyacentes a un mismo vértice en el complemento de A, como se muestra en la Figura 2.5, en donde $\{a_1, v\} \neq \{a_2, v\}$.

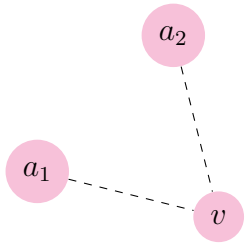


Figura 2.5

.

Proposición 2.2.5 Sea $X = (V, E)$ un grafo $d-$regular con n vértices, se cumple lo siguiente:

a) Si X es un $(n, d, c)-$expander, entonces $h(X) \geq \frac{c}{2}$.

b) X es un $\left(n, d, \frac{h(X)}{d}\right)-$expander.

Demostración.

a) Si X es un $(n, d, c)-$expander, entonces para cada $A \subset V$ con $|A| \leq \frac{n}{2}$ se cumple que

$$|\partial A| \geq c\left(1 - \frac{|A|}{n}\right)|A| = c\left(\frac{|V - A|}{n}\right)|A|.$$

Así que

$$c \leq \frac{|\partial A| n}{|A||V - A|},$$

como $|V - A| \geq \frac{n}{2}$

$$c \leq \frac{|\partial A| n}{|A|}\frac{2}{n},$$

entonces

$$\frac{c}{2} \leq \frac{|\partial A|}{|A|},$$

por el Lema 2.2.3 $|\partial A| \leq |E(A, V \setminus A)|$, así que $\frac{c}{2} \leq \frac{|E(A,V\setminus A)|}{|A|}$. Entonces por la Definición 2.1.3 de la constante isoperimétrica se cumple que $h(X) \geq \frac{c}{2}$.

b) Para cada $A \subset V$ con $|A| \leq \frac{n}{2}$ tenemos que

$$h(X) \leq \frac{|E(A, V \setminus A)|}{|A|} = \frac{|E(A, V \setminus A)||V - A|}{|A||V - A|} \leq \frac{|E(A, V \setminus A)|n}{|A||V - A|}.$$

Dado que X es un grafo $d-$regular, para cada vértice $v \in \partial A$ hay d aristas incidentes en v, pero puede que no todas estas aristas tengan como punto final un vértice de A, así que puede haber a lo más d aristas de la forma $\{a, v\}$ en $E(A, V \setminus A)$. Entonces $|E(A, V \setminus A)| \leq d|\partial A|$, así que

$$h(X) \leq \frac{d|\partial A|n}{|A||V - A|}.$$

Por consiguiente,

$$\begin{aligned} |\partial A| &\geq \frac{h(X)}{d}\left(\frac{|A||V - A|}{n}\right) \\ &= \frac{h(X)}{d}\left(\frac{|A|(n - |A|)}{n}\right) \\ &= \frac{h(X)}{d}\left(1 - \frac{|A|}{n}\right)|A|, \end{aligned}$$

es decir, para cada $A \subset V$ con $|A| \leq \frac{n}{2}$ se cumple que

$$|\partial A| \geq \frac{h(X)}{d}\left(1 - \frac{|A|}{n}\right)|A|.$$

Por lo tanto, X es un $\left(n, d, \frac{h(X)}{d}\right)-$expander.

■

Observación 2.2.6 En la Definición 2.2.1 tenemos que si $A \subset V$ tal que $|A| \leq \frac{n}{2}$, entonces $1 - \frac{|A|}{n} \geq \frac{1}{2}$, por lo que $\varepsilon = \frac{c}{2}$ es una constante de expansión de vértices más compacta para nuestra definición, como se muestra a continuación.

Definición 2.2.7 Sea X un grafo $d-$regular con n vértices y $\varepsilon > 0$, decimos que X es un $\varepsilon-$expander si para cada $A \subset V$ con $|A| \leq \frac{|V|}{2}$ se cumple que

$$|\partial A| \geq \varepsilon |A|.$$

Proposición 2.2.8 Sea $X = (V, E)$ un grafo $d-$regular con n vértices. Entonces se cumple lo siguiente:

a) Si X es un $\varepsilon-$expander, entonces $h(X) \geq \varepsilon$.

b) X es un $\left(\frac{h(X)}{d}\right)$–expander.

Demostración.
Se sigue de la Proposición 2.2.5. ■

Ahora que establecimos relaciones entre la constante de expansión de vértices y la constante isoperimétrica, podemos definir las familias de grafos expanders mediante la constante de expansión de vértices.

Teorema 2.2.9 Si (X_n) es una sucesión de grafos $d-$regulares tal que $|X_n| \to \infty$ si $n \to \infty$, entonces (X_n) es una familia de grafos expanders si y solo si existe $\varepsilon > 0$ tal que para cada $n \in \mathbb{N}$, X_n es un $\varepsilon-$expander.

Demostración.
Si (X_n) es una familia de grafos expander, entonces existe $\varepsilon_1 > 0$ tal que para cada $n \in \mathbb{N}$ se cumple que $h(X_n) \geq \varepsilon_1$. Por la Proposición 2.2.8 tenemos que para cada $n \in \mathbb{N}$, X_n es un $\left(\frac{h(X_n)}{d}\right)$–expander, entonces para cada $A_n \subset V_n$ con $|A_n| \leq \frac{|V_n|}{2}$, se cumple que

$$|\partial A_n| \geq \frac{h(X_n)}{d}|A_n| \geq \frac{\varepsilon_1}{d}|A_n|.$$

Sea $\varepsilon = \frac{\varepsilon_1}{d}$ tenemos que para cada $n \in \mathbb{N}$, X_n es un $\varepsilon-$expander. Ahora, si existe $\varepsilon > 0$ tal que para cada $n \in \mathbb{N}$, X_n es un $\varepsilon-$expander. Por la Proposición 2.2.8 tenemos que $h(X_n) \geq \varepsilon$, entonces $(h(X_n))$ es una sucesión acotada lejos de cero. Por lo tanto, (X_n) es una familia de grafos expanders. ■

2.2.1. Grafos biexpanders

Definición 2.2.10 Sea $X = (V^- \cup V^+, E)$ un grafo bipartito $d-$regular donde los aristas van de V^- a V^+ y $|V^-| = |V^+| = n$. Sea $c > 0$ decimos que X es un $(n, d, c)-$biexpander si para cada $A \subset V^-$ con $|A| \leq \frac{n}{2}$ se cumple que

$$|\partial A| \geq \left[1 + c\left(1 - \frac{|A|}{n}\right)\right]|A|.$$

Observación 2.2.11 Los primeros grafos expanders construidos fueron mediante grafos bipartitos, es por ello que en algunos textos se considera grafos expanders cuando se trabaja con bipartitos y cuando se trabaja con grafos no bipartitos reciben el nombre de *magnificadores*. Nosotros consideraremos grafos expanders cuando trabajemos con grafos no bipartitos y cuando usemos grafos bipartitos los llamaremos grafos biexpanders.

Notemos que la definición 2.2.10 de biexpanders es muy similar a la definición 2.2.1 de grafo expander, de hecho es posible pasar de un grafo expander a un biexpander utilizando la doble cubierta extendida (ver Definición 1.2.29).

Proposición 2.2.12 Sea $X = (V, E)$ un grafo $(n, d, c)-$expander, entonces su doble cubierta extendida es un grafo $(n, d+1, c)-$biexpander.

Demostración.

Sea $V = \{v_1, \ldots, v_n\}$ el conjunto de vértices de X y sea Y la cubierta doble extendida de X, tenemos que Y es un grafo bipartito con conjunto de vértices $V^- \cup V^+$ donde V^- y V^+ son copias de V en el que v_i^- y v_j^+ son adyacentes si y solo si $i = j$ o $\{v_i, v_j\} \in E$, de ahí que Y es un grafo $(d+1)-$regular. Sea $A^- \subset V^-$ con $A^- \leq \frac{n}{2}$, recordemos que A^- es copia de algún $A \subset V$, entonces

$$\begin{aligned}
|\partial A^-| = |A| + |\partial A| &\geq |A| + c\left(1 - \frac{|A|}{n}\right)|A| \\
&= \left[1 + c\left(1 - \frac{|A|}{n}\right)\right]|A| \\
&= \left[1 + c\left(1 - \frac{|A^-|}{n}\right)\right]|A^-|,
\end{aligned}$$

es decir, $|\partial A^-| \geq \left[1 + c\left(1 - \frac{|A^-|}{n}\right)\right]|A^-|$. Entonces $Y = (V^- \cup V^+,\ E)$ es un grafo bipartito $(d+1)-$regular con $|V^-| = |V^+| = n$, donde para cada $A^- \subset V^-$ con $A^- \leq \frac{n}{2}$ se cumple que

$$|\partial A^-| \geq \left[1 + c\left(1 - \frac{|A^-|}{n}\right)\right]|A^-|.$$

Por lo tanto, Y es $(n, d+1, c)-$biexpander.

■

Observación 2.2.13 De manera similar a la Observación 2.2.6, si consideramos $\varepsilon = \frac{c}{2}$ tenemos la siguiente definición de grafo biexpander.

Definición 2.2.14 Sea $X = (V^- \cup V^+, E)$ un grafo bipartito $d-$regular donde las aristas van de V^- a V^+y $|V^-| = |V^+| = n$. Sea $\varepsilon > 0$ decimos que X es un $\varepsilon-$biexpander si para cada $A \subset V^-$ con $|A| \leq \frac{n}{2}$ tenemos que

$$|\partial A| \geq (1+\varepsilon)|A|.$$

En el caso de que X sea un grafo bipartito cuyas particiones tengan distintas cardinalidades, existe una definición de grafo biexpander.

Definición 2.2.15 Sea $X = (V^- \cup V^+, E)$ un grafo bipartito $(d_{V^-}, d_{V^+})-$regular donde los aristas van de V^- a V^+ y $|V^-| = m$ $|V^+| = n$ con $m > n$. Sea $\varepsilon > 0$ decimos que X es un $(m, n, d_{V^-}, d_{V^+}, \varepsilon)$-biexpander si para cada $A \subset V^-$ con $|A| \leq \frac{m}{2}$ se cumple que

$$|\partial A| \geq \varepsilon|A|.$$

2.3. Brecha espectral

La brecha espectral es una constante que relaciona la regularidad del grafo con su segundo valor propio más grande en valor absoluto. En esta sección estudiaremos la conexión que existe entre la brecha espectral y la constante isoperimétrica, para ello haremos uso del Laplaciano discreto y el Teorema Rayleigh- Ritz.

2.3.1. Laplaciano discreto

Sea $X = (V, E)$ un grafo, le asignaremos una orientación al conjunto de aristas del grafo, es decir, para cada $e \in E$ etiquetaremos los vértices a los que une como e^- el inicio de e y e^+ el final de e.

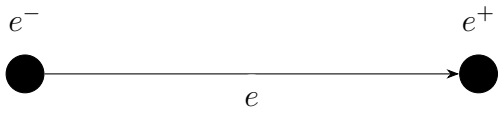


Figura 2.6

Definición 2.3.1 Sea $X = (V, E)$ un grafo, el *gradiente* de X es la función $\mathcal{D}\colon L^2(V) \to L^2(E)$ definida para cada $f \in L^2(V)$ como

$$(\mathcal{D}(f))(e) = f(e^+) - f(e^-).$$

$(\mathcal{D}(f))(e)$ mide el cambio de f a lo largo de la arista e del grafo.

Definición 2.3.2 Sea $X = (V, E)$ un grafo, la *divergencia* de X es la función $\mathcal{D}^*\colon L^2(E) \to L^2(V)$ definida para cada $f \in L^2(E)$ como

$$(\mathcal{D}^*(f))(v) = \sum_{\substack{e\in E\\ v=e^+}} f(e) - \sum_{\substack{e\in E\\ v=e^-}} f(e).$$

$(\mathcal{D}^*(f))(v)$ mide el flujo total de entrada del vértice v.

Definición 2.3.3 Sea $X = (V, E)$ un grafo, el *Laplaciano* de X es la función $\Delta\colon L^2(V) \to L^2(V)$ definida por $\Delta = \mathcal{D}^* \circ \mathcal{D}$.

Lema 2.3.4 Si $X = (V, E)$ es un grafo $d-$regular y $\mathscr{A}$ su operador de adyacencia, entonces $\Delta = dI - \mathscr{A}$.

Demostración.
Sea $f \in L^2(V)$ y $v \in V$

$$\begin{aligned}
(\Delta(f))(v) &= (\mathcal{D}^* \circ \mathcal{D}(f))(v)\\
&= \sum_{\substack{e\in E\\ v=e^+}} \mathcal{D}(f)(e) - \sum_{\substack{e\in E\\ v=e^-}} \mathcal{D}(f)(e)\\
&= \sum_{\substack{e\in E\\ v=e^+}} (f(e^+) - f(e^-)) - \sum_{\substack{e\in E\\ v=e^-}} (f(e^+) - f(e^-))\\
&= \left(\sum_{\substack{e\in E\\ v=e^+}} f(v) - \sum_{\substack{e\in E\\ v=e^+\\ w=e^-}} f(w)\right) - \left(\sum_{\substack{e\in E\\ v=e^-\\ w=e^+}} f(w) - \sum_{\substack{e\in E\\ v=e^-}} f(v)\right)\\
&= \left(\sum_{\substack{e\in E\\ v=e^+}} f(v) + \sum_{\substack{e\in E\\ v=e^-}} f(v)\right) - \left(\sum_{\substack{e\in E\\ v=e^+\\ w=e^-}} f(w) + \sum_{\substack{e\in E\\ v=e^-\\ w=e^+}} f(w)\right)\\
&= df(v) - \sum_{w\in N_X(v)} f(w)\\
&= ((dI - \mathscr{A})(f))(v),
\end{aligned}$$

es decir, $(\Delta(f))(v) = ((dI - \mathscr{A})(f))(v)$ para cada $f \in L^2(V)$ y $v \in V$. Por lo tanto $\Delta = dI - \mathscr{A}$. ■

Corolario 2.3.5 Δ es un operador lineal.

Observación 2.3.6 Por el Lema 2.3.4 podemos expresar los valores propios de $\mathscr{A}$ en términos de Δ y viceversa.

Teorema 2.3.7 Sea $X = (V, E)$ un grafo $d-$regular, $f \in L^2(V)$ y $g \in L^2(E)$, entonces

$$\langle \mathcal{D}(f), g\rangle_2 = \langle f, \mathcal{D}^*(g)\rangle_2 \qquad \text{y} \qquad \langle \Delta(f), f\rangle_2 = \sum_{e\in E} |f(e^+) - f(e^-)|^2.$$

Demostración.

$$\begin{aligned}
\langle \mathcal{D}(f), g\rangle_2 = \sum_{e\in E} (\mathcal{D}(f))(e)\overline{g(e)} &= \sum_{e\in E} (f(e^+) - f(e^-))\overline{g(e)} \\
&= \sum_{e\in E} f(e^+)\overline{g(e)} - \sum_{e\in E} f(e^-)\overline{g(e)} \\
&= \sum_{\substack{e\in E \\ v=e^+}} f(v)\overline{g(e)} - \sum_{\substack{e\in E \\ v=e^-}} f(v)\overline{g(e)} \\
&= \sum_{v\in V} f(v) \sum_{\substack{e\in E \\ v=e^+}} \overline{g(e)} - \sum_{v\in V} f(v) \sum_{\substack{e\in E \\ v=e^-}} \overline{g(e)} \\
&= \sum_{v\in V} f(v)\overline{(\sum_{\substack{e\in E \\ v=e^+}} g(e) - \sum_{\substack{e\in E \\ v=e^-}} g(e))} \\
&= \sum_{v\in V} f(v)\overline{((\mathcal{D}^*(g))(v))} \\
&= \langle f, \mathcal{D}^*(g)\rangle_2,
\end{aligned}$$

es decir, $\langle \mathcal{D}(f), g\rangle_2 = \langle f, \mathcal{D}^*(g)\rangle_2$.

Luego

$$\begin{aligned}
\langle \Delta(f), f\rangle_2 = \langle \mathcal{D}^* \circ \mathcal{D}(f), f\rangle_2 &= \overline{\langle f, \mathcal{D}^*(\mathcal{D}(f))\rangle_2} \\
&= \overline{\langle \mathcal{D}(f), \mathcal{D}f\rangle_2} \\
&= \langle \mathcal{D}(f), \mathcal{D}(f)\rangle_2 \\
&= \sum_{e\in E} (f(e^+) - f(e^-))\overline{(f(e^+) - f(e^-))} \\
&= \sum_{e\in E} |(f(e^+) - f(e^-))|^2,
\end{aligned}$$

es decir, $\langle \Delta(f), f\rangle_2 = \sum_{e\in E} |(f(e^+) - f(e^-))|^2$. ■

2.3.2. Teorema Rayleigh-Ritz

Denotemos por $\lambda_2(X)$ al segundo valor propio más grande asociado a un grafo X. El Teorema Rayleigh- Ritz nos proporciona un método útil para determinar $\lambda_2(X)$.

Teorema 2.3.8 (Rayleigh-Ritz) Sea $X = (V, E)$ un grafo $d-$regular con $|V| = n$ entonces

$$\lambda_2(X) = \max_{f \in L_1^2(V,\mathbb{R})} \frac{\langle \mathscr{A}(f), f\rangle_2}{\langle f, f\rangle_2} = \max_{\substack{f \in L_1^2(V,\mathbb{R}) \\ \|f\|_2 = 1}} \langle \mathscr{A}(f), f\rangle_2.$$

Equivalentemente, tenemos que

$$d - \lambda_2(X) = \min_{f \in L_1^2(V,\mathbb{R})} \frac{\langle \Delta(f), f\rangle_2}{\langle f, f\rangle_2} = \min_{\substack{f \in L_1^2(V,\mathbb{R}) \\ \|f\|_2 = 1}} \langle \Delta(f), f\rangle_2.$$

Demostración.

Sea $\{f_1, g_2, \ldots, g_n\}$ una base ortonormal de $L^2(V, \mathbb{R})$ tal que g_i es una eigenfunción de $\mathscr{A}$ asociada al valor propio λ_i con $i \in \{2, \ldots, n\}$ y f_1 es la función constante 1 que también funge como eigenfunción asociada al valor propio $\lambda_1 = d$.

Sea $f \in L_1^2(V, \mathbb{R})$ con $\|f\|_2 = 1$, entonces $f = c_1 f_1 + c_2 g_2 + \cdots + c_n g_n$ para algunos $c_i \in \mathbb{R}$ y $0 = \langle f, f_1\rangle_2 = c_1\langle f_1, f_1\rangle_2 + c_2\langle g_2, f_1\rangle_2 + \cdots + c_n\langle g_n, f_1\rangle_2 = c_1$. Así que $f = c_2 g_2 + \cdots + c_n g_n$.
Luego

$$\begin{aligned}
\langle \mathscr{A}(f), f\rangle_2 &= \left\langle \mathscr{A}\left(\sum_{i=2}^n c_i g_i\right), \sum_{j=2}^n c_j g_j \right\rangle_2 \\
&= \left\langle \sum_{i=2}^n \lambda_i c_i g_i, \sum_{j=2}^n c_j g_j \right\rangle_2 \\
&= \sum_{i=2}^n \sum_{j=2}^n \langle \lambda_i c_i g_i, c_j g_j\rangle_2 \\
&= \sum_{i=2}^n \sum_{j=2}^n \lambda_i c_i c_j \langle g_i, g_j\rangle_2 \\
&= \sum_{i=2}^n \lambda_i c_i^2 \\
&\leq \lambda_2(X) \sum_{i=2}^n c_i^2 \\
&= \lambda_2(X)\|f\|_2^2 \\
&= \lambda_2(X).
\end{aligned}$$

Entonces $\lambda_2(X) \geq \max\limits_{\substack{f \in L_1^2(V,\mathbb{R}) \\ \|f\|_2 = 1}} \langle \mathscr{A}(f), f\rangle_2$.

Dado que $g_2 \in L_1^2(V, \mathbb{R})$ con $\|g_2\| = 1$ y $\langle \mathscr{A}(g_2), g_2\rangle_2 = \langle \lambda_2(X) g_2, g_2\rangle_2 = \lambda_2(X)$,

tenemos que

$$\lambda_2(X) = \max_{\substack{f\in L_1^2(V,\mathbb{R})\\ \|f\|_2=1}} \langle \mathscr{A}(f), f\rangle_2.$$

Luego, por el Lema 2.3.4 tenemos que

$$\langle \Delta(f), f\rangle_2 = \langle (dI - \mathscr{A})(f), f\rangle_2 = d\langle f, f\rangle_2 - \langle \mathscr{A}(f), f\rangle_2 = d\|f\|_2^2 - \langle \mathscr{A}(f), f\rangle_2 \geq d - \lambda_2(X),$$

entonces $d - \lambda_2(X) \leq \min_{\substack{f\in L_1^2(V,\mathbb{R})\\ \|f\|_2=1}} \langle \Delta(f), f\rangle_2$.

Y dado que $\langle \Delta(g_2), g_2\rangle = d\langle g_2, g_2\rangle_2 - \langle \mathscr{A}(g_2), g_2\rangle_2 = d - \lambda_2(X)$, tenemos que

$$d - \lambda_2 = \min_{\substack{f\in L_1^2(V,\mathbb{R})\\ \|f\|_2=1}} \langle \Delta(f), f\rangle_2.$$

■

Observación 2.3.9 Por el Corolario 1.2.38 el operador de adyacencia $\mathscr{A}$ de un grafo es autoadjunto, entonces para cada $f \in L_1^2(V)$ tenemos que $\langle \mathscr{A}(f), f\rangle_2 = \langle f, \mathscr{A}f\rangle_2 = \overline{\langle \mathscr{A}(f), f\rangle_2}$, así que $\langle \mathscr{A}(f), f\rangle_2$ es un real. Siguiendo las ideas planteadas en la prueba del Teorema 2.3.8 se demuestra que

$$\lambda_2(X) = \max_{\substack{f\in L_1^2(V)\\ \|f\|_2=1}} \langle \mathscr{A}(f), f\rangle_2.$$

2.3.3. Desigualdad de Cheeger

Sea X un grafo $d-$regular, tenemos que

$$\frac{d - \lambda_2(X)}{2} \leq h(X) \leq \sqrt{2d(d - \lambda_2(X))} \tag{2.1}$$

estas desigualdades fueron dadas por Cheeger [19] y Buster [16] para el caso continuo, posteriormente Dodziuk [25], Alon y Milman [4] dieron pruebas independientes para el caso discreto. A continuación probaremos (2.1) mediante los Teoremas 2.3.10 y 2.3.11 haciendo uso del Laplaciano discreto y el Teorema Rayleigh-Ritz.

Teorema 2.3.10 Sea $X = (V, E)$ un grafo $d-$regular entonces

$$\frac{d - \lambda_2(X)}{2} \leq h(X).$$

Demostración.

Sea $F \subseteq V$ tal que $h(X) = |E(F, V\backslash F)|/|F|$. Definimos las siguientes funciones

$$g(v) = \begin{cases} |V \setminus F| & \text{si } \ v \in F \\ -|F| & \text{si } \ v \in V \setminus F \end{cases}$$

y $f = g/\|g\|_2$.

Notemos que que $f, g \in L_1^2(V, \mathbb{R})$ ya que

$$\begin{aligned}\langle g, f_1\rangle = \sum_{v\in V} g(v) &= \sum_{v\in F} |V \setminus F| + \sum_{v\in V\setminus F} -|F| \\ &= |F||V \setminus F| - |V \setminus F||F| = 0.\end{aligned}$$

Por el Teorema 2.3.7 tenemos que

$$\begin{aligned}\langle \Delta(g), g\rangle_2 = \sum_{e\in E} |g(e^+) - g(e^-)|^2 &= \sum_{e\in E(F,V\setminus F)} (|V \setminus F| + |F|)^2 \\ &= |E(F, V \setminus F)|(|V \setminus F| + |F|)^2.\end{aligned}$$

Además

$$\begin{aligned}\|g\|_2^2 = \sum_{v\in V} |g(v)|^2 &= \sum_{v\in F} |V \setminus F|^2 + \sum_{v\in V\setminus F} (-|F|)^2 \\ &= |F||V \setminus F|^2 + |V \setminus F||F|^2 \\ &= |V \setminus F||F|(|V \setminus F| + |F|).\end{aligned}$$

Entonces

$$\begin{aligned}\langle \Delta(f), f\rangle_2 = \frac{\langle \Delta(g), g\rangle}{\|g\|_2^2} &= \frac{|E(F, V \setminus F)|(|V \setminus F| + |F|)^2}{|V \setminus F||F|(|V \setminus F| + |F|)} \\ &= h(X)\left(\frac{|V \setminus F| + |F|}{|V \setminus F|}\right) \\ &\leq h(X)2.\end{aligned}$$

Luego, por el Teorema Rayleigh-Ritz 2.3.8 tenemos que

$$\begin{aligned}d - \lambda_2(X) &\leq \langle \Delta(f), f\rangle_2 \\ &\leq 2h(X).\end{aligned}$$

Por lo tanto, $\dfrac{d - \lambda_2(X)}{2} \leq h(X)$. ■

Teorema 2.3.11 Sea $X = (V, E)$ un grafo $d-$regular, entonces

$$h(X) \leq \sqrt{2d(d - \lambda_2(X))}.$$

La prueba de este teorema es más laboriosa por lo que la dividiremos en los Lemas 2.3.12 y 2.3.15.

Sea $g \in L_1^2(V,\mathbb{R}) - \{0\}$ tal que $\mathscr{A}(g) = \lambda_2(X)\ g$, entonces $0 = \langle g, f_1\rangle = \sum_{v\in V} g(v)$, por lo que $g^{\leftarrow}(\mathbb{R}_+) = \{v \in V \mid g(v) \geq 0\} \subset V$. La función $-g$ también es una eigenfunción asociada a $\lambda_2(X)$, sea $\widetilde{g}$ definida como sigue

$$\widetilde{g} = \begin{cases} g & \text{si } |g^{\leftarrow}(\mathbb{R}_+)| \leq \frac{|V|}{2}, \\ -g & \text{si } |V \setminus g^{\leftarrow}(\mathbb{R}_+)| \leq \frac{|V|}{2}. \end{cases}$$

Sea $V^+ = \{v \in V \mid \widetilde{g}(v) \geq 0\}$ y $f \in L^2(V,\mathbb{R})$ definida por

$$f(v) = \begin{cases} \widetilde{g}(v) & \text{si } v \in V^+, \\ 0 & \text{en otro caso.} \end{cases}$$

Lema 2.3.12

$$\frac{\langle \Delta(f), f\rangle_2}{\langle f, f\rangle_2} \leq d - \lambda_2(X)$$

Demostración.

Sea $v \in V$. Por el Lema 2.3.4 tenemos que

$$(\Delta(f))(v) = (dI - \mathscr{A}(f))(v) = df(v) - (\mathscr{A}(f))(v) = df(v) - \sum_{w\in N_X(v)} f(w).$$

Si $v \in V^+$,

$$\begin{aligned}
(\Delta(f))(v) = df(v) - \sum_{w\in N_X(v)} f(w) &= d\,\widetilde{g}(v) - \left(\sum_{\substack{w\in N_X(v)\\ w\in V^+}} f(w) + \sum_{\substack{w\in N_X(v)\\ w\in V\setminus V^+}} f(w) \right) \\
&= d\,\widetilde{g}(v) - \left(\sum_{\substack{w\in N_X(v)\\ w\in V^+}} \widetilde{g}(w) + \sum_{\substack{w\in N_X(v)\\ w\in V\setminus V^+}} 0 \right) \\
&= d\,\widetilde{g}(v) - \sum_{\substack{w\in N_X(v)\\ w\in V^+}} \widetilde{g}(w) \\
&\leq d\,\widetilde{g}(v) - \sum_{w\in N_X(v)} \widetilde{g}(w) \\
&= d\,\widetilde{g}(v) - (\mathscr{A}(\widetilde{g}))(v) \\
&= d\,\widetilde{g}(v) - \lambda_2(X)\widetilde{g}(v),
\end{aligned}$$

es decir, $(\Delta(f))(v) \leq d\,\widetilde{g}(v) - \lambda_2(X)\widetilde{g}(v)$ para cada $v \in V^+$.

Luego

$$\begin{aligned}
\langle \Delta(f), f\rangle_2 = \sum_{v\in V}(\Delta(f))(v)\overline{f(v)} &= \sum_{v\in V^+}(\Delta(f))(v)\overline{f(v)} + \sum_{v\in V\setminus V^+}(\Delta(f))(v)\overline{f(v)} \\
&= \sum_{v\in V^+}(\Delta(f))(v)\overline{\widetilde{g}(v)} + \sum_{v\in V\setminus V^+}\Delta f(v)\overline{0} \\
&= \sum_{v\in V^+}\Delta f(v)\widetilde{g}(v) \\
&\leq \sum_{v\in V^+}(d\,\widetilde{g}(v) - \lambda_2(X)\widetilde{g}(v))\widetilde{g}(v) \\
&= \sum_{v\in V^+}(d-\lambda_2(X))\widetilde{g}(v)^2 \\
&= (d-\lambda_2(X))\sum_{v\in V^+}\widetilde{g}(v)^2 \\
&= (d-\lambda_2(X))\sum_{v\in V^+}f(v)^2 \\
&= (d-\lambda_2(X))\langle f, f\rangle_2,
\end{aligned}$$

es decir, $\langle \Delta(f), f\rangle_2 \leq (d-\lambda_2(X))\langle f, f\rangle_2$. Por lo tanto, $\dfrac{\langle \Delta f, f\rangle_2}{\langle f, f\rangle_2} \leq (d-\lambda_2(X)$. ■

Si se orientan las aristas del grafo, de tal forma que para cada $e \in E$, , $f(e^+) \geq f(e^-)$. Podemos definir la siguiente constante positiva

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

Lema 2.3.13

$$B_f \leq \sqrt{2d\langle \Delta(f), f\rangle_2\langle f, f\rangle_2}$$

Demostración.

$$\begin{aligned}
B_f = \sum_{e\in E}\left(f(e^+)^2 - f(e^-)^2\right) &= \sum_{e\in E}\left(f(e^+) + f(e^-)\right)\left(f(e^+) - f(e^-)\right) \\
&= \sum_{e\in E}\left(f(e^+) + f(e^-)\right)\left(\overline{f(e^+) - f(e^-)}\right) \\
&= \sum_{e\in E}\left(f(e^+) + f(e^-)\right)\left(\overline{(\mathcal{D}(f))(e)}\right).
\end{aligned}$$

Sea $\phi \in L^2(E, \mathbb{R})$ tal que $\phi(e) = f(e^+) + f(e^-)$, entonces

$$B_f = \sum_{e\in E}\left(f(e^+) + f(e^-)\right)\left(\overline{(\mathcal{D}(f))(e)}\right)$$

$$
\begin{aligned}
&= \sum_{e\in E} (\phi(e)) \left(\overline{(\mathcal{D}(f))(e)}\right) \\
&= \langle \phi, \mathcal{D}(f)\rangle_2 \\
&\leq |\langle \phi, \mathcal{D}(f)\rangle_2| \\
&\leq \|\phi\|_2 \cdot \|\mathcal{D}(f)\|_2 && \text{(Desigualdad Cauchy Schwatz)} \\
&= \sqrt{\sum_{e\in E} |f(e^+) + f(e^-)|^2} \cdot \sqrt{\sum_{e\in E} |f(e^+) - f(e^-)|^2} \\
&= \sqrt{\sum_{e\in E} (f(e^+) + f(e^-))^2} \cdot \sqrt{\langle \Delta(f), f\rangle_2} && \text{(Teorema 2.3.7)} \\
&\leq \sqrt{\sum_{e\in E} 2\,(f(e^+)^2 + f(e^-)^2)} \cdot \sqrt{\langle \Delta(f), f\rangle_2} && ((a+b)^2 \leq 2(a^2+b^2)\ a, b \in \mathbb{R}) \\
&= \sqrt{2\sum_{e\in E} f(e^+)^2 + f(e^-)^2} \cdot \sqrt{\langle \Delta(f), f\rangle_2} \\
&= \sqrt{2d\sum_{v\in V} f(v)^2} \cdot \sqrt{\langle \Delta(f), f\rangle_2} \\
&= \sqrt{2d\langle f, f\rangle_2} \cdot \sqrt{\langle \Delta(f), f\rangle_2} \\
&= \sqrt{2d\langle f, f\rangle_2 \langle \Delta(f), f\rangle_2}.
\end{aligned}
$$

Por lo tanto, $B_f \leq \sqrt{2d\langle f, f\rangle_2\langle \Delta(f), f\rangle_2}$. ■

Lema 2.3.14

$$h(X)\langle f, f\rangle_2 \leq B_f$$

Demostración.

La prueba de este lema hace uso de dividir los vértices del grafo en curvas de nivel, al ser un concepto más geométrico algunos resultados son difíciles de seguir. Por lo que se le invita al lector consultar el Ejemplo 2.3.16 para tener una noción más clara de las curvas de nivel de un grafo.

Sean $0 = \beta_0, \beta_1, \ldots, \beta_r$ los valores de f sobre los vértices del grafo y $L_i = \{v \in V \mid f(v) \geq \beta_i\}$ con $i \in \{0, 1, \ldots, r\}$. Los conjuntos L_i serán nuestras curvas de nivel. Notemos que

$$L_r \subseteq L_{r-1} \subseteq \cdots \subseteq L_1 \subseteq L_0 = V,$$

$E(L_0, V\setminus L_0) = \emptyset$ y para $i \geq 1$, $L_i \subseteq V^+$. Sea e una arista tal que $f(e^+) - f(e^-) \neq 0$, entonces $f(e^-) = \beta_j$ y $f(e^+) = \beta_i$ con $j \leq i$

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

$$
\begin{aligned}
&= \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} f(e^+)^2 - f(e^-)^2 + \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j=i}} f(e^+)^2 - f(e^-)^2\\
&= \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} \beta_i^2 - \beta_j^2\\
&= \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} \beta_i^2 - \beta_j^2 + \big((\beta_{i-1}^2 - \beta_{i-1}^2) + \cdots + (\beta_{j+1}^2 - \beta_{j+1}^2)\big)\\
&= \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} (\beta_i^2 - \beta_{i-1}^2) + (\beta_{i-1}^2 - \beta_{i-2}^2) + \cdots + (\beta_{j+1}^2 - \beta_j^2)\\
&= \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} \sum_{l=j+1}^{i} (\beta_l^2 - \beta_{l-1}^2),
\end{aligned}
$$

es decir,

$$
B_f = \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} \sum_{l=j+1}^{i} (\beta_l^2 - \beta_{l-1}^2). \tag{2.2}
$$

Notemos que e es una arista que conecta al vértice $e^+ (f(e^+) = \beta_i)$ con el vértice $e^- (f(e^-) < \beta_j)$, así que e cruza cada curva de nivel β_l entre e^+ y e^- con $j < l \leq i$. En la expresión de B_f esto corresponde a la expansión de $\beta_l^2 - \beta_l^2$ sumando $\beta_i^2 - \beta_i^2$ de cada curva de nivel β_l por la que e cruza, es decir, $\beta_l^2 - \beta_l^2$ aparece para cada arista $e \in E(L_l, V \setminus L_l)$. Entonces

$$
B_f = \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} \sum_{l=j+1}^{i} (\beta_l^2 - \beta_{l-1}^2) = \sum_{l=1}^{r} |E(L_l, V \setminus L_l)|(\beta_l^2 - \beta_{l-1}^2). \tag{2.3}
$$

Dado que para $i \geq 1$, $L_i \subseteq V^+$ y $|V^+| \leq \frac{|V|}{2}$, entonces $|L_i| \leq \frac{|V|}{2}$, así que por la Definición 2.1.3 de la constante isoperimétrica $\frac{|E(L_i, V\setminus L_i)|}{|L_i|} \geq h(X)$, de ahí que

$$
|E(L_i, V \setminus L_i)| \geq |L_i| h(X). \tag{2.4}
$$

Sustituyendo (2.4) en (2.3) tenemos que

$$\begin{aligned}
B_f &= \sum_{l=1}^{r} |E(L_l, V \setminus L_l)|(\beta_l^2 - \beta_{l-1}^2) \\
&\geq \sum_{l=1}^{r} |L_l| h(X)(\beta_l^2 - \beta_{l-1}^2) \\
&= h(X) \sum_{l=1}^{r} |L_l|(\beta_l^2 - \beta_{l-1}^2) \\
&= h(X) \left(|L_1|(\beta_1^2 - \beta_0^2) + \cdots + |L_r|(\beta_r^2 - \beta_{r-1}^2) \right) \\
&= h(X) \left(|L_r|\beta_r^2 + (|L_{r-1}| - |L_r|)\beta_{r-1}^2) + \cdots + (|L_1| - |L_2|)\beta_1^2 \right) \\
&= h(X) \left(|L_r|\beta_r^2 + \sum_{l=1}^{r-1} (|L_l| - |L_{l+1}|)\beta_l^2 \right).
\end{aligned}$$

Notemos que para $i < r$, $L_i \setminus L_{i+1}$ es el conjunto de nivel donde f toma el valor β_i, es decir, $|L_i \setminus L_{i+1}| = |f^{\leftarrow}(\beta_i)|$. Entonces

$$\begin{aligned}
B_f &\geq h(X) \left(|L_r|\beta_r^2 + \sum_{l=1}^{r-1} (|L_l| - |L_{l+1}|)\beta_l^2 + 0 \right) \\
&= h(X) \left(|f^{\leftarrow}(\beta_r)|\beta_r^2 + \sum_{l=1}^{r-1} |f^{\leftarrow}(\beta_l)| \cdot \beta_l^2 + |f^{\leftarrow}(\beta_0)|\beta_0^2 \right) \\
&= h(X) \left(\sum_{l=0}^{r} |f^{\leftarrow}(\beta_l)| \cdot \beta_l^2 \right) \\
&= h(X) \sum_{v \in V} f(v)^2 \\
&= h(X) \langle f, f \rangle_2.
\end{aligned}$$

Por lo tanto, $B_f \geq h(X)\langle f, f \rangle_2$. ■

Lema 2.3.15

$$h(X)^2 \leq 2d \, \frac{\langle \Delta f, f \rangle_2}{\langle f, f \rangle_2}$$

Demostración.

De los Lemas 2.3.13 y 2.3.14 tenemos que

$$h(X)\langle f, f \rangle_2 \leq \sqrt{2d \langle \Delta(f), f \rangle_2 \langle f, f \rangle_2}.$$

Entonces

$$h(X)^2 \leq \frac{2d\langle \Delta(f), f \rangle_2}{\langle f, f \rangle_2}$$

■

Demostración del Teorema 2.3.11.

De los Lemas 2.3.12 y 2.3.15 tenemos que

$$h(X)^2 \leq \frac{2d\langle \Delta(f), f\rangle}{\langle f, f\rangle} \leq 2d(d - \lambda_2(X)).$$

Por lo tanto, $h(X) \leq \sqrt{2d(d - \lambda_2(X))}$.

■

Ejemplo 2.3.16 Consideremos el grafo $C_8 = (V, E)$ y la función $f\colon V \longrightarrow \mathbb{R}$ tal que

$$\begin{aligned} f(v_1) &= 3 & f(v_5) &= 3 \\ f(v_2) &= 0 & f(v_6) &= 0 \\ f(v_3) &= 1 & f(v_7) &= 0 \\ f(v_4) &= 2 & f(v_8) &= 2. \end{aligned}$$

A cada $e \in E$ le daremos una orientación de tal forma que $f(e^+) \geq f(e^-)$.

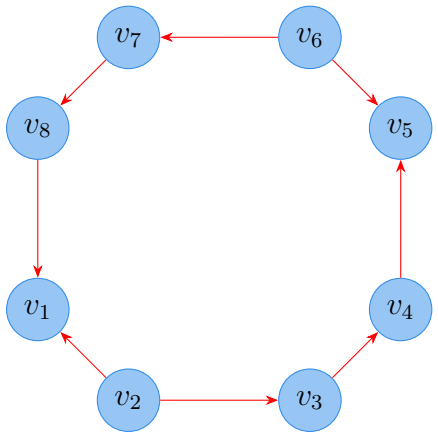


Figura 2.7: C_8 orientado.

Luego $\beta_0 = 0$, $\beta_1 = 1$, $\beta_2 = 2$ y $\beta_3 = 3$ son los valores que toma f por lo que las curvas de nivel de C_8 son:

$$\begin{aligned} L_0 &= \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}, \\ L_1 &= \{v_1, v_3, v_4, v_5, v_8\}, \\ L_2 &= \{v_1, v_4, v_5, v_8\}, \\ L_3 &= \{v_1, v_5\}. \end{aligned}$$

Por otro lado,

$$E(L_0, V \setminus L_0) = \emptyset,$$

$$E(L_1, V \setminus L_1) = \{\{v_2, v_1\}, \{v_2, v_3\}, \{v_6, v_5\}, \{v_7, v_8\}\},$$
$$E(L_2, V \setminus L_2) = \{\{v_2, v_1\}, \{v_3, v_4\}, \{v_6, v_5\}, \{v_7, v_8\}\},$$
$$E(L_3, V \setminus L_3) = \{\{v_2, v_1\}, \{v_8, v_1\}, \{v_6, v_5\}, \{v_4, v_5\}\}.$$

En la Figura 2.8 se ilustran las curvas de nivel para el grafo C^8 orientado.

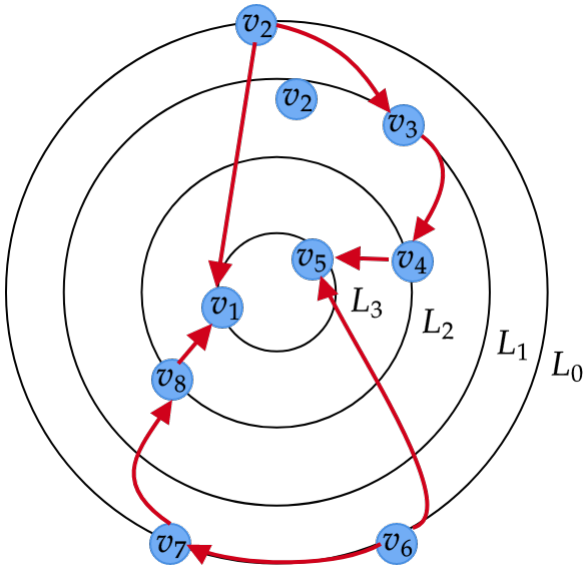


Figura 2.8: Curvas de nivel de C^8.

Veamos que se satisfacen (2.2) y (2.3).

$$\begin{aligned}
B_f &= \sum_{e \in E} f(e^+)^2 - f(e^-)^2 \\
&= \sum_{\substack{e \in E \\ f(e^-)=\beta_j \\ f(e^+)=\beta_i \\ j<i}} f(e^+)^2 - f(e^-)^2 + \sum_{\substack{e \in E \\ f(e^-)=\beta_j \\ f(e^+)=\beta_i \\ j=i}} f(e^+)^2 - f(e^-)^2 \\
&= \sum_{\substack{e \in E \\ f(e^-)=\beta_j \\ f(e^+)=\beta_i \\ j<i}} \beta_i^2 - \beta_j^2 + |\{\{v_6, v_7\}\}| \cdot 0 \\
&= \sum_{\substack{e \in E \\ f(e^-)=\beta_j \\ f(e^+)=\beta_i \\ j<i}} \beta_i^2 - \beta_j^2 + \left((\beta_{i-1}^2 - \beta_{i-1}^2) + \cdots + (\beta_{j+1}^2 - \beta_{j+1}^2)\right)
\end{aligned}$$

$$= \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} (\beta_i^2-\beta_{i-1}^2)+(\beta_{i-1}^2-\beta_{i-2}^2)+\cdots+(\beta_{j+1}^2-\beta_j^2)$$

$$= \sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} \sum_{l=j+1}^{i} (\beta_l^2-\beta_{l-1}^2)$$

Por lo que se cumple (2.2). Luego

$$\sum_{\substack{e\in E\\ f(e^-)=\beta_j\\ f(e^+)=\beta_i\\ j<i}} \sum_{l=j+1}^{i} (\beta_l^2-\beta_{l-1}^2)$$

$$= \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_1}} \sum_{l=1}^{1}(\beta_l^2-\beta_{l-1}^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_2}} \sum_{l=1}^{2}(\beta_l^2-\beta_{l-1}^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_3}} \sum_{l=1}^{3}(\beta_l^2-\beta_{l-1}^2)$$

$$+ \sum_{\substack{e\in E\\ f(e^-)=\beta_1\\ f(e^+)=\beta_2}} \sum_{l=2}^{2}(\beta_l^2-\beta_{l-1}^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_1\\ f(e^+)=\beta_3}} \sum_{l=2}^{3}(\beta_l^2-\beta_{l-1}^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_2\\ f(e^+)=\beta_3}} \sum_{l=3}^{3}(\beta_l^2-\beta_{l-1}^2)$$

$$= \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_1}} (\beta_1^2-\beta_0^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_2}} (\beta_1^2-\beta_0^2)+(\beta_2^2-\beta_1^2)$$

$$+ \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_3}} (\beta_1^2-\beta_0^2)+(\beta_2^2-\beta_1^2)+(\beta_3^2-\beta_2^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_1\\ f(e^+)=\beta_2}} (\beta_2^2-\beta_1^2)$$

$$+ \sum_{\substack{e\in E\\ f(e^-)=\beta_1\\ f(e^+)=\beta_3}} (\beta_2^2-\beta_1^2)+(\beta_3^2-\beta_2^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_2\\ f(e^+)=\beta_3}} (\beta_3^2-\beta_2^2)$$

$$= \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_1}} (\beta_1^2-\beta_0^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_2}} (\beta_1^2-\beta_0^2)+(\beta_2^2-\beta_1^2)$$

$$+ \sum_{\substack{e\in E\\ f(e^-)=\beta_0\\ f(e^+)=\beta_3}} (\beta_1^2-\beta_0^2)+(\beta_2^2-\beta_1^2)+(\beta_3^2-\beta_2^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_1\\ f(e^+)=\beta_2}} (\beta_2^2-\beta_1^2)$$

$$+ \sum_{\substack{e\in E\\ f(e^-)=\beta_1\\ f(e^+)=\beta_3}} (\beta_2^2-\beta_1^2) + (\beta_3^2-\beta_2^2) + \sum_{\substack{e\in E\\ f(e^-)=\beta_2\\ f(e^+)=\beta_3}} (\beta_3^2-\beta_2^2)$$

$$\begin{aligned}
&= \left|\left\{\{v_2,v_3\}\right\}\right| \cdot (\beta_1^2-\beta_0^2) + \left|\left\{\{v_7,v_8\}\right\}\right| \cdot \left[(\beta_1^2-\beta_0^2)+(\beta_2^2-\beta_1^2)\right]\\
&\quad + \left|\left\{\{v_2,v_1\},\{v_6,v_5\}\right\}\right| \cdot \left[(\beta_1^2-\beta_0^2)+(\beta_2^2-\beta_1^2)+(\beta_3^2-\beta_2^2)\right]\\
&\quad + \left|\left\{\{v_3,v_4\}\right\}\right| \cdot (\beta_2^2-\beta_1^2) + |\emptyset| \cdot \left[(\beta_2^2-\beta_1^2)+(\beta_3^2-\beta_2^2)\right]\\
&\quad + \left|\left\{\{v_4,v_5\},\{v_8,v_1\}\right\}\right| \cdot (\beta_3^2-\beta_2^2)
\end{aligned}$$

$$\begin{aligned}
&= (\beta_1^2-\beta_0^2) \cdot \left[\left|\left\{\{v_2,v_3\}\right\}\right| + \left|\left\{\{v_7,v_8\}\}\right\}\right| + \left|\left\{\{v_2,v_1\},\{v_6,v_5\}\}\right\}\right|\right]\\
&\quad + (\beta_2^2-\beta_1^2) \cdot \left[\left|\left\{\{v_7,v_8\}\right\}\right| + \left|\left\{\{v_2,v_1\},\{v_6,v_5\}\right\}\right| + \left|\left\{\{v_3,v_4\}\right\}\right|\right]\\
&\quad + (\beta_3^2-\beta_2^2) \cdot \left[\left|\left\{\{v_2,v_1\},\{v_6,v_5\}\right\}\right| + \left|\left\{\{v_4,v_5\},\{v_8,v_1\}\right\}\right|\right]
\end{aligned}$$

$$\begin{aligned}
&= (\beta_1^2-\beta_0^2)\left|\left\{\{v_2,v_3\},\{v_7,v_8\},\{v_2,v_1\},\{v_6,v_5\}\right\}\right| +\\
&\quad (\beta_2^2-\beta_1^2)\left|\left\{\{v_7,v_8\},\{v_2,v_1\},\{v_6,v_5\},\{v_3,v_4\}\right\}\right| +\\
&\quad (\beta_3^2-\beta_2^2)\left|\left\{\{v_2,v_1\},\{v_6,v_5\},\{v_4,v_5\},\{v_8,v_1\}\right\}\right|
\end{aligned}$$

$$\begin{aligned}
&= (\beta_1^2-\beta_0^2)|E(L_1,V\setminus L_1)| + (\beta_2^2-\beta_1^2)|E(L_2,V\setminus L_2)|\\
&\quad + (\beta_3^2-\beta_2^2)|E(L_3,V\setminus L_3)|\\
&= \sum_{l=1}^{3} |E(L_l,V\setminus L_l)|(\beta_l^2-\beta_{l-1}^2).
\end{aligned}$$

Por lo tanto, se verifica (2.3).

Definición 2.3.17 Si X es un grafo conexo $d-$regular, $d-\lambda_2(X)$ es llamada la *brecha espectral* de X.

La desigualdad de Cheeger 2.1 nos muestra que entre más grande sea la brecha espectral, mejor será la constante isoperimétrica y por ende mejor expander. Por lo tanto podemos caracterizar una familia de grafos expander en base a la brecha espectral.

Teorema 2.3.18 Sea (X_n) una sucesión de grafos $d-$regulares tales que $|X_n| \to \infty$ cuando $n \to \infty$. (X_n) es una familia de grafos expanders si y solo si la sucesión $(d-\lambda_2(X_n))$ está acotada lejos de cero.

Demostración.

Si (X_n) es una familia de grafos expander, entonces existe $\varepsilon > 0$ tal que para cada $n \in \mathbb{N}$, $h(X_n) \geq \varepsilon$. Por la desigualdad de Cheeger (2.1) tenemos que

$$\sqrt{2d(d - \lambda_2(X_n))} \geq h(X_n) \geq \varepsilon,$$

entonces $d - \lambda_2(X_n) \geq \frac{\varepsilon^2}{2d} > 0$. Por lo tanto, $(d - \lambda_2(X_n))$ está acotada lejos de cero.

Ahora, si $(d - \lambda_2(X_n))$ está acotada lejos de cero, existe $\varepsilon > 0$ tal que para cada $n \in \mathbb{N}$, $d - \lambda_2(X_n) \geq \varepsilon$. Por la desigualdad de Cheeger 2.1 tenemos que

$$h(X_n) \geq \frac{d - \lambda_2(X_n)}{2} \geq \frac{\varepsilon}{2}.$$

Por lo tanto, (X_n) es una familia de grafos expanders. ■

Ejemplo 2.3.19 El grafo de Cayley $Cay(\mathbb{Z}/n\mathbb{Z}, \{1, -1\})$ es el grafo ciclo C^n con n vértices. La matriz de adyacencia de C^n es la siguiente matriz circulante

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

Sea $\xi = \exp(2\pi i/n)$ y $a \in \{0, 1, ..., n-1\}$. Los valores propios de C^n son

$$\begin{aligned} \chi_a &= \xi^a + \xi^{a(n-1)} \\ &= \cos\left(\frac{2\pi a}{n}\right) + i \sin\left(\frac{2\pi a}{n}\right) + \cos\left(\frac{2\pi a(n-1)}{n}\right) + i \sin\left(\frac{2\pi a(n-1)}{n}\right) \\ &= 2\cos\left(\frac{2\pi a}{n}\right) \end{aligned}$$

Si n es par

$$Spec(C^n) = \begin{pmatrix} -2 & 2\cos\left(\frac{2\pi((n/2)-1)}{n}\right) & \dots & 2\cos\left(\frac{4\pi}{n}\right) & 2\cos\left(\frac{2\pi}{n}\right) & 2 \\ 1 & 2 & \dots & 2 & 2 & 1 \end{pmatrix}$$

Si n es impar

$$Spec(C^n) = \begin{pmatrix} 2\cos\left(\frac{2\pi((n/2)-1)}{n}\right) & \dots & 2\cos\left(\frac{4\pi}{n}\right) & 2\cos\left(\frac{2\pi}{n}\right) & 2 \\ 2 & \dots & 2 & 2 & 1 \end{pmatrix}$$

El segundo valor propio más grande del grafo ciclo C^n es $2\cos\left(\frac{2\pi}{n}\right)$. Como los grafos ciclo son $2-$regulares tenemos que su brecha espectral es $2 - 2\cos\left(\frac{2\pi}{n}\right)$. Luego

$$\lim_{n\to\infty} 2 - 2\cos\left(\frac{2\pi}{n}\right) = 0.$$

Por lo tanto, (C^n) no es una familia de grafos expanders.

Observación 2.3.20 En el ejemplo anterior mostramos una familia de grafos que no es expander, no obstante dar un ejemplo concreto de una familia de grafos expander no es una tarea sencilla. En el capítulo 3 se desarrollará más el tema de la construcción y la no-construcción de familias de grafos expanders.

Definición 2.3.21 Sea X un grafo $d-$regular con n vértices y sean $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ los valores propios asociados a X. Definimos la *constante de expansión espectral* de X como

$$\lambda(X) = \text{máx}\{|\lambda_i| : 1 \leq i \leq n \text{ con } |\lambda_i| \neq d\}.$$

Observación 2.3.22 Algunos autores(ver [37] y [58]) suelen definir al grafo X como $\lambda(X)-$espectral expander o $(n, d, \lambda(X))-$expander.

Dado que $\lambda_2(X) \leq \lambda(X)$ tenemos que $d - \lambda(X) \leq d - \lambda_2(X)$. Entonces un corolario del Teorema 2.3.18 es el siguiente.

Corolario 2.3.23 Sea (X_n) una sucesión de grafos $d-$regulares tales que $|X_n| \to \infty$ cuando $n \to \infty$. Si la sucesión $(d - \lambda(X_n))$ está acotada lejos de cero, entonces (X_n) es una familia de grafos expanders.

La siguiente proposición nos da un método para calcular la constante de expansión espectral de un grafo, de manera similar al que nos da el Teorema Rayleight-Ritz 2.3.8 para calcular el segundo valor propio más grande del grafo.

Proposición 2.3.24 Sea $X = (V, E)$ un grafo $d-$regular con $|V| = n$, entonces

$$\lambda(X) = \max_{f \in L_1^2(V,\mathbb{R})} \frac{|\langle \mathscr{A}(f), f\rangle_2|}{\langle f, f\rangle_2} = \max_{\substack{f \in L_1^2(V,\mathbb{R}) \\ \|f\|_2 = 1}} |\langle \mathscr{A}(f), f\rangle_2|.$$

Demostración.

Sea $\{f_1, g_2, \ldots, g_n\}$ una base ortonormal de $L^2(V, \mathbb{R})$ tal que g_i es una eigenfunción de $\mathscr{A}$ asociada al valor propio λ_i con $i \in \{2, \ldots, n\}$ y f_1 es la función constante 1 que también funge como eigenfunción asociada al valor propio $\lambda_1 = d$.

Sea $f \in L_1^2(V, \mathbb{R})$ con $\|f\|_2 = 1$, entonces $f = c_1 f_1 + c_2 g_2 + \cdots + c_n g_n$ para algunos $c_i \in \mathbb{R}$ y $0 = \langle f, f_1\rangle_2 = c_1\langle f_1, f_1\rangle_2 + c_2\langle g_2, f_1\rangle_2 + \cdots + c_n\langle g_n, f_1\rangle_2 = c_1$. Así que $f = c_2 g_2 + \cdots + c_n g_n$.

Luego

$$\begin{aligned} |\langle \mathscr{A}(f), f\rangle_2| &= \left| \left\langle \mathscr{A}\left(\sum_{i=2}^{n} c_i g_i\right), \sum_{j=2}^{n} c_j g_j \right\rangle_2 \right| \\ &= \left| \left\langle \sum_{i=2}^{n} \lambda_i c_i g_i, \sum_{j=2}^{n} c_j g_j \right\rangle_2 \right| \end{aligned}$$

$$\begin{aligned}
&\leq \sum_{i=2}^{n}\sum_{j=2}^{n} |\langle \lambda_i c_i g_i, c_j g_j\rangle_2| \\
&= \sum_{i=2}^{n}\sum_{j=2}^{n} |\lambda_i c_i c_j \langle g_i, g_j\rangle_2| \\
&= \sum_{i=2}^{n} |\lambda_i||c_{i|}^2 \\
&\leq \lambda(X)\sum_{i=2}^{n} |c_i|^2 \\
&= \lambda(X)\|f\|_2^2 \\
&= \lambda(X).
\end{aligned}$$

Entonces $\lambda(X) \geq \max\limits_{\substack{f\in L_1^2(V,\mathbb{R}) \\ \|f\|_2=1}} |\langle \mathscr{A}(f), f\rangle_2|$.

Dado que existe un valor propio asociado a X, digamos λ_i tal que $\lambda(X) = |\lambda_i|$, la eigenfunción $g_i \in L_1^2(V,\mathbb{R})$ con $\|g_i\| = 1$ satisface que

$$|\langle \mathscr{A}(g_i), g_i\rangle_2| = |\langle \lambda_i g_i, g_i\rangle_2| = |\lambda_i| = \lambda(X).$$

Por lo tanto, $\lambda(X) = \max\limits_{\substack{f\in L_1^2(V,\mathbb{R}) \\ \|f\|_2=1}} |\langle \mathscr{A}(f), f\rangle_2|$. ■

Al igual que la brecha espectral, la constante de expansión espectral nos da información acerca de la conectividad del grafo. El siguiente Lema dado por Alon y Chung [2] nos da información acerca del número de aristas que pueden ser incidentes a un subconjunto de vértices del grafo.

Lema 2.3.25 ([2], Lema 2.3) Sea $X = (V, E)$ un grafo $d-$regular con n vértices y constante de expansión espectral $\lambda(X)$. Sea $A \subset V$ con $|A| = \gamma n$, con $0 < \gamma < 1$. Entonces, el número de aristas contenidos en el subgrafo inducido por A en X es a lo más

$$\frac{nd}{2}(\gamma^2 + \frac{\lambda(X)}{d}\gamma(1-\gamma))$$

Demostración.

Denotemos por $E(A)$ al conjunto de aristas que unen dos vértices de A. Probemos que $E(A) \leq \frac{nd}{2}(\gamma^2 + \frac{\lambda(X)}{d}\gamma(1-\gamma))$. Sea $\widetilde{f} \in L^2(V)$ dada por

$$\widetilde{f}(v) = \begin{cases} \frac{-1}{|A|} & \text{si } v \in A \\ \frac{1}{n-|A|} & \text{si } v \notin A. \end{cases}$$

Notemos que $\widetilde{f} \in L_1^2(V)$ ya que

$$\begin{aligned}\langle \widetilde{f}, f_1\rangle_2 = \sum_{v\in V} \widetilde{f}(v)\overline{f_1(v)} = \sum_{v\in V} \widetilde{f}(v) &= \sum_{v\in A} \widetilde{f}(v) + \sum_{v\notin A} \widetilde{f}(v)\\ &= \sum_{x\in A} \left(\tfrac{-1}{|A|}\right) + \sum_{x\notin A} \tfrac{1}{n-|A|}\\ &= |A|\left(\tfrac{-1}{|A|}\right) + (n-|A|)\tfrac{1}{n-|A|}\\ &= 0.\end{aligned}$$

Además

$$\begin{aligned}\|\widetilde{f}\|_2^2 = \langle \widetilde{f}, \widetilde{f}\rangle_2 = \sum_{v\in V} |\widetilde{f}(v)|^2 &= \sum_{v\in A} |\widetilde{f}(v)|^2 + \sum_{v\notin A} |\widetilde{f}(v)|^2\\ &= \sum_{v\in A} \left(\tfrac{-1}{|A|}\right)^2 + \sum_{v\notin A} \left(\tfrac{1}{n-|A|}\right)^2\\ &= |A|\left(\tfrac{1}{|A|^2}\right) + (n-|A|)\left(\tfrac{1}{(n-|A|)^2}\right)\\ &= \tfrac{1}{|A|} + \tfrac{1}{n-|A|},\end{aligned}$$

es decir, $\|\widetilde{f}\|_2^2 = \frac{1}{|A|} + \frac{1}{n-|A|}$. Luego por Teorema 2.3.7 tenemos que

$$\begin{aligned}\langle \Delta\widetilde{f}, \widetilde{f}\rangle_2 &= \sum_{e\in E} |\widetilde{f}(e^+) - \widetilde{f}(e^-)|^2\\ &= \sum_{\substack{e\in E\\ e^+\in A\\ e^-\in A}} |\widetilde{f}(e^+) - \widetilde{f}(e^-)|^2 + \sum_{\substack{e\in E\\ e^+\notin A\\ e^-\notin A}} |\widetilde{f}(e^+) - \widetilde{f}(e^-)|^2 + \sum_{\substack{e\in E\\ e^+\in A\\ e^-\notin X}} |\widetilde{f}(e^+) - \widetilde{f}(e^-)|^2\\ &+ \sum_{\substack{e\in E\\ e^+\notin X\\ e^-\in A}} |\widetilde{f}(e^+) - \widetilde{f}(e^-)|^2\\ &= \sum_{\substack{e\in E\\ e^+\in A\\ e^-\notin A}} \left|\tfrac{-1}{|A|} - \tfrac{1}{n-|A|}\right|^2 + \sum_{\substack{e\in E\\ e^+\notin A\\ e^-\in A}} \left|\tfrac{1}{n-|A|} + \tfrac{1}{|A|}\right|^2\\ &= \sum_{e\in E(A,V\setminus A)} \left(\tfrac{1}{|A|} + \tfrac{1}{n-|A|}\right)^2\\ &= |E(A, V\setminus A)|\left(\tfrac{1}{|A|} + \tfrac{1}{n-|A|}\right)^2,\end{aligned}$$

es decir, $\langle \Delta\widetilde{f}, \widetilde{f}\rangle_2 = |E(A, V\setminus A)|\left(\frac{1}{|A|} + \frac{1}{n-|A|}\right)^2$. Consideremos $f = \frac{\widetilde{f}}{\|\widetilde{f}\|_2}$, de los cálculos anteriores tenemos que

$$\langle \Delta f, f\rangle_2 = \frac{\langle \Delta\widetilde{f}, \widetilde{f}\rangle_2}{\|\widetilde{f}\|_2^2} = \frac{|E(A, V\setminus A)|\left(\frac{1}{|A|} + \frac{1}{n-|A|}\right)^2}{\frac{1}{|A|} + \frac{1}{n-|A|}} = |E(A, V\setminus A)|\left(\tfrac{1}{|A|} + \tfrac{1}{n-|A|}\right).$$

Luego, de la Proposición 2.3.24 y del Lema 2.3.4 tenemos que

$$\begin{aligned}\lambda(X) \geq |\langle \mathscr{A}(f), f\rangle_2| &= |\langle (dI - \Delta)(f), f\rangle_2| \\ &= |d\langle f, f\rangle_2 - \langle \Delta(f), f\rangle_2| \\ &= \left| d - |E(A, V \setminus A)| \left(\tfrac{1}{|A|} + \tfrac{1}{n-|A|}\right)\right|\end{aligned}$$

Entonces

$$-|E(A, V \setminus A)| \leq \frac{\lambda(X) - d}{\frac{1}{|A|} + \frac{1}{n-|A|}}.$$

Dado que $|A| = \gamma n$ tenemos que

$$-|E(A, V \setminus A)| \leq \frac{\lambda(X) - d}{\frac{1}{\gamma n} + \frac{1}{n-\gamma n}} = \frac{\lambda(X) - d}{\frac{n-\gamma n+\gamma n}{\gamma n^2 - \gamma^2 n^2}} = \frac{\lambda(X) - d}{\frac{1}{\gamma n - \gamma^2 n}} = (\lambda(X) - d)(\gamma n - \gamma^2 n),$$

es decir, $-|E(A, V \setminus A)| \leq \lambda(X)(\gamma n - \gamma^2 n) - d(\gamma n - \gamma^2 n)$. Luego, al ser X es un grafo $d-$regular tenemos que el total de aristas que salen de A son $d|A|$, pero estas aristas pueden tener como punto final un vértice en $V \setminus A$ así que pertenecen a $E(A, V \setminus A)$, o bien pueden tener puntos iniciales y finales en vértices de A así que este tipo de aristas están en $E(A)$ pero se estarían contando dos veces. Por lo tanto

$$2|E(A)| + |E(A, V \setminus A)| = d|A|.$$

Entonces

$$\begin{aligned}|E(A)| = \frac{d|A| - |E(A, V \setminus A)|}{2} &\leq \frac{d\gamma n + \lambda(X)(\gamma n - \gamma^2 n) - d(\gamma n - \gamma^2 n)}{2} \\ &= \frac{\lambda(X)(\gamma n - \gamma^2 n) + d\gamma^2 n}{2} \\ &= \frac{nd}{2}\left(\frac{\lambda(X)}{d}(\gamma(1-\gamma)) + \gamma^2\right).\end{aligned}$$

Por lo tanto, $|E(A)| \leq \frac{nd}{2}\left(\frac{\lambda(X)}{d}(\gamma(1-\gamma)) + \gamma^2\right)$. ■

2.4. Constante de Kazhdan

En las sección anterior relacionamos la constante isoperimétrica con la brecha espectral de cualquier grafo X, pero en el caso de un grafo de Cayley $X = Cay(G, S)$ existe otra constante que está relacionada con las representaciones irreducibles de G, que recibe el nombre de constante de Kazhdan. En esta sección daremos algunas de sus propiedades y mostraremos la relación que tiene con la constante isoperimétrica y la brecha espectral.

Definición 2.4.1 Sea G un grupo finito y $S \subseteq G$. Si (V, ρ) es una representación unitaria de G, con producto interno $G-$invariante $\langle \cdot, \cdot \rangle$. Para $S \neq \emptyset$, definimos la constante

$$\kappa'(G, S, \rho, \langle \cdot, \cdot \rangle) = \min_{\|v\|=1} \max_{s \in S} \|\rho(s)v - v\|. \tag{2.5}$$

Si $S = \emptyset$ definimos $\kappa'(G, \emptyset, \rho, \langle \cdot, \cdot \rangle) = 0$.

Observación 2.4.2 El mínimo en (2.5) existe. Si elegimos una base $\mathcal{B}$ para V e identificamos a V con $\mathbb{C}^n$ donde $n = dim V$, dado que todo elemento de V lo podemos ver en términos de la base $\mathcal{B}$ y las funciones de las operaciones suma, resta, multiplicación y la raíz cuadrada de números no negativos son continuas, tenemos que $\|\rho(s)v - v\|$ es una función continua.

Recordemos que si f y g son continuas, tenemos que $\max\{f, g\} = \frac{1}{2}(f+g+|f-g|)$ así que $\max\{f, g\}$ es una función continua, generalizando este hecho tenemos que el máximo de un número finito de funciones continuas es continua. Como S es un conjunto finito, tenemos que $\{\|\rho(s)v - v\| : s \in S\}$ es un conjunto finito de funciones continuas, entonces $\max\{\|\rho(s)v - v\| : s \in S\} = \max_{s \in S} \|\rho(s)v - v\|$ es una función continua.

Luego, como la esfera unitaria en V es cerrada y acotada por Teorema de Heine-Borel tenemos que la esfera unitaria en V es compacta y una función continua en un conjunto compacto alcanza su mínimo. Por lo tanto, el mínimo en (2.5) existe.

Observación 2.4.3 El hecho de que el mínimo exista implica que para cualquier representación unitaria irreducible $\rho\colon G \longrightarrow GL(V)$ existe un vector unitario $v \in V$ y $s \in S$ tales que $\|\rho(s)v - v\| = \kappa'(G, S, \rho, \langle \cdot, \cdot \rangle)$.

En la definición de $\kappa'(G, S, \rho, \langle \cdot, \cdot \rangle)$ pedimos que el producto interno sobre V sea $G-$invariante, este producto existe por el Teorema 1.3.7. La siguiente proposición nos muestra que $\kappa'(G, S, \rho, \langle \cdot, \cdot \rangle)$ no depende del producto interno, es decir, $\kappa'(G, S, \rho, \langle \cdot, \cdot \rangle) = \kappa'(G, S, \rho)$.

Proposición 2.4.4 Sea G un grupo finito, $S \subseteq G$ y (V, ρ) es una representación unitaria de G. Si $\langle \cdot, \cdot \rangle$ y $\langle \cdot, \cdot \rangle'$ son dos productos internos $G-$invariantes en V con normas $\| \cdot \|$ y $\| \cdot \|'$ respectivamente, entonces

$$\kappa'(G, S, \rho, \langle \cdot, \cdot \rangle) = \kappa'(G, S, \rho, \langle \cdot, \cdot \rangle').$$

Demostración.

Usando $\langle \cdot, \cdot \rangle$ en el Teorema de Maschke 1.3.24 podemos descomponer a V en una suma directa ortogonal de subespacios irreducibles $G-$invariantes de V, es decir, $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$. Haciendo lo mismo con $\langle \cdot, \cdot \rangle'$ tenemos que $V = V_1' \oplus V_2' \oplus \cdots \oplus V_m'$. Por la Proposición 1.3.26 tenemos que $n = m$ y reordenando los términos $V_1 \cong V_1', \ldots, V_n \cong V_n'$, por lo que existe un isomorfismo $G-$invariante $\phi_i\colon V_i \to V_i'$ para cada $i \in \{1, \ldots, n\}$, con estos isomorfismos consideremos el

isomorfismo $G-$invariante $\phi\colon V \to V$ tal que $\phi(V_i) = V_i'$ para cada $i \in \{1, \ldots, n\}$. Luego por la Proposición 1.3.14, tenemos que

$$\begin{aligned} \langle \cdot, \cdot \rangle'' \colon V \times V &\longrightarrow \mathbb{C} \\ (v, w) &\longmapsto \langle v, w \rangle'' = \langle \phi(v), \phi(w) \rangle' \end{aligned} \tag{2.6}$$

es un producto interno sobre V. Observe que $V_1 \oplus \cdots \oplus V_n$ sigue siendo una suma directa ortogonal con respecto a $\langle \cdot, \cdot \rangle''$. Entonces por la Proposición 1.3.21 existen números reales positivos $C_1, \ldots, C_n$ tales que para $v, w \in V_i$

$$\langle v, w \rangle'' = C_i \langle v, w \rangle. \tag{2.7}$$

Dado que $V = V_1 \oplus \cdots \oplus V_n$ tenemos que para cada $v \in V$ existen únicos $v_i \in V_i$ con $i \in \{1, \ldots, n\}$ tales que $v = \sum_{i=1}^{n} v_i$. Luego, consideremos la siguiente función

$$\begin{aligned} \psi\colon \{v \in V : \ \|v\| = 1\} &\longrightarrow \{v \in V : \ \|v\|' = 1\} \\ v = \sum_{i=1}^{n} v_i &\longmapsto \sum_{i=1}^{n} \frac{\phi(v_i)}{\sqrt{C_i}}. \end{aligned}$$

Sean $u, v \in \{v \in V : \|v\| = 1\}$ con $v = \sum_{i=1}^{n} v_i$ y $u = \sum_{i=1}^{n} u_i$ tales que $\psi(v) = \psi(u)$ así que $\sum_{i=1}^{n} \frac{\phi(v_i)}{\sqrt{C_i}} = \sum_{i=1}^{n} \frac{\phi(u_i)}{\sqrt{C_i}}$ de ahí que $\sum_{i=1}^{n} \frac{\phi(v_i) - \phi(u_i)}{\sqrt{C_i}} = 0$, entonces

$$\begin{aligned} 0 &= \left\langle \sum_{i=1}^{n} \frac{\phi(v_i) - \phi(u_i)}{\sqrt{C_i}}, \sum_{i=1}^{n} \frac{\phi(v_i) - \phi(u_i)}{\sqrt{C_i}} \right\rangle \\ &= \sum_{i=1}^{n} \frac{1}{\sqrt{C_i}} \left\langle \phi(v_i) - \phi(u_i), \sum_{i=1}^{n} \frac{\phi(v_i) - \phi(u_i)}{\sqrt{C_i}} \right\rangle \\ &= \sum_{i=1}^{n} \frac{1}{\sqrt{C_i}} \overline{\left\langle \sum_{i=1}^{n} \frac{\phi(v_i) - \phi(u_i)}{\sqrt{C_i}}, \phi(v_i) - \phi(u_i), \right\rangle} \\ &= \sum_{i=1}^{n} \frac{1}{\sqrt{C_i}} \sum_{i=1}^{n} \frac{1}{\sqrt{C_i}} \left\langle \phi(v_i) - \phi(u_i), \phi(v_i) - \phi(u_i) \right\rangle. \end{aligned}$$

Por consiguiente $\langle \phi(v_i) - \phi(u_i), \phi(v_i) - \phi(u_i), \rangle = 0$, así que $\phi(v_i) - \phi(u_i) = 0$, entonces $\phi(v_i) = \phi(u_i)$ y como ϕ es inyectiva tenemos que $v_i = u_i$ para cada $i \in \{1, \ldots n\}$, de ahí que $v = u$. Por lo tanto, ψ es inyectiva.

Luego, sea $u \in \{v \in V : \ \|v\|' = 1\}$ tenemos que $u = \sum_{i=1}^{n} u_i$ para algunos $u_i \in V_i'$ con $i \in \{1, \ldots n\}$, como $\sqrt{C_i}\ u_i \in V_i'$ y ϕ es un isomorfismo $G-$invariante existe

$v_i \in V_i$ tal que $\phi(v_i) = \sqrt{C_i}\ u_i$. Tomemos $v = \sum_{i=1}^{n} v_i$, notemos que $v \in V$ con $\|v\| = 1$ ya que

$$\begin{aligned}
\langle v, v\rangle = \left\langle \sum_{i=1}^{n} v_i, \sum_{j=1}^{n} v_j \right\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n}\langle v_i, v_j\rangle &= \sum_{i=1}^{n}\langle v_i, v_i\rangle + \sum_{i=1}^{n}\sum_{\substack{j=1\\ j\neq i}}^{n}\langle v_i, v_j\rangle \\
&= \sum_{i=1}^{n}\langle v_i, v_i\rangle \\
&= \sum_{i=1}^{n}\frac{\langle v_i, v_i\rangle''}{C_i} \\
&= \sum_{i=1}^{n}\frac{\langle \phi(v_i), \phi(v_i)\rangle'}{C_i} \\
&= \sum_{i=1}^{n}\frac{C_i\langle u_i, u_i\rangle'}{C_i} \\
&= \sum_{i=1}^{n}\langle u_i, u_i\rangle' + \sum_{i=1}^{n}\sum_{\substack{j=1\\ j\neq i}}^{n}\langle u_i, u_j\rangle' \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\langle u_i, u_j\rangle' \\
&= \left\langle \sum_{i=1}^{n} u_i, \sum_{i=1}^{n} u_i \right\rangle' \\
&= \langle u, u\rangle' \\
&= 1.
\end{aligned}$$

Entonces $v \in \{v \in V :\ \|v\| = 1\}$ es tal que

$$\psi(v) = \sum_{i=1}^{n}\frac{\phi(v_i}{\sqrt{C_i}} = \sum_{i=1}^{n}\frac{\sqrt{C_i}u_i}{\sqrt{C_i}} = \sum_{i=1}^{n} u_i = u.$$

Así que ψ es sobreyectiva y por consiguiente, biyectiva.

Sean $s \in S$ y $v \in \{v \in V : \|v\| = 1\}$ con $v = \sum_{i=1}^{n} v_i$, por la Observación 1.3.23 tenemos que para cada $l \in \{1, \ldots, n\}$ $\rho(s)v_l \in V_l$ y $\rho(s)\phi(v_l) \in V_l'$, así que $\rho(s)v_l - v_l \in V_l$ y para $\alpha \in \mathbb{C} \setminus \{0\}$ $\alpha(\rho(s)\phi(v_l) - \phi(v_l)) \in V_l'$, entonces para $i, j \in \{1, \ldots, n\}$ con $i \neq j$ ocurre que

$$\langle \rho(s)v_i - v_i,\ \rho(s)v_j - v_j\rangle = 0$$

y

$$\langle \alpha\left(\rho(s)\phi(v_i) - \phi(v_i)\right),\ \alpha\left(\rho(s)\phi(v_j) - \phi(v_j)\right)\rangle' = 0,$$

así que por el Teorema de Pitágoras

$$\left\|\sum_{i=1}^{n} \rho(s)v_i - v_i\right\|^2 = \sum_{i=1}^{n} \|\rho(s)v_i - v_i\|^2 \tag{2.8}$$

y

$$\left(\left\|\sum_{i=1}^{n} \alpha\rho(s)\phi(v_i) - \phi(v_i)\right\|'\right)^2 = \sum_{i=1}^{n} (\|\alpha\rho(s)\phi(v_i) - \phi(v_i)\|')^2, \tag{2.9}$$

luego

$$\begin{aligned}
\|\rho(s)v - v\|^2 &= \left\|\sum_{i=1}^{n} \rho(s)v_i - v_i\right\|^2 \\
&= \sum_{i=1}^{n} \|\rho(s)v_i - v_i\|^2 && \text{(Por 2.8)} \\
&= \sum_{i=1}^{n} C_i^{-1}(\|\rho(s)v_i - v_i\|'')^2 && \text{(Por 2.7)} \\
&= \sum_{i=1}^{n} C_i^{-1}(\|\rho(s)\phi(v_i) - \phi(v_i)\|')^2 && \text{(Por la definición de } \langle\cdot,\cdot\rangle'' \text{ 2.6)} \\
&= \sum_{i=1}^{n} (\|\tfrac{1}{\sqrt{C_i}} \cdot \left(\rho(s)\phi(v_i) - \phi(v_i)\right)\|)')^2 \\
&= \left(\left\|\sum_{i=1}^{n} \tfrac{1}{\sqrt{C_i}} \cdot \left(\rho(s)\phi(v_i) - \phi(v_i)\right)\right\|'\right)^2 && \text{(Por 2.9)} \\
&= \left(\left\|\sum_{i=1}^{n} \rho(s)\tfrac{\phi(v_i)}{\sqrt{C_i}} - \tfrac{\phi(v_i)}{\sqrt{C_i}}\right\|'\right)^2 \\
&= \left(\left\|\sum_{i=1}^{n} \rho(s)\psi(v_i) - \psi(v_i)\right\|'\right)^2 \\
&= \left(\left\|\rho(s)\sum_{i=1}^{n} \psi(v_i) - \sum_{i=1}^{n} \psi(v_i)\right\|'\right)^2 \\
&= \left(\|\rho(s)(\psi(v)) - \psi(v)\|'\right)^2,
\end{aligned}$$

es decir, $\|\rho(s)v - v\|^2 = \left(\|\rho(s)(\psi(v)) - \psi(v)\|'\right)^2$.

Luego, si denotamos por $v' = \psi(v)$ tenemos que

$$\begin{aligned}\min_{\|v\|=1} \max_{s\in S} \|\rho(s)v - v\| &= \min_{\|v\|=1} \max_{s\in S} \|\rho(s)\psi(v) - \psi(v)\|' \\ &= \min_{\|v\|'=1} \max_{s\in S} \|\rho(s)v' - v'\|'.\end{aligned}$$

Por lo tanto, $\kappa'(G, S, \rho, \langle\cdot,\cdot\rangle) = \kappa'(G, S, \rho, \langle\cdot,\cdot\rangle')$. ■

Lema 2.4.5 Si (V, ρ) y (W, ϕ) son representaciones unitarias de G equivalentes, entonces $\kappa'(G, S, \rho) = \kappa'(G, S, \phi)$.

Demostración.

Como (V, ρ) y (W, ϕ) son equivalentes (Definición 1.3.12) existe un $G-$isomorfismo $\psi\colon V \to W$, así que para cada $g \in G$ y $v \in V$, $\psi(\rho(g)v) = \phi(g)\psi(v)$. Sea $\langle\cdot,\cdot\rangle$ un producto interno $G-$invariante sobre W y sea

$$\begin{aligned}\langle\cdot,\cdot\rangle'\colon V \times V &\longrightarrow \mathbb{C} \\ (v_1, v_2) &\longmapsto \langle v_1, v_2\rangle' = \langle\psi(v_1), \psi(v_2)\rangle,\end{aligned}$$

por la Proposición 1.3.14, $\langle\cdot,\cdot\rangle'$ es un producto interno sobre V. Notemos que $\|v\|' = 1$ si y solo si $\|\psi(v)\| = 1$. Si $w = \psi(v)$ tenemos que

$$\begin{aligned}\kappa'(G, S, \rho) &= \min_{\|v\|'=1} \max_{s\in S} \|\rho(s)v - v\|' \\ &= \min_{\|v\|'=1} \max_{s\in S} \|\psi(\rho(s)v - v)\| \\ &= \min_{\|v\|'=1} \max_{s\in S} \|\phi(s)\psi(v) - \psi(v)\| \\ &= \min_{\|w\|=1} \max_{s\in S} \|\phi(s)w - w\| = \kappa'(G, S, \phi).\end{aligned}$$

Por lo tanto, $\kappa'(G, S, \rho)' = \kappa'(G, S, \phi)$. ■

Definición 2.4.6 Sea G un grupo finito no trivial y sea $S \subseteq G$, Definimos

$$\kappa(G, S) = \min_{\rho}\{\kappa'(G, S, \rho)\}. \tag{2.10}$$

El mínimo es sobre todas las representaciones unitarias no triviales irreducibles de G. $\kappa(G, S)$ es llamada la *constante de Kazhdan* del par (G, S).

Observación 2.4.7 Por del Teorema 1.3.33 G tiene sólo un número finito de representaciones irreducibles, salvo equivalencia. Además, el Corolario 1.3.34 nos garantiza la existencia de representaciones irreducibles no triviales. Entonces, por el Lema 2.4.5, la constante de Kazhdan se toma sobre un conjunto finito de valores. Por lo tanto, existe un mínimo.

Observación 2.4.8 La constante de Kazhdan nos dice que para cualquier representación unitaria irreducible y para cualquier vector unitario v sobre el espacio de representación, existe un elemento en S que mueve a v a una distancia a lo menos κ. Más aún κ es la constante más grande que satisface lo anterior.

Observación 2.4.9 Por la Observación 2.4.3 existe un vector unitario $v' \in V$ y $s \in S$ tal que $\|\rho(s)v' - v'\| = \kappa'(G, S, \rho) = \min\limits_{\|v\|=1} \max\limits_{s\in S} \|\rho(s)v - v\|$. Así que para cada $w \in V$

$$\kappa'(G, S, \rho) = \|\rho(s)v' - v'\| \leq \left\|\rho(s)\frac{w}{\|w\|} - \frac{w}{\|w\|}\right\| = \frac{1}{\|w\|} \cdot \|\rho(s)w - w\|.$$

Luego, por la definición de la constante de Kazhdan, $\kappa(G, S) \leq \kappa'(G, S, \rho)$, entonces

$$\kappa(G, S) \leq \frac{1}{\|w\|} \cdot \|\rho(s)w - w\|.$$

Por lo tanto, si $w \in V$ existe $s \in S$ tal que $\|\rho(s)w - w\| \geq \|w\|\, \kappa(G, S)$.

Ejemplo 2.4.10 Sea $G = \mathbb{Z}/5\mathbb{Z}$ y $S = \{\overline{1}\}$. Por el Corolario 1.3.37 para cada $a \in \{1, \ldots, 5\}$, (V, ρ_a) es una representación irreducible de G donde para cada $g \in G$ y $v \in \mathbb{C}$ ocurre que $\rho_a(\overline{g})v = \exp(\frac{2\pi iag}{5})v$. Sea $v \in \mathbb{C}$ con $\|v\| = 1$ y $a \in \{1, \ldots, 5\}$

$$\begin{aligned}\|\rho_a(\overline{1})v - v\| = \|\exp(\tfrac{2\pi iag}{5})v - v\| &= \|(\exp(\tfrac{2\pi iag}{5}) - 1)v\| \\ &= |\exp(\tfrac{2\pi iag}{5}) - 1| \cdot \|v\| \\ &= |\exp(\tfrac{2\pi iag}{5}) - 1|,\end{aligned}$$

donde

$$\begin{aligned}\left|\exp(\tfrac{2\pi iag}{5}) - 1\right| &= |\cos\left(\tfrac{2\pi ag}{5}\right) - 1 + i\sin(\tfrac{2\pi ag}{5})| \\ &= \sqrt{(\cos(\tfrac{2\pi ag}{5}) - 1)^2 + (\sin(\tfrac{2\pi ag}{5}))^2} \\ &= \sqrt{(\cos(\tfrac{2\pi ag}{5})^2 - 2\cos(\tfrac{2\pi ag}{5}) + 1) + (\sin(\tfrac{2\pi ag}{5}))^2} \\ &= \sqrt{2 - 2\cos(\tfrac{2\pi ag}{5})} \\ &= \sqrt{2(1 - \cos(\tfrac{2\pi ag}{5})) \cdot \frac{2}{2}} \\ &= 2\sqrt{\frac{1 - \cos(\frac{2\pi ag}{5})}{2}} \\ &= 2\sin(\tfrac{2\pi ag}{5} \cdot \tfrac{1}{2}) \qquad \left(\sin(\tfrac{\alpha}{2}) = \sqrt{\tfrac{1-\cos(\alpha)}{2}}\right) \\ &= 2\sin(\tfrac{\pi ag}{5}).\end{aligned}$$

Entonces

$$\|\rho_1(\overline{1})v - v\| = 2\sin(\tfrac{\pi}{5}) = 1{,}17 \qquad \|\rho_2(\overline{1})v - v\| = 2\sin(\tfrac{2\pi}{5}) = 1{,}90$$
$$\|\rho_3(\overline{1})v - v\| = 2\sin(\tfrac{3\pi}{5}) = 1{,}90 \qquad \|\rho_4(\overline{1})v - v\| = 2\sin(\tfrac{4\pi}{5}) = 1{,}17$$

$$\|\rho_5(\overline{1})v - v\| = 2\sin(\pi) = 0.$$

Así que $\kappa'(G, S, \rho_1) = \kappa'(G, S, \rho_4) = 1{,}17$, $\kappa'(G, S, \rho_2) = \kappa'(G, S, \rho_3) = 1{,}90$ y $\kappa'(G, S, \rho_5) = 0$. Dado que ρ_5 es la representación trivial tenemos que $\kappa(G, S) = \text{mín}\{\kappa'(G, S, \rho_a) : a \in \{1, \ldots, 4\}\} = 1{,}17$.

La siguiente proposición nos muestra que la constante de Kazhdan no suele ser muy grande.

Proposición 2.4.11 Sea G un grupo finito no trivial y sea $S \subseteq G$. Entonces $\kappa(G, S) \leq 2$.

Demostración.

Sea (V, ρ) una representación unitaria irreducible de G y $\langle \cdot, \cdot \rangle$ un producto interno sobre V, entonces para cada $v \in V$ y $s \in S$

$$\|\rho(s)v\| = \sqrt{\langle \rho(s)v, \rho(s)v \rangle} = \sqrt{\langle v, v \rangle} = \|v\|.$$

Sea u un vector unitario de V y $s \in S$, por la desigualdad del triángulo tenemos que

$$\|\rho(s)v - v\| \leq \|\rho(s)v\| + \|v\| = \|v\| + \|v\| = 1 + 1 = 2.$$

Por lo tanto, $\kappa(G, S) \leq 2$. ■

Ahora que ya conocemos la información básica de la constante de Kazhdan, procederemos a relacionarla con la constante isoperimétrica y la brecha espectral. Pero como la constante de Kazhdan se toma sobre todas las representaciones unitarias no triviales irreducibles de G, nos apoyaremos de la constante $\kappa'(G, S, \widehat{L})$ donde $\widehat{L}$ es la representación regular izquierda restringida a $L_1^2(G)$ (al restringir evitamos la representación trivial) mediante los dos lemas siguientes.

Lema 2.4.12 Sea G un grupo finito no trivial y $S \subseteq G$ con $d = |S|$. Consideremos $\kappa = \kappa(G, S)$ y $\rho\colon G \to GL(V)$ una representación de G que no contiene a la representación trivial. Entonces $\kappa'(G, S, \rho) \geq \frac{\kappa}{\sqrt{d}}$.

Demostración.

Por el Teorema de Maschke 1.3.24 podemos descomponer a V como una suma directa ortogonal de subespacios $G-$invariantes irreducibles $V_1 \oplus V_2 \oplus \cdots \oplus V_n$. Luego sea ρ_i el homomorfismo asociado a V_i, es decir, $\rho_{V_i} = \rho_i$ para cada $i \in \{1, \ldots, n\}$ y sea v un vector unitario con $v = \sum_{i=0}^{n} v_i$ donde $v_i \in V_i$, por la Observación 2.4.9 para cada v_i existe $s_j \in S$ tal que $\|\rho_i(s_i)v_i - v_i\| \geq \kappa\|v_i\|$. Sean $g_1, \ldots, g_d$ los

elementos de S y sea $w_j = \sum_{s_i=g_j} v_i$ (por ejemplo si para v_2 y v_5 tenemos que $s_2 = s_5 = g_1$ entonces $w_1 = \sum_{s_i=g_1} v_i = v_2 + v_5$) podemos escribir a $v = \sum_{j=1}^{d} w_j$. Notemos que si $j, l \in \{1, \ldots, d\}$ con $j \neq l$ entonces $g_j \neq g_l$, así que los s_i que son iguales a g_j no pueden ser los mismos que los de g_l, por consiguiente los v_i que son sumandos de $\sum_{s_i=g_j} v_i$ no pueden ser los mismos que los de $\sum_{s_i=g_l} v_i$ y como $\langle \cdot, \cdot \rangle$ es aditivo y cada v_i es ortogonal a $v_{i'}$ si $i \neq i'$ tenemos que $w_j = \sum_{s_i=g_l} v_i$ es ortogonal a $w_l = \sum_{s_i=g_l} v_i$, es decir, w_j es ortogonal a w_l si $j \neq l$. Como v es un vector unitario

$$1 = \|v\|^2 = \sum_{j=1}^{d} \|w_j\|^2 \leq \sum_{j=1}^{d} \|w_{l_0}\|^2 = d \cdot \|w_{l_0}\|^2,$$

es decir, $\frac{1}{d} \leq \|w_{l_0}\|^2 = \sum_{s_i=g_1} \|v_i\|$ para algún $l_0 \in \{1, \ldots, d\}$.

Luego

$$\begin{aligned}
\|\rho(g_{l_0})v - v\|^2 &= \left\| \rho(g_{l_0}) \sum_{j=1}^{d} w_j - \sum_{j=1}^{d} w_j \right\|^2 \\
&= \left\| \sum_{j=1}^{d} \rho(g_{l_0}) w_j - w_j \right\|^2 \\
&\geq \|\rho(g_{l_0}) w_{l_0} - w_{l_0}\|^2 \\
&= \left\| \rho(g_{l_0}) \sum_{s_i=g_{l_0}} v_i - \sum_{s_i=g_{l_0}} v_i \right\|^2 \\
&= \left\| \sum_{s_i=g_{l_0}} \rho(g_{l_0}) v_i - v_i \right\|^2,
\end{aligned}$$

es decir,

$$\|\rho(g_{l_0})v - v\|^2 \geq \left\| \sum_{s_i=g_{l_0}} \rho(g_{l_0}) v_i - v_i \right\|^2. \tag{2.11}$$

Para cada v_i recordemos que, $\rho(g_{l_0})v_i = \rho_i(g_{l_0})v_i \in V_i$, entonces $\rho(g_{l_0})v_i - v_i \in V_i$ así que para $i \neq i'$, $\langle \rho(g_{l_0})v_i - v_i,\ \rho(g_{l_0})v_{i'} - v_{i'} \rangle = 0$.

Entonces

$$\left\| \sum_{s_i=g_{l_0}} \rho(g_{l_0})v_i - v_i \right\|^2 = \sum_{s_i=g_{l_0}} \|\rho(g_{l_0})v_i - v_i\|^2 = \sum_{s_i=g_{l_0}} \|\rho_i(g_{l_0})v_i - v_i\|^2$$
$$\geq \sum_{s_i=g_{l_0}} \kappa^2 \|v_i\|^2$$
$$= \kappa^2 \sum_{s_i=g_{l_0}} \|v_i\|^2$$
$$= \kappa^2 \|w_{l_0}\|^2$$
$$\geq \frac{\kappa^2}{d},$$

es decir,

$$\left\| \sum_{s_i=g_{l_0}} \rho(g_{l_0})v_i - v_i \right\|^2 \geq \frac{\kappa^2}{d}. \tag{2.12}$$

Luego, de (2.11) y (2.12) tenemos que $\|\rho(g_1)v - v\|^2 \geq \frac{\kappa^2}{d}$. Así que para cada vector unitario v se cumple que $\max_{s\in S} \|\rho(s)v - v\| \geq \frac{\kappa}{\sqrt{d}}$ Entonces $\min\limits_{\|v\|=1} \max\limits_{s\in S} \|\rho(s)v - v\| \geq \frac{\kappa}{\sqrt{d}}$. Por lo tanto, $\kappa'(G, S, \rho) \geq \frac{\kappa}{\sqrt{d}}$. ■

Lema 2.4.13 Sea G un grupo finito no trivial y $S \subseteq G$ con $d = |S|$. Consideremos $\kappa = \kappa(G, S)$, $\widehat{L}$ la restricción de la representación regular izquierda L a $L_1^2(G)$ y $\kappa(G, S, \widehat{L}) = \kappa'(G, S, \widehat{L})$. Entonces $\kappa \geq \widehat{\kappa} \geq \frac{\kappa}{\sqrt{d}}$.

Demostración.

Sea (V, ρ) una representación irreducible no trivial de G, por la demostración del Corolario 1.3.34 tenemos que V es un subespacio invariante de $L_1^2(G)$, entonces si v es un vector unitario de V, tenemos que v es un vector unitario en $L_1^2(G)$ y por definición de $\widehat{\kappa} = \kappa'(G, S, \widehat{L})$ existe $s_0 \in S$ tal que $\|\widehat{L}(s_0)v - v\| \geq \widehat{\kappa}$. Por la Observación 1.3.23, para todo $s \in S$, $\widehat{L}(s)v = \widehat{L}_V(s)v = \rho(s)v$, así que $\widehat{\kappa} \leq \|\rho(s_0)v - v\|$, pero $\kappa = \min\limits_{\|v\|=1} \max\limits_{s\in S} \|\rho(s)V - v\|$ entonces $\kappa \geq \widehat{\kappa}$. Luego, por la demostración del Corolario 1.3.34 tenemos que $L^2(G) = L_1^2(G) \oplus \mathbb{C}f_1$ y que la representación trivial 1 cae en el espacio $\mathbb{C}f_1$, entonces $L \cong \widehat{L} \oplus 1$ y $(L_1^2(G), \widehat{L})$ es una representación de G que no contiene a la representación 1, así que por el Lema 2.4.12 $\widehat{\kappa} = \kappa(G, S, \widehat{L}) \geq \frac{\kappa}{\sqrt{d}}$. Por lo tanto, $\kappa \geq \widehat{\kappa} \geq \frac{\kappa}{\sqrt{d}}$. ■

Proposición 2.4.14 Sea G un grupo finito no trivial y S un conjunto simétrico de generadores de G con $d = |S|$. Consideremos $\kappa = \kappa(G, S)$ y $h = h(Cay(G, S))$. Entonces $h \geq \frac{\kappa^2}{4d}$.

Demostración.

Sea $A \subset G$ tal que $|A| \leq \frac{|G|}{2}$, $B = G \setminus A$ y $\widehat{\kappa} = \kappa(G, S, \widehat{L})$ donde $\widehat{L}$ es la

restricción de L a $L^2_1(G)$. Sea $\widetilde{f} \in L^2(G)$ dada por

$$\widetilde{f}(x) = \begin{cases} |B| & \text{si } x \in A \\ -|A| & \text{si } x \in B. \end{cases}$$

Notemos que $\widetilde{f} \in L^2_1(G)$ ya que

$$\begin{aligned} \langle \widetilde{f}, f_1 \rangle_2 = \sum_{x \in G} \widetilde{f}(x)\overline{f_1(x)} = \sum_{x \in G} \widetilde{f}(x) &= \sum_{x \in A} \widetilde{f}(x) + \sum_{x \in B} \widetilde{f}(x) \\ &= \sum_{x \in A} |B| + \sum_{x \in B} -|A| \\ &= |A|\,|B| + (-|B|\,|A|) \\ &= 0. \end{aligned}$$

Además

$$\begin{aligned} \|\widetilde{f}\|_2^2 = \langle \widetilde{f}, \widetilde{f} \rangle_2 = \sum_{x \in G} |\widetilde{f}(x)|^2 &= \sum_{x \in A} |\widetilde{f}(x)|^2 + \sum_{x \in B} |\widetilde{f}(x)|^2 \\ &= \sum_{x \in A} |B|^2 + \sum_{x \in B} |A|^2 \\ &= |A|\,|B|^2 + |B|\,|A|^2 \\ &= |A|\,|B|(|B| + |A|) \\ &= |A|\,|B||G|, \end{aligned}$$

es decir,

$$\|\widetilde{f}\|_2^2 = |A|\,|B||G|. \tag{2.13}$$

Sea $f = \frac{\widetilde{f}}{\|\widetilde{f}\|_2}$, tenemos que f es un vector unitario en $L^2_1(G)$, así que por la definición de $\widehat{\kappa}$ tenemos que existe $s_0 \in S$ tal que

$$\|\widehat{L}(s_0)f - f\|_2^2 \geq \widehat{\kappa}^2. \tag{2.14}$$

Recordemos que para cada $x, y \in G$, $[\widehat{L}(y)f](x) = [L(y)f](x) = f(y^{-1}x)$ entonces

$$|\widetilde{f}(s_0^{-1}x) - \widetilde{f}(x)| = \begin{cases} & \text{si } s_0^{-1}x \in A \text{ y } x \in B \\ |B| + |A| & \text{o} \\ & \text{si } x \in A \text{ y } s_0^{-1}x \in B, \\ \\ 0 & \text{en otro caso.} \end{cases}$$

Sea $E_{s_0^{-1}}$ el conjunto de aristas en $Cay(G, S)$ de la forma $\{x, s_0^{-1}x\}$ donde $x \in A$ y $s_0^{-1}x \in B$ o $s_0^{-1}x \in A$ y $x \in B$. Entonces

$$\|\widehat{L}(s_0)\widetilde{f} - \widetilde{f}\|_2^2 = \sum_{x \in G} |\widehat{L}(s_0)\widetilde{f}(x) - \widetilde{f}(x)|^2 = \sum_{x \in G} |\widetilde{f}(s_0^{-1}x) - \widetilde{f}(x)|^2.$$

Si s_0^{-1} es el neutro de G, entonces $\|\widehat{L}(s_0)\widetilde{f} - \widetilde{f}\|_2 = 0$. Luego, si s_0^{-1} no es el neutro de G, tenemos que

$$\begin{aligned}\|L(s_0)\widetilde{f} - \widetilde{f}\|_2^2 &= \sum_{x\in G} |\widetilde{f}(s_0^{-1}x) - \widetilde{f}(x)|^2 \\ &= \sum_{\substack{x\in A \\ s_0^{-1}x\in B}} |\widetilde{f}(s_0^{-1}x) - \widetilde{f}(x)|^2 + \sum_{\substack{s_0^{-1}x\in A \\ x\in B}} |\widetilde{f}(s_0^{-1}x) - \widetilde{f}(x)|^2 \\ &= |E_{s_0^{-1}}|(|B| + |A|)^2 \\ &= |E_{s_0^{-1}}|\ |G|^2.\end{aligned}$$

Si s_0^{-1} tiene orden 2, tenemos que s_0^{-1} es su propio inverso, entonces si $x, y \in G$ tales que $s_0^{-1}x = y$ tenemos que $s_0^{-1}y = s_0^{-1}(s_0^{-1}x) = x$, así que $|\widetilde{f}(s_0^{-1}x) - \widetilde{f}(x)| = |\widetilde{f}(s_0^{-1}y) - \widetilde{f}(y)|$, por consiguiente $\|\widehat{L}(s_0)\widetilde{f} - \widetilde{f}\|_2^2 = 2|E_{s_0^{-1}}|\ |G|^2$ ya que habrá sumandos que aparezcan dos veces.

Entonces

$$\|\widehat{L}(s_0)\widetilde{f} - \widetilde{f}\|_2^2 = \begin{cases} 0 & \text{si } s_0^{-1} \text{ es el elemento neutro,} \\ 2|E_{s_0^{-1}}|\ |G|^2 & \text{si } s_0^{-1} \text{ tiene orden 2,} \\ |E_{s_0^{-1}}|\ |G|^2 & \text{si } s_0^{-1} \text{ tiene orden mayor que 2.} \end{cases}$$

Así que $\|\widehat{L}(s_0)\widetilde{f} - \widetilde{f}\|_2^2 \leq 2|E_{s_0^{-1}}|\ |G|^2$, además por (2.14) y (2.13) tenemos que

$$\begin{aligned}\widehat{\kappa}^2 \leq \|\widehat{L}(s_0)f - f\|_2^2 = \frac{\|\widehat{L}(s_0)\widetilde{f} - \widetilde{f}\|_2^2}{\|\widetilde{f}\|_2^2} \\ \leq \frac{2|E_{s_0^{-1}}|\ |G|^2}{|A|\ |B|\ |G|} \\ = \frac{2|E_{s_0^{-1}}|\ |G|}{|A|\ |B|},\end{aligned}$$

y como $|B| \geq \frac{|G|}{2}$, tenemos que

$$\widehat{\kappa}^2 \leq \frac{2|E_{s_0^{-1}}|\ |G|}{|A|\ |B|} \leq \frac{4|E_{s_0^{-1}}|\ |G|}{|A|\ |G|} = \frac{4|E_{s_0^{-1}}|}{|A|}.$$

De ahí que $\dfrac{\widehat{\kappa}^2}{4} \leq \dfrac{|E_{s_0^{-1}}|}{|A|}$.

Recordemos que $E_{s_0^{-1}}$ es el conjunto de aristas de la forma $\{x, s_0^{-1}x\}$ donde $x \in A$ y $s_0^{-1}x \in B$ o bien $s_0^{-1}x \in A$ y $x \in B$, en cualquiera de los dos casos $\{x, s_0^{-1}x\}$ es una arista que tiene un extremo en A y otro extremo en $B = G \setminus A$, así que $E_{s_0^{-1}} \subseteq E(A, G \setminus A)$, de ahí que $|E_{s_0^{-1}}| \leq |E(A, G \setminus A)|$. Entonces

$$\frac{\widehat{\kappa}^2}{4} \leq \frac{|E(A, G \setminus A)|}{|A|}.$$

Luego, por la Definición 2.1.3 de la constante isoperimétrica tenemos que $h \geq \frac{\widehat{\kappa}^2}{4}$. Además, por el Lema 2.4.13 tenemos que $\widehat{\kappa} \geq \frac{\kappa}{\sqrt{d}}$, entonces $h \geq \frac{\widehat{\kappa}^2}{4} \geq \frac{\kappa^2}{4d}$. Por lo tanto, $h \geq \frac{\kappa^2}{4d}$. ■

Proposición 2.4.15 Sea G un grupo finito no trivial y sea S un conjunto simétrico de generadores de G con $d = |S|$. Consideremos $\kappa = \kappa(G, S)$ y λ_2 el segundo valor propio más grande de $Cay(G, S)$, entonces $\kappa \geq \sqrt{\frac{2(d-\lambda_2)}{d}}$.

Demostración.

Sea $\widehat{L}$ es la restricción de L a $L_1^2(G)$ y f un vector unitario en $L_1^2(G)$. Probemos que existe $s_0 \in S$ tal que

$$\|\widehat{L}(s_0)f - f\|_2 \geq \sqrt{\frac{2(d-\lambda_2)}{d}}.$$

Sea $\mathscr{A}$ el operador de adyacencia del grafo $Cay(G, S)$. Por la Observacion 2.3.9 del Teorema Rayleigh-Ritz tenemos que

$$\lambda_2 = \max_{\substack{f \in L_1^2(G) \\ \|f\|_2 = 1}} \langle \mathscr{A}(f), f \rangle_2.$$

Entonces

$$\begin{aligned}
\lambda_2 \geq \langle \mathscr{A}(f), f \rangle_2 &= \sum_{x \in G} \mathscr{A}f(x)\, \overline{f(x)} \\
&= \sum_{x \in G} \sum_{s \in S} f(s^{-1}x)\, \overline{f(x)} \qquad \text{(Por la Observación 1.2.51)} \\
&= \sum_{s \in S} \sum_{x \in G} f(s^{-1}x)\, \overline{f(x)} \\
&= \sum_{s \in S} \langle \widehat{L}(s)f, f \rangle_2, \qquad \text{(Por la Definición 1.3.31)}
\end{aligned}$$

dado que $\langle \mathscr{A}(f), f \rangle_2$ es un real, tenemos que $\sum_{s \in S} \langle \widehat{L}(s)f, f \rangle_2 = \sum_{s \in S} Re(\langle \widehat{L}(s)f, f \rangle_2)$, es decir, $\lambda_2 \geq \sum_{s \in S} Re(\langle \widehat{L}(s)f, f \rangle_2)$. Además, como S es un conjunto finito tenemos

que $\{Re(\langle \widehat{L}(s)f, f\rangle_2) : s \in S\}$ también lo es. Por lo tanto, existe $s_0 \in S$ tal que para todo $s \in S$, $Re(\langle \widehat{L}(s)f, f\rangle_2) \geq Re(\langle \widehat{L}(s_0)f, f\rangle_2)$, entonces

$$\begin{aligned} d - \lambda_2 \leq d - \sum_{s\in S} Re(\langle \widehat{L}(s)f, f\rangle_2) &\leq d - \sum_{s\in S} Re(\langle \widehat{L}(s_0)f, f\rangle_2) \\ &= d - d[Re(\langle \widehat{L}(s_0)f, f\rangle_2)] \\ &= d[1 - Re(\langle \widehat{L}(s_0)f, f\rangle_2)]. \end{aligned}$$

Así que $s_0 \in S$ tal que

$$1 - Re(\langle \widehat{L}(s_0)f, f\rangle_2) \geq \frac{d-\lambda_2}{d}.$$

Luego

$$\begin{aligned} \|\widehat{L}(s_0)f - f\|_2 &= \sqrt{\langle \widehat{L}(s_0)f - f, \widehat{L}(s_0)f - f\rangle_2} \\ &= \sqrt{\langle \widehat{L}(s_0)f, \widehat{L}(s_0)f\rangle_2 - \langle \widehat{L}(s_0)f, f\rangle_2 - \langle f, \widehat{L}(s_0)f\rangle_2 + \langle f, f\rangle_2} \\ &= \sqrt{1 - \langle \widehat{L}(s_0)f, f\rangle_2 - \overline{\langle f, \widehat{L}(s_0)f\rangle_2} + 1} \\ &= \sqrt{2 - 2Re(\langle \widehat{L}(s_0)f, f\rangle_2)} \\ &= \sqrt{2[1 - Re(\langle \widehat{L}(s_0)f, f\rangle_2)]} \\ &\geq \sqrt{2\left(\frac{d-\lambda_2}{d}\right)}, \end{aligned}$$

es decir, $s_0 \in S$ tal que $\|\widehat{L}(s_0)f - f\|_2 \geq \sqrt{\frac{2(d-\lambda_2)}{d}}$, entonces

$$\max_{s\in S} \|\widehat{L}(s)f - f\|_2 \geq \|\widehat{L}(s_0)f - f\|_2 \geq \sqrt{\frac{2(d-\lambda_2)}{d}},$$

para cada $f \in L_1^2(G)$ unitario, por consiguiente

$$\widehat{\kappa} = \min_{\substack{f\in L_1^2(G) \\ \|f\|_2=1}} \max_{s\in S} \|\widehat{L}(s)f - f\|_2 \geq \|L(s_0)f - f\|_2 \geq \sqrt{\frac{2(d-\lambda_2)}{d}},$$

es decir, $\widehat{\kappa} \geq \sqrt{\frac{2(d-\lambda_2)}{d}}$, luego por el Lema 2.4.13 $\kappa \geq \widehat{\kappa} \geq \sqrt{\frac{2(d-\lambda_2)}{d}}$. Por lo tanto, $\kappa \geq \sqrt{\frac{2(d-\lambda_2)}{d}}$. ■

Mediante las relaciones, mostradas en las Proposiciones 2.4.14 y 2.4.15, entre la constante de Kazhdan, la constante isoperimétrica y la brecha espectral, podemos caracterizar una familia de grafos expanders mediante la constante de Kazhdan, a través del siguiente Teorema.

Teorema 2.4.16 Sea d un entero positivo y sea (G_n) una sucesión de grupos con $|G_n| \to \infty$ cuando $n \to \infty$. Para cada $n \in \mathbb{N}$ sea S_n un conjunto simétrico de generadores de G tal que $|S_n| = d$. Entonces $(Cay(G_n, S_n))$ es una familia de grafos expanders si y solo si existe $\varepsilon > 0$ tal que para cada $n \in \mathbb{N}$ se cumple que $\kappa(G_n, S_n) \geq \varepsilon$.

Demostración.

Si $(Cay(G_n, S_n))$ es una familia de grafos expanders, por el Teorema 2.3.18 existe $\varepsilon > 0$ tal que para cada $n \in \mathbb{N}$ se cumple que $d - \lambda_2(Cay(G_n, S_n)) \geq \varepsilon$, entonces

$$\sqrt{\frac{2(d - \lambda_2(Cay(G_n, S_n)))}{d}} \geq \sqrt{\frac{2\varepsilon}{d}} > 0,$$

y por la Proposición 2.4.15 tenemos que

$$\kappa(G_n, S_n) \geq \sqrt{\frac{2(d - \lambda_2(Cay(G_n, S_n)))}{d}},$$

así que $\kappa(G_n, S_n) \geq \sqrt{\frac{2\varepsilon}{d}}$. Por lo tanto, si $\varepsilon' = \sqrt{\frac{2\varepsilon}{d}}$ tenemos que para cada $n \in \mathbb{N}$ se cumple que $\kappa(G_n, S_n) \geq \varepsilon'$. Ahora, si existe $\varepsilon > 0$ tal que para cada $n \in \mathbb{N}$ se cumple que $\kappa(G_n, S_n) \geq \varepsilon$, entonces

$$\frac{\kappa(G_n, S_n)^2}{4d} \geq \frac{\varepsilon^2}{4d} > 0,$$

y por la Proposición 2.4.14 tenemos que

$$h(Cay(G_n, S_n)) \geq \frac{\kappa(G_n, S_n)^2}{4d},$$

de ahí que $h(Cay(G_n, S_n)) \geq \frac{\varepsilon^2}{4d}$. Entonces, si $\varepsilon' = \frac{\varepsilon^2}{4d}$ tenemos que para cada $n \in \mathbb{N}$ se cumple que $h(Cay(G_n, S_n)) \geq \varepsilon'$, es decir, $(h(Cay(G_n, S_n)))$ está acotada lejos de cero. Por lo tanto, $(Cay(G_n, S_n))$ es una familia de grafos expanders.

■

Capítulo 3
Construcción de expanders y algunas familias de grafos no-expander

Ahora que conocemos qué es una familia de grafos expanders, entendemos que calcular cualquier constante estudiada en el capitulo 2 a una familia de grafos es una tarea laboriosa, por consiguiente dar construcciones explicitas de familias de grafos expanders resulta complicado, tanto así que se han dado resultados de cómo algunas familias de grafos no generan familias de expanders.

En este capitulo daremos un resumen de las primeras construcciones de grafos expanders, así como un método de construcción a partir de grafos de Ramanujan y por último exhibiremos algunas familias de grafos de Cayley que no forman familias de grafos expanders.

3.1. Construcción de Margulis

La primera construcción explícita de familias de grafos expanders fue dada por Margulis [53] quien construyó una familia de biexpanders 5−regular. Cabe destacar que él en un principio estaba interesado en construir familias de concentradores que son una familia de grafos que contiene grafos biexpanders.

En esta sección mostraremos un resumen de la construcción original que se presenta en su articulo "*Explicit Construction of Concentrators*" [53], así como algunas construcciones que se dieron a base del trabajo de Margulis.

Definición 3.1.1 Sea X un grafo bipartito con bipartición (I, O) tal que $|I| = |O|$. Sean c y α números positivos tales que $c > 1$ y $\alpha < 1$, decimos que X es un $(\alpha, c)-$concentrador si para cada $A \subset I$ con $|A| \leq \alpha|I|$ se cumple que

$$|\partial A| \geq c|A|.$$

Observación 3.1.2 Cuando $\alpha = \frac{1}{2}$ tenemos la Definición 2.2.14 de grafo biexpander, es decir, X es un $(c-1)-$biexpander.

Construcción original de Margulis: Sea m un entero positivo, consideremos $I_m = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$ y $O_m = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$, donde $\frac{\mathbb{Z}}{m\mathbb{Z}}$ es el grupo de los enteros módulo m. Definimos el grafo bipartito X_m con bipartición (I_m, O_m) de manera que cada elemento $(x, y) \in I_m$ esta conectado a los siguientes cinco elementos de O_m:

$$1)(x,y) \qquad 2)(x+1,y) \qquad 3)(x,y+1) \qquad 4)(x,x+y) \qquad 5)(-y,x)$$

Ejemplo 3.1.3 Tomemos $m = 2$, entonces X_2 es un grafo bipartito donde cada partición cuenta con cuatro elementos, los cuales están conectados a los elementos mostrados en la Tabla 3.1.

Vértice	Vecinos				
(x,y)	(x,y)	$(x+1,y)$	$(x,y+1)$	$(x,x+y)$	$(-y,x)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(1,1)$	$(0,1)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(1,0)$	$(1,1)$

Tabla 3.1

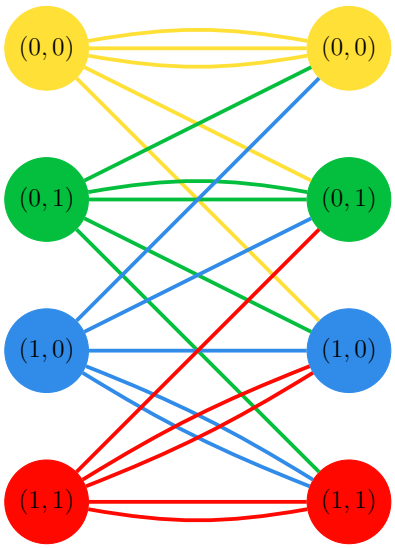


Figura 3.1: X_2.

Para este tipo de grafos, Margulis demuestra el siguiente Teorema.

Teorema 3.1.4 ([53], Teorema 2.3) Existe una constante positiva d tal que para cada entero $m > 1$, X_m es un $(1 + d(1 - \alpha), \alpha)-$concentrador para cualquier α que satisfaga que $0 < \alpha < 1$.

Observación 3.1.5 Desafortunadamente el valor de d es desconocido, Margulis solo prueba su existencia.

Observación 3.1.6 Cuando $\alpha \leq \frac{1}{2}$, tenemos que X_m satisface la Definción 2.2.10, es decir X_m un $(m^2, 5, d)-$biexpander.

Ejemplo 3.1.7 En el Ejemplo 3.1.3 construimos a X_2, para calcular su constante de expansión de vértices, tomemos un subconjunto A de I_2 con $|A| \leq \frac{4}{2} = 2$ y veamos que ocurre con ∂A.

- Caso $|A| = 1$

A	∂A	$\lvert\partial A\rvert$
$\{(0,0)\}$	$\{(0,0),(1,0),(0,1)\}$	3
$\{(0,1)\}$	$\{(0,1),(1,1),(0,0),(1,0)\}$	4
$\{(1,0)\}$	$\{(1,0),(0,0),(1,1),(0,1)\}$	4
$\{(1,1)\}$	$\{(1,1),(0,1),(1,0)\}$	3

Estimemos el valor de la constante de expansión de vértices c de la definición de biexpander 2.2.10.

- Si $|\partial A| = 3$,
$$3 = |\partial A| \geq [1 + c(1 - \tfrac{1}{4})]1 = 1 + \frac{3c}{4}$$
así que $c \leq \frac{8}{3}$.
- Si $|\partial A| = 4$,
$$4 = |\partial A| \geq [1 + c(1 - \tfrac{1}{4})]1 = 1 + \frac{3c}{4}$$
así que $c \leq 4$.

- Caso $|A| = 2$

Para tomar 2 elementos de un conjunto de 4 elementos hay 6 posibles formas

A	∂A	$\lvert\partial A\rvert$
$\{(0,0),(0,1)\}$	$\{(0,0),(1,0),(0,1),(1,1)\}$	4
$\{(0,0),(1,0)\}$	$\{(0,0),(1,0),(0,1),(1,1)\}$	4
$\{(0,0),(1,1)\}$	$\{(0,0),(1,0),(0,1),(1,1),\}$	4
$\{(0,1),(1,0)\}$	$\{(0,1),(1,1),(0,0),(1,0)\}$	4
$\{(0,1),(1,1)\}$	$\{(0,1),(1,1),(0,0),(1,0)\}$	4
$\{(1,0),(1,1)\}$	$\{(1,0),(0,0),(1,1),(0,1),\}$	4

Estimemos el valor de la constante de expansión c de la definición de biexpander 2.2.10
$$4 = |\partial A| \geq [1 + c(1 - \tfrac{2}{4})]2 = [1 + \tfrac{c}{2}]2,$$
es decir, $2 \geq 1 + \frac{c}{2}$ así que $c \leq 2$.

Entonces $c = \text{mín}\{\frac{8}{3}, 4, 2\} = 2$. Por lo tanto, X_2 es un $(4, 5, 2)-$biexpander.

Para concluir la revisión de esta construcción daremos un esbozo de las herramientas que utilizó Margulis para la demostración de Teorema 3.1.4.

Sea H_z el grupo multiplicativo de las matrices con entradas enteras de la forma

$$\begin{pmatrix} a & b & u \\ c & d & v \\ 0 & 0 & 1 \end{pmatrix}$$

con determinante 1. Y sea S_z el grupo multiplicativo de las matrices con entradas enteras de la forma

$$\begin{pmatrix} 1 & 0 & u \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix}.$$

Luego, para cada entero positivo m definimos T_m como una función biyectiva que va de H_z a una transformación lineal de $\frac{\mathbb{Z}}{\mathbb{Z}m} \times \frac{\mathbb{Z}}{\mathbb{Z}m}$ dada por

$$[T_m(h)](x, y) = (ax + by + u, cx + dy + v)$$

para cada $(x, y) \in \frac{\mathbb{Z}}{\mathbb{Z}m} \times \frac{\mathbb{Z}}{\mathbb{Z}m}$ donde $h = \begin{pmatrix} a & b & u \\ c & d & v \\ 0 & 0 & 1 \end{pmatrix}$.

Posteriormente, a cada una de estas funciones biyectivas se le asocia un operador lineal en $L^2(I_m)$ denotado por $\widetilde{T}_m(h)$ de la siguiente manera, si $f \in L^2(I_m)$ entonces para cualquier $(x, y) \in I_m$

$$[\widetilde{T}_m(h)]f(x, y) = f\left([T_m^{-1}(h)](x, y)\right).$$

Así que

$$\begin{aligned} \widetilde{T}_m \colon H_z &\longrightarrow GL(L^2(I_m)) \\ h &\longmapsto \widetilde{T}_m(h) \end{aligned}$$

donde

$$\begin{aligned} \widetilde{T}_m(h) \colon L^2(I_m) &\longrightarrow L^2(I_m) \\ f &\longmapsto [\widetilde{T}_m(h)]f \end{aligned}$$

y

$$\begin{aligned} [\widetilde{T}_m(h)]f \colon I_m &\longrightarrow I_m \\ (x, y) &\longmapsto [\widetilde{T}_m(h)]f(x, y) = f\left([T_m^{-1}(h)](x, y)\right). \end{aligned}$$

Se prueba que $\widetilde{T}_m$ es un homomorfismo de grupos, por lo que $(L^2(I_m), \widetilde{T}_m)$ es una representación de H_z, más aún, cumple con ser unitaria. Por último, una herramienta en la que se basa fuertemente la prueba es la propiedad (T), la cual abordaremos brevemente en la siguiente sección, esta propiedad es aplicada al grupo H_z, su subgrupo S_z y la representación $(L^2(I_m), \widetilde{T}_m)$.

3.1.1. Construcción de Angluin

En 1979, Angluin [6] escribió unas notas acerca de la prueba de Margulis y dio una construcción más simple que satisface el Teorema 3.1.4, mediante el siguiente Lema.

Lema 3.1.8 ([6], Lema 1) Sea $\{h_1, h_2, \dots h_k\} \subseteq H_z$ que genera a H_z. Para cada entero m mayor que 1, definimos G_m al grafo obtenido de conectar cada $(x, y) \in I_m$ con los siguientes $k+1$ elementos de O_m :

$$(x, y),\ [T_m(h_1)](x, y),\ [T_m(h_2)](x, y),\ \dots,\ [T_m(h_k)](x, y).$$

Entonces el Teorema 3.1.4 se cumple para G_m en lugar de X_m.

Sean

$$h_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{y} \qquad h_2 = \begin{pmatrix} 0 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Angluin muestra que $\{h_1, h_2\}$ generan al grupo de matrices H_z. Obteniendo así una construcción de grado 3 que satisface el Teorema 3.1.4.

Por lo tanto, para cada entero positivo m, G_m es un grafo $(m^2, 3, d)-$biexpander donde cada vértice (x, y) de I_m esta conectado con los siguientes tres vértices de O_m

$$1)(x, y) \qquad 2)(x + y, y) \qquad 3)(y + 1, -x).$$

Ejemplo 3.1.9 Tomemos $m = 2$, entonces G_2 es un grafo bipartito donde cada partición cuenta con cuatro elementos, los cuales están conectados a los elementos mostrados en la Tabla 3.2.

Vértice	Vecinos		
(x, y)	(x, y)	$(x + y, y)$	$(y + 1, -x)$
$(0, 0)$	$(0, 0)$	$(0, 0)$	$(1, 0)$
$(0, 1)$	$(0, 1)$	$(1, 1)$	$(0, 0)$
$(1, 0)$	$(1, 0)$	$(1, 0)$	$(1, 1)$
$(1, 1)$	$(1, 1)$	$(0, 1)$	$(0, 1)$

Tabla 3.2

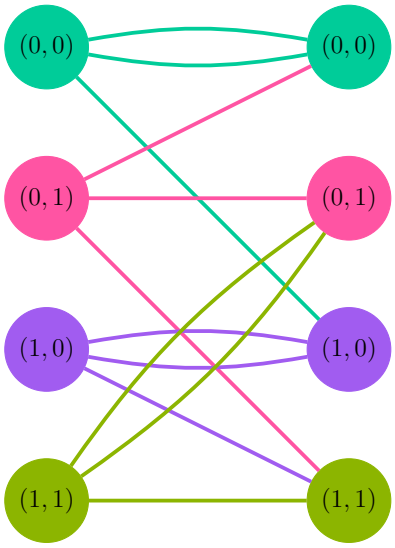


Figura 3.2: G_2.

3.1.2. Construcciones de Gabber y Galil

En 1981, Gabber y Galil [32] proponen dos construcciones similares a la de Margulis, en las cuales se conoce la constante de expansión de vértices.

Sea m un entero positivo, consideremos $I_m = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} = O_m$, donde $\frac{\mathbb{Z}}{m\mathbb{Z}}$ es el grupo de los enteros módulo m.

Construcción 1: Definimos el grafo bipartito Y_m con bipartición (I_m, O_m) de manera que cada elemento $(x, y) \in I_m$ esta conectado a las siguientes cinco permutaciones de O_m:

$$\begin{aligned}\sigma_0(x, y) =&(x, y),\\ \sigma_1(x, y) =&(x, x + y),\\ \sigma_2(x, y) =&(x, x + y + 1),\\ \sigma_3(x, y) =&(x + y, y),\\ \sigma_4(x, y) =&(x + y + 1, y).\end{aligned}$$

Construcción 2: Definimos el grafo bipartito $\widetilde{Y}_m$ con bipartición (I_m, O_m) de manera que cada elemento $(x, y) \in I_m$ esta conectado a las siguientes siete permutaciones de O_m:

$$\begin{aligned}\sigma_0(x, y) =&(x, y),\\ \sigma_1(x, y) =&(x, y + 2x),\\ \sigma_2(x, y) =&(x, y + 2x + 1),\\ \sigma_3(x, y) =&(x, y + 2x + 2),\end{aligned}$$

$$\begin{aligned}\sigma_4(x,y) =&(x+2y,y),\\ \sigma_5(x,y) =&(x+2y+1,y),\\ \sigma_6(x,y) =&(x+2y+2,y).\end{aligned}$$

Ejemplo 3.1.10 Veamos los primeros tres elementos de la familia (Y_m).

Para $m=2$ tenemos que Y_2 es un grafo bipartito donde cada partición tiene cuatro elementos, los cuales están conectados a los elementos mostrados en la Tabla 3.3.

Vértice	Vecinos				
(x,y)	(x,y)	$(x,x+y)$	$(x,x+y+1)$	$(x+y,y)$	$(x+y+1,y)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,1)$	$(0,0)$	$(1,0)$
$(0,1)$	$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(0,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,0)$	$(1,0)$	$(0,0)$
$(1,1)$	$(1,1)$	$(1,0)$	$(1,1)$	$(0,1)$	$(1,1)$

Tabla 3.3

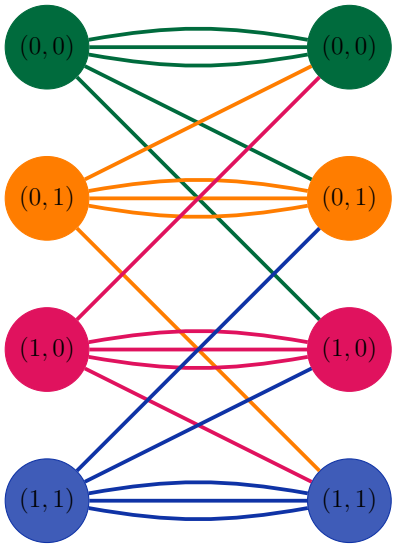


Figura 3.3: Y_2.

Para $m=3$ tenemos que Y_3 es un grafo bipartito donde cada partición tiene nueve elementos, los cuales están conectados a los elementos mostrados en la Tabla 3.4.

Vértice	Vecinos				
(x, y)	(x, y)	$(x, x+y)$	$(x, x+y+1)$	$(x+y, y)$	$(x+y+1, y)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,1)$	$(0,0)$	$(1,0)$
$(0,1)$	$(0,1)$	$(0,1)$	$(0,2)$	$(1,1)$	$(2,0)$
$(0,2)$	$(0,2)$	$(0,2)$	$(0,0)$	$(2,2)$	$(0,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,0)$	$(2,1)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(2,1)$	$(0,1)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(1,1)$
$(2,0)$	$(2,0)$	$(2,2)$	$(2,0)$	$(2,0)$	$(0,2)$
$(2,1)$	$(2,1)$	$(2,0)$	$(2,1)$	$(0,1)$	$(1,2)$
$(2,2)$	$(2,2)$	$(2,1)$	$(2,2)$	$(1,2)$	$(2,2)$

Tabla 3.4

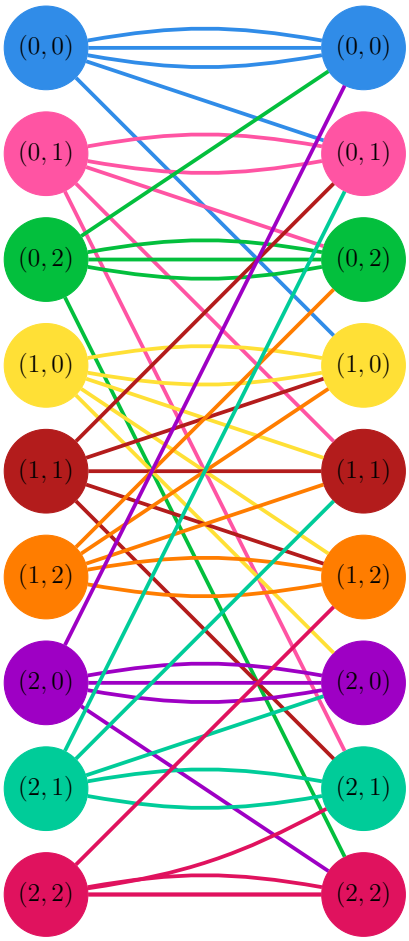


Figura 3.4: Y_3.

Y para $m = 4$ tenemos que Y_4 es un grafo bipartito donde cada partición tiene dieciséis elementos, los cuales están conectados a los elementos mostrados en la Tabla 3.5.

Vértice	Vecinos				
(x, y)	(x, y)	$(x, x+y)$	$(x, x+y+1)$	$(x+y, y)$	$(x+y+1, y)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,1)$	$(0,0)$	$(1,0)$
$(0,1)$	$(0,1)$	$(0,1)$	$(0,2)$	$(1,1)$	$(2,1)$
$(0,2)$	$(0,2)$	$(0,2)$	$(0,3)$	$(2,2)$	$(3,2)$
$(0,3)$	$(0,3)$	$(0,3)$	$(0,0)$	$(3,3)$	$(0,3)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,0)$	$(2,0)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,3)$	$(2,1)$	$(3,1)$
$(1,2)$	$(1,2)$	$(1,3)$	$(1,0)$	$(3,2)$	$(0,2)$
$(1,3)$	$(1,3)$	$(1,0)$	$(1,1)$	$(0,3)$	$(1,3)$
$(2,0)$	$(2,0)$	$(2,2)$	$(2,3)$	$(2,0)$	$(3,0)$
$(2,1)$	$(2,1)$	$(2,3)$	$(2,0)$	$(3,1)$	$(0,1)$
$(2,2)$	$(2,2)$	$(2,0)$	$(2,1)$	$(0,2)$	$(1,2)$
$(2,3)$	$(2,3)$	$(2,1)$	$(2,2)$	$(1,3)$	$(2,3)$
$(3,0)$	$(3,0)$	$(3,3)$	$(3,0)$	$(3,0)$	$(0,0)$
$(3,1)$	$(3,1)$	$(3,0)$	$(3,1)$	$(0,1)$	$(1,1)$
$(2,2)$	$(2,2)$	$(3,1)$	$(3,2)$	$(1,2)$	$(2,2)$
$(3,3)$	$(3,3)$	$(3,2)$	$(3,3)$	$(2,3)$	$(3,3)$

Tabla 3.5

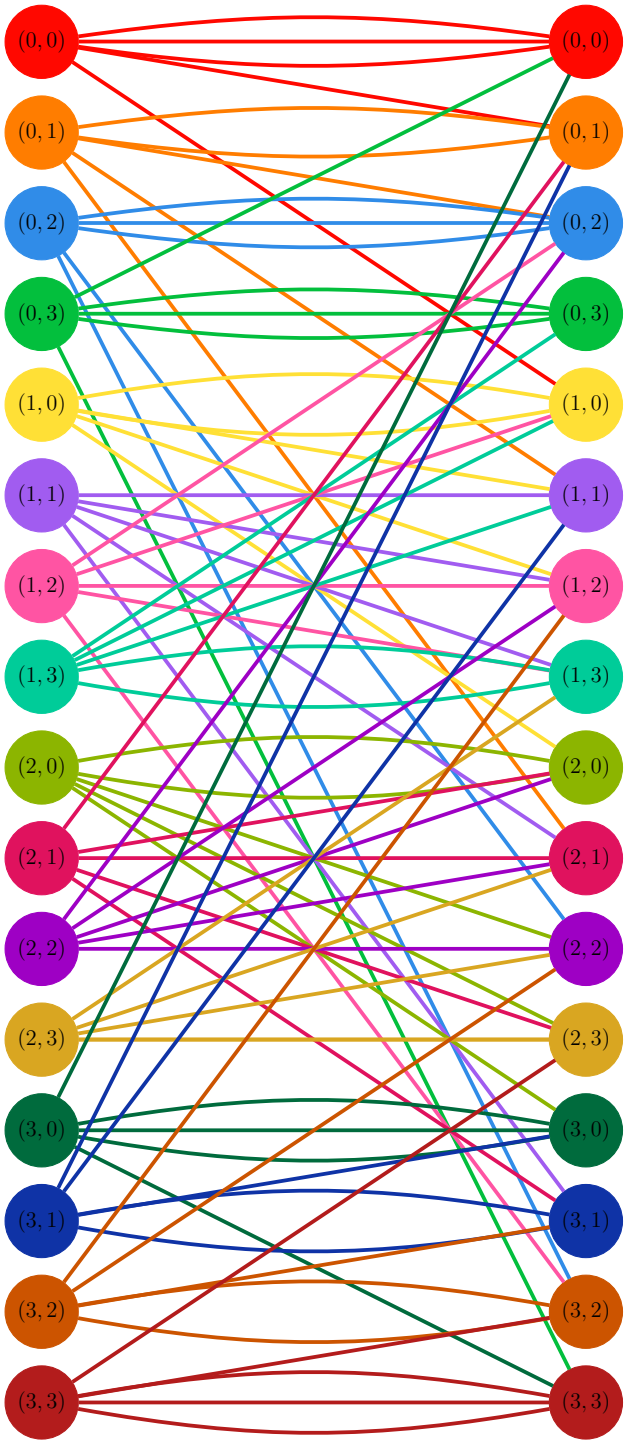

(0, 0)
(0, 1)
(0, 2)
(0, 3)
(1, 0)
(1, 1)
(1, 2)
(1, 3)
(2, 0)
(2, 1)
(2, 2)
(2, 3)
(3, 0)
(3, 1)
(3, 2)
(3, 3)
(0, 0)
(0, 1)
(0, 2)
(0, 3)
(1, 0)
(1, 1)
(1, 2)
(1, 3)
(2, 0)
(2, 1)
(2, 2)
(2, 3)
(3, 0)
(3, 1)
(3, 2)
(3, 3)

Figura 3.5: Y_4.

Para este tipo de grafos Gabber y Galil demuestran el siguiente Teorema:

Teorema 3.1.11 ([32], Teorema 2) Sea m un entero positivo, Y_m es un $(m^2, 5, \frac{2-\sqrt{3}}{4})$-biexpander y $\widetilde{Y}_m$ es un $(m^2, 7, \frac{2-\sqrt{3}}{2})-$biexpander.

A partir de éstas construcciones Jimbo y Maruoka [42], mostraron que para cada entero $m > 1$ los grafos bipartitos $8-$regulares T_m con bipartición (I_m, O_m) donde cada elemento $(x, y) \in I_m$ esta conectado a las permutaciones $\sigma_i(x, y)$ y $\sigma_i^{-1}(x, y)$ con $i \in \{1, 2, 4, 5\}$ de la construcción 3.1.2, su segundo valor propio más grande del grafo $\lambda_2 \leq 5\sqrt{2}$. Y en base a este resultado Alon, Gabber y Milman [3] crearon familias 9-regulares y $12-$regulares en donde se da una mejor estimación de la constante de expansión.

3.2. Propiedad (T) de Kazhdan

En 1967 Kazhdan creó una propiedad para grupos localmente compactos definida en términos de representaciones unitarias llamada la Propiedad (T). En esta sección utilizaremos está propiedad para construir familias de grafos expanders, para ello haremos uso de la definición de la Propiedad (T) mediante la constante de Kazhdan (Definición 2.4.6), para ver otras definiciones y más resultados de la Propiedad (T) consulte [12], [15], [29], [35] y [47].

Definición 3.2.1 Un *grupo topológico* es una terna $(G, \cdot, \tau)$ donde:

i) $(G, \cdot)$ es un grupo.

ii) (G, τ) es un espacio topológico.

iii) Las funciones

$$\begin{aligned} \cdot \colon G \times G &\longrightarrow G & \qquad \iota \colon G &\longrightarrow G \\ (x, y) &\longmapsto xy & \qquad x &\longmapsto x^{-1} \end{aligned}$$

son continuas.

iv) $\{e\}$ es un conjunto cerrado.

Observación 3.2.2 Una manera práctica de expresar *iii)* es pedir la continuidad de la función

$$\begin{aligned} \phi \colon G \times G &\longrightarrow G \\ (x, y) &\longmapsto xy^{-1}. \end{aligned}$$

Ejemplos 3.2.3

1) $(\mathbb{R}, +)$ con la topología euclidiana.

2) $(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$ con la topología inducida de $\mathbb{R}$.

3) Cualquier grupo G con la topología discreta.

4) El grupo lineal general $GL(n, \mathbb{C})$, es decir, el grupo multiplicativo de las matrices invertibles de tamaño $n \times n$ con coeficientes en $\mathbb{C}$, con la topología generada por la métrica

$$d(A, B) = \left(\sum_{i,j=1}^{n} |a_{ij} - b_{ij}|^2 \right)^{1/2}$$

y sus subgrupos $O(n)$ el grupo de las matrices ortogonales y $SL(n, \mathbb{C})$ el grupo lineal especial.

Definición 3.2.4 Un grupo topológico G cuya topología es localmente compacta se dice que es un *grupo localmente compacto*.

Observación 3.2.5 De ahora en adelante todos los grupos topológicos se consideran localmente compactos, a menos que se indiqué lo contrario.

En un grupo topológico G las representaciones se suelen definir como homomorfismos de grupos que van de G en un espacio de Hilbert H que son fuertemente continuas, es decir $\rho\colon G \to L^2(G)$ es una representación unitaria de G si ρ es un homomorfismo de grupos y para cada $f \in L^2(G)$ la función $g \mapsto \rho(g)f$ es una función continua [12].

Nosotros vamos a trabajar con el espacio de Hilbert $L^2(G)$ que en esta sección lo debemos considerar como $L^2(G, \mu)$ donde μ es la medida de Haar. La representación regular izquierda (Definición 1.3.31) es una representación unitaria para un grupo topológico localmente compacto G en el espacio de Hilbert $L^2(G)$. La prueba de esta afirmación se puede consultar en el Ejemplo 2 de la página 135 de [10].

Dado que los grupos topológicos no son el objeto de estudio de este trabajo no los desarrollaremos a profundidad, si el lector desea conocer más le recomendamos ver [17], [23] y [10]. De aquí en adelante solo basta recordar qué es un grupo topológico y la definición de la constante de Kazhdan.

Definición 3.2.6 Sea G un grupo topológico, decimos que G tiene la *Propiedad (T)* si existe un conjunto compacto Q tal que $\kappa(G, Q) > 0$.

Observación 3.2.7 Como todo conjunto finito es compacto, tenemos que G tiene la Propiedad (T) si existe un conjunto finito Q tal que $\kappa(G, Q) > 0$ (ver Definición 2.4.6 de la constante de Kazhdan).

Observación 3.2.8 Al conjunto Q de la Definición 3.2.6 se le conoce como conjunto de Kazhdan.

Proposición 3.2.9 Sea G un grupo topológico finitamente generado por S. Si G que tiene la Propiedad (T) entonces $\kappa(G,S) > 0$.

Demostración.

Supongamos que $\kappa(G,S) = 0$, por definición tenemos que para cada representación unitaria no trivial ρ se cumple que $\|\rho(s)v - v\| = 0$ para cada vector unitario v y para cada $s \in S$. Por lo que $\rho(s)v = v$ para cada vector unitario v y para cada $s \in S$. Dado que ρ es un homomorfismo de grupos tenemos que para cada vector unitario v

$$\rho(s^r)v = \rho(s)^r v = \underbrace{\rho(s) \circ \cdots \circ \rho(s)}_{r-veces} v = v,$$

es decir, para cada vector unitario v, $s \in S$ y $r \in \mathbb{Z}$, $\rho(s^r)v = v$.

Sean $s_1, \ldots, s_l$ los elementos de S, Q el conjunto de Kazhdan de G y $q \in Q$, entonces $q = s_1^{r_1} s_2^{r_2} \cdots s_l^{r_l}$ con $r_1, \ldots r_l \in \mathbb{Z}$. Entonces para cada vector unitario v se cumple que

$$\begin{aligned} \|\rho(q)v - v\| = \|\rho(s_1^{r_1} s_2^{r_2} \cdots s_l^{r_l})v - v\| &= \|\rho(s_1^{r_1})\rho(s_2^{r_2}) \cdots \rho(s_l^{r_l})v - v\| \\ &= \|v - v\| \\ &= 0, \end{aligned}$$

es decir, para cada representación unitaria no trivial ρ se cumple que $\|\rho(q)v - v\| = 0$ para cada vector unitario v y para cada $q \in Q$, entonces $\kappa(G,Q) = 0$ lo que contradice el hecho de que G tenga la Propiedad de (T). Por lo tanto, $\kappa(G,S) > 0$. ■

Como mencionamos al inició del capítulo, la Propiedad (T) fue utilizada por Margulis para la existencia de familias de grafos expanders, posteriormente Lubotzky profundizó más en el estudio de la Propiedad (T) logrando una construcción de familias de grafos expanders.

Proposición 3.2.10 ([47], Proposición 3.3.1.) Sea G un grupo finitamente generado que tiene la Propiedad (T). Consideremos (N_n) la familia de subgrupos normales de G de índice finito tales que $|G/N_n| \to \infty$ cuando $n \to \infty$ y S un conjunto simétrico de generadores de G tal que $|S| = d$. Si π_n es la proyección canónica de G/N_n. Entonces la familia $Cay(G/N_n, \pi_n(S))$ es una familia de grafos expanders.

Demostración.

Sea $N_n \in (N_n)$, denotemos por $H_n = G/N_n$. Consideremos la representación regular de H_n, que es $(L^2(H_n), L)$. Por la prueba del Corolario 1.3.34 podemos descomponer a $L^2(H_n)$ como $L^2(H_n) \cong L^2_1(H_n) \oplus \mathbb{C}f_1$, además se probó que el espacio de las funciones constantes $\mathbb{C}f_1$ le corresponde la representación trivial,

por lo que $L^2_1(H_n)$ contiene representaciones no triviales. Sea $A \subset H_n$ tal que $|A| \leq \frac{|H_n|}{2}$ y $B = H_n \setminus A$. Consideremos la siguiente función

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

Notemos que $f \in L^2_1(H_n)$ ya que

$$\begin{aligned} \langle f, f_1 \rangle = \sum_{x \in H_n} f(x) &= \sum_{x \in A} |B| + \sum_{x \in B} -|A| \\ &= |A|\,|B| - |B|\,|A| = 0. \end{aligned}$$

Además

$$\begin{aligned} \|f\|_2^2 = \sum_{x \in H_n} |f(x)|^2 &= \sum_{x \in A} |B|^2 + \sum_{x \in B} (-|A|)^2 \\ &= |A|\,|B|^2 + |B|\,|A|^2 \\ &= |B|\,|A|\,|H_n|. \end{aligned}$$

Como G tiene la Propiedad (T), por la Observación 2.4.9 tenemos que para f existe algún $s \in S$ tal que

$$\|L(s)f - f\|_2 \geq \kappa(G, S)\|f\|_2. \tag{3.1}$$

Notemos que

$$[L(s)f](x) = f(s^{-1}x) \begin{cases} |B| & \text{si } s^{-1}x \in A \\ -|A| & \text{si } s^{-1}x \in B. \end{cases}$$

Entonces

$$\begin{aligned} ([L(s)f] - f)(x) = f(s^{-1}x) - f(x) &= \begin{cases} |B| + |A| & \text{si } s^{-1}x \in A \text{ y } x \in B \\ -(|B| + |A|) & \text{si } s^{-1}x \in B \text{ y } x \in A \\ 0 & \text{en otro caso} \end{cases} \\ &= \begin{cases} |H_n| & \text{si } s^{-1}x \in A \text{ y } x \in B \\ -(|H_n|) & \text{si } s^{-1}x \in B \text{ y } x \in A \\ 0 & \text{en otro caso.} \end{cases} \end{aligned}$$

Sea $E_s(A, B)$ el conjunto de aristas del grafo de Cayley $Cay(H_n, \pi_n(S))$ entre A y su complemento que están generados por el elemento s de la desigualdad (3.1). Si s no es su propio inverso $|E_s(A, B)| = |\{x \in B | s^{-1}x \in A\} \cup \{x \in A | s^{-1}x \in B\}|$ ya que si $s^2 = 1$ para los elementos $x \in A$ tales que $s^{-1}x \in B$ tenemos que que

$s^{-1}(s^{-1}x) = x \in A$, por lo que $\{x, s^{-1}x\}$ y $\{s^{-1}(s^{-1}x), s^{-1}x\}$ son la misma arista. Por lo tanto,

$$|E_s(A,B)| \geq \frac{1}{2}|\{x \in B | s^{-1}x \in A\} \cup \{x \in A | s^{-1}x \in B\}|. \tag{3.2}$$

Luego

$$\begin{aligned}
\|L(s)f - f\|_2^2 &= \sum_{x \in H_n} |([L(s)f] - f)(x)|^2 \\
&= \sum_{\substack{x \in A \\ xs^{-1} \in B}} |([L(s)f] - f)(x)|^2 + \sum_{\substack{x \in B \\ xs^{-1} \in A}} |([L(s)f] - f)(x)|^2 \\
&= \sum_{\substack{x \in A \\ xs^{-1} \in B}} |H_n|^2 + \sum_{\substack{x \in B \\ xs^{-1} \in A}} |-(|H_n|)|^2 \\
&= |\{x \in B | s^{-1}x \in A\} \cup \{x \in A | s^{-1}x \in B\}| \, |H_n|^2.
\end{aligned}$$

Entonces por la desigualdad (3.2) y (3.1)

$$\begin{aligned}
2|E_s(A,B)| \, |H_n|^2 \geq \|L(s)f - f\|_2^2 &\geq \kappa(G,S)^2 \, \|f\|_2^2 \\
&= \kappa(G,S) \, |B| \, |A| \, |H_n|.
\end{aligned}$$

Así que $\frac{|E_s(A,B)|}{|A|} \geq \frac{\kappa(G,S)^2 \, |B|}{2|H_n|}$. Dado que $|B| \geq \frac{|H_n|}{2}$ y $E_s(A,B) \subseteq E(A,B)$ tenemos que $\frac{|E(A,B)|}{|A|} \geq \frac{\kappa(G,S)^2}{4}$, así que $\frac{\kappa(G,S)^2}{4}$, entonces por la Definición de la constante isoperimétrica 2.1.3 tenemos que $h(Cay(H_n, \pi_n(S))) \geq \frac{\kappa(G,S)^2}{4}$. Así que para cada subgrupo normal H_n, $h(Cay(H_n, \pi_n(S))) \geq \frac{\kappa(G,S)^2}{4}$, de ahí que $(h(Cay(H_n, \pi_n(S))))$ esta acotada lejos cero. Por lo tanto, $(Cay(H_n, \pi_n(S)))$ es una familia de grafos expanders. ■

Una construcción mas reciente que hace uso de la Propiedad (T) es la que proponen Martin Kassabov, Alexander Lubotzky, and Nikolay Nikolov mediante el siguiente Teorema.

Teorema 3.2.11 ([43], Teorema 1) Existe $k \in \mathbb{N}$ y $\varepsilon > 0$ tal que para cada grupo simple no abeliano finito G, que no sea un grupo de Suzuki, tiene un conjunto S de k generadores para los cuales el grafo de Cayley $Cay(G,S)$ es un $\varepsilon-$expander.

La prueba del teorema anterior es la acumulación de diversos trabajos por lo que invitamos al lector revisar [43].

3.3. Grafos de Ramanujan

En el capítulo 2 estudiamos la constante de expansión espectral (Definición 2.3.21) y su relación con las familias de grafos expanders. Un dato interesante

sobre esta constante es que es posible estimar que tan grande puede ser mediante el Teorema de Alon-Boppana el cual nos dice que para un grafo $d-$regular X el límite superior para su constante de expansión espectral $\lambda(X)$ es $2\sqrt{d-1}$. [45]. Los grafos que alcanzan este límite son conocidos como grafos de Ramanujan y al tener una constante de expansión espectral tan grande se convierten en los mejores ejemplos de grafos expanders, así que en esta sección nos dedicaremos a conocer un poco de los grafos de Ramanujan y mostraremos la construcción de una familia de grafos Ramanujan que a su vez es expander.

Definición 3.3.1 Sea $X = (V, E)$ un grafo $d-$regular y $\lambda(X)$ su constante de expansión espectral, decimos que X es un *grafo de Ramanujan* si

$$\lambda(X) \leq 2\sqrt{d-1}.$$

Ejemplo 3.3.2 El grafo 3−regular de la Figura 3.6 se llama grafo de Petersen, el cual nosotros lo estaremos denotando por $P10$. Con ayuda del software *SageMath* V.10.0 [61] obtendremos su espectro.

```
[1]: P10= graphs.PetersenGraph()
     P10.spectrum()
```

```
[1]: [3, 1, 1, 1, 1, 1, -2, -2, -2, -2]
```

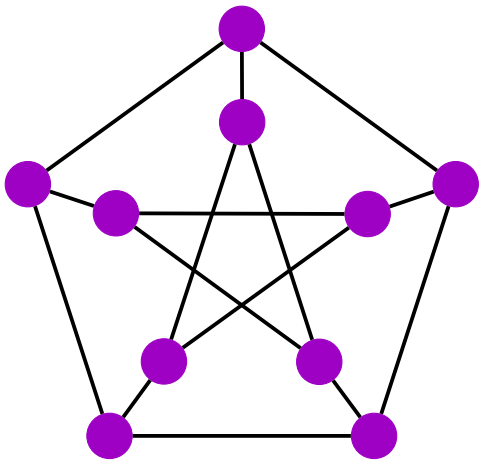


Figura 3.6: Grafo de Petersen.

El grafo de Petersen es un grafo de Ramanujan ya que su constante de expansión espectral es $\lambda(P10) = \text{máx}\{|1|, |-2|\} = 2$ y $2 < 2{,}822 \cong 2\sqrt{3-1}$.

Ejemplo 3.3.3 Los grafos ciclo C^n son grafos 2-regulares, entonces por el Teorema 1.2.42 para cada $\lambda \in Spec(C^n)$ se cumple $|\lambda| \leq 2$, entonces $\lambda(C^n) \leq 2 = 2\sqrt{2-1}$. Por lo tanto, los grafos ciclo son grafos de Ramanujan.

Teorema 3.3.4 Sea (X_n) una sucesión de grafos de Ramanujan d- regulares con $d \geq 3$, entonces (X_n) es una familia de grafos expanders.

Demostración.

Sea (X_n) una sucesión de grafos de Ramanujan d- regulares con $d \geq 3$, por definición tenemos que para cada $n \in \mathbb{N}$ $\lambda(X_n) \leq 2\sqrt{d-1}$, pero por la definición de la constante de expansión espectral tenemos que $\lambda_2(X_n) \leq \lambda(X_n)$, así que $\lambda_2(X_n) \leq 2\sqrt{d-1}$. Luego por la desigualdad de Cheeger 2.1 tenemos que

$$\frac{d-2\sqrt{d-1}}{2} \leq \frac{d-\lambda_2(X_n)}{2} \leq h(X_n).$$

Dado que $d \geq 3$ tenemos que $\frac{d-2\sqrt{d-1}}{2} \geq \frac{3-2\sqrt{2}}{2} > 0$. Entonces para cada $n \in \mathbb{N}$ se cumple que $h(X_n) \geq \frac{3-2\sqrt{2}}{2}$, es decir, $(h(X_n))$ está acotada lejos de cero. Por lo tanto, si $d \geq 3$, cualquier sucesión de grafos de Ramanujan $d-$regulares es una familia de grafos expanders. ■

Observación 3.3.5 Mediante el Teorema 3.3.4 tenemos una forma más sencilla que la del Ejemplo 2.3.19 para probar que los grafos ciclo (C^n) no son familias de grafos expanders.

Entonces la construcción de familias de grafos expanders, se resume en construir familias de grafos de Ramanujan $d-$regulares para un d fijo mayor o igual a tres.

3.3.1. Construcción de Lubotzky, Phillips y Sarnak

En 1988, Lubotzky, Phillips y Sarnak [49] construyeron una familia infinita de grafos de Ramanujan a partir de grafos de Cayley de los grupos $PSL(2,\mathbb{Z}/q\mathbb{Z})$[1] y $PGL(2,\mathbb{Z}/q\mathbb{Z})$[2].

Sean p y q un par de primos relativos congruentes a 1 módulo 4 y sea i un entero tal que $i^2 \equiv (-1) \mod q$. Por el Teorema de los cuatro cuadrados de Jacobi (ver A.0.4) hay $8(p+1)$ soluciones $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ para $\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2 = p$. Entre ellas hay $p+1$ soluciones donde a_0 es mayor que cero e impar y a_j es par para $j \in \{1,2,3\}$. A cada solución α le asociamos la siguiente matriz en $PGL(2,\mathbb{Z}/q\mathbb{Z})$.

$$\overline{\alpha} = \begin{pmatrix} \alpha_0 + i\alpha_1 & \alpha_2 i + \alpha_3 \\ -\alpha_2 + i\alpha_3 & \alpha_0 - i\alpha_1 \end{pmatrix}$$

Si usamos este conjunto de matrices como el conjunto simétrico de generadores S de un grafo de Cayley, obtenemos un grafo $(p+1)$-regular que denotaremos

[1] El grupo lineal especial proyectivo $PSL(2,\mathbb{Z}/q\mathbb{Z})$ es el cociente del grupo $SL(2,\mathbb{Z}/q\mathbb{Z})$ (el grupo lineal especial de matrices de tamaño 2×2 con determinante 1 y entradas sobre el campo $\mathbb{Z}/q\mathbb{Z}$.) con su centro $\{I\}$, donde I es la matriz identidad de tamaño 2×2

[2] El grupo lineal general proyectivo $PGL(2,\mathbb{Z}/q\mathbb{Z})$ es el cociente $GL(2,\mathbb{Z}/q\mathbb{Z})$ con su centro $\{\alpha I : \alpha \in \mathbb{Z}/q\mathbb{Z}\}$, donde I es la matriz identidad de tamaño 2×2.

por X^{pq}. En [49] se prueba que X^{pq} es un grafo de Ramanujan debido a que la expansión espectral $\lambda(X^{pq})$ (ver Definición 2.3.21) es menor a $2\sqrt{p}$.

Además X^{pq} puede ser bipartito o no, esto se define partir del símbolo de Legendre (ver A.0.3) de p y q.

- Si $\left(\frac{p}{q}\right) = -1$.
  - $X^{pq} = Cay(PGL(2, \mathbb{Z}/q\mathbb{Z}), S)$.
  - X^{pq} es bipartito.
  - $|X^{pq}| = q(q^2 - 1)$.
  - $g(X^{pq}) \geq 4 \log_p q - \log_p 4$.
- Si $\left(\frac{p}{q}\right) = 1$.
  - $X^{pq} = Cay(PSL(2, \mathbb{Z}/q\mathbb{Z}), S)$, ya que los elementos de S generan a $PSL(2, \mathbb{Z}/\mathbb{Z}_q)$
  - X^{pq} no es bipartito.
  - $|X^{pq}| = \frac{q(q^2-1)}{2}$.
  - $g(X^{pq}) \geq 2 \log_p q$.

Dado que hay una infinidad de primos q congruentes a 1 mód 4 (ver A.0.7), existe una familia infinita de grafos de Ramanujan $(p+1)-$regulares y por ende una familia infinita de grafos expanders.

3.4. Algunas familias de grafos no-expanders

Durante el estudio de construcciones de familias de grafos expanders, se han encontrados resultados sobre familias de grafos de Cayley que no forman familias de grafos expanders, esto es de gran interés dado que nos da un panorama por donde no debemos buscar familias de grafos expanders.

Para el desarrollo se esta sección se utilizó material de [45].

3.4.1. Principio de no expansión de cocientes

El estudio del grupo cociente de un grupo G es una herramienta rápida para estudiar el comportamiento de los elementos de G a través de sus clases laterales. Esto puede trasladarse a los grafos de Cayley, donde el grafo del grupo cociente recibe el nombre de grafo cociente. En esta subsección daremos algunas de sus propiedades mediante el uso de cubiertas (Definición 1.2.17) y la brecha espectral (Definición 2.3.17) que nos servirán para probar que si una sucesión de grupos (G_n) tiene una sucesión de grupos cocientes que no forma una familia de grafos expanders, entonces (G_n) tampoco lo forma.

Definición 3.4.1 Sean X, Y grafos y ϕ un homomorfismo de X a Y. Sea $f \in L^2(Y)$. Definimos $f^* \in L^2(X)$ como $f^* = f \circ \phi$ y decimos que f^* es el pullback de f vía ϕ.

Lema 3.4.2 Sean $X = (V, E), Y = (V', E')$ grafos tales que X cubre a Y. Si $\mathscr{A}, \widetilde{\mathscr{A}}$ son los operadores de adyacencia de X y Y respectivamente y $f \in L^2(Y)$, entonces

$$\left(\widetilde{\mathscr{A}}(f)\right)^* = \mathscr{A}(f^*).$$

Demostración.

Sea ϕ una cubierta de X a Y (ver Definición 1.2.17) y $v \in V$, si e es una arista incidente en v denotaremos por $e(v)$ al otro vértice incidente en la arista e. Tenemos que

$$\left(\widetilde{\mathscr{A}}(f)\right)^*(v) = \left(\left(\widetilde{\mathscr{A}}(f)\right) \circ \phi\right)(v) = \left(\widetilde{\mathscr{A}}(f)\right)(\phi(v)) = \sum_{w \in N_Y(\phi(v))} f(\phi(w))$$
$$= \sum_{e' \in E'_\phi(v)} f(e'(\phi(v))$$

y

$$\left(\mathscr{A}(f^*)\right)(v) = \sum_{u \in N_X(v)} f^*(u) = \sum_{u \in N_X(v)} f(\phi(u)) = \sum_{e \in E(v)} f(\phi(e((u)))).$$

Como ϕ es una cubierta de X a Y, entonces $\phi_{E_v} : E_v \to E_{\phi(v)}$ es biyectiva. Así que para cada $e' \in E_{\phi(v)}$ existe $e \in E_v$ tal que $e' = \phi(e)$, es decir, $\{\phi(v), e'(\phi(v))\} = \{\phi(v), \phi(e(v))\}$, por consiguiente $e'(\phi(v)) = \phi(e(v))$. Entonces

$$\left(\widetilde{\mathscr{A}}(f)\right)^*(v) = \sum_{e' \in E'_\phi(v)} f(e'(\phi(v)) = \sum_{e \in E(v)} f(\phi(e((u))) = \left(\mathscr{A}(f^*)\right)(v),$$

es decir, $\left(\widetilde{\mathscr{A}}(f)\right)^*(v) = \sum_{e \in E(v)} f(\phi(e((u))) = \left(\mathscr{A}(f^*)\right)(v)$ para cada $v \in V$. Por lo tanto, $\left(\widetilde{\mathscr{A}}(f)\right)^* = \left(\mathscr{A}(f^*)\right)$.

■

Lema 3.4.3 Sean $X = (V, E), Y = (V', E')$ grafos tales que X cubre a Y. Entonces cada valor propio de Y es un valor propio de X.

Demostración.

Sean $\mathscr{A}, \widetilde{\mathscr{A}}$ los operadores de adyacencia de X y Y respectivamente y sea $\lambda \in Spec(\widetilde{\mathscr{A}})$, entonces existe $f \in L^2(Y) \setminus \{0\}$ tal que $\widetilde{\mathscr{A}}(f) = \lambda f$. Por el Lema 3.4.2 tenemos que $\left(\mathscr{A}(f^*)\right) = \left(\widetilde{\mathscr{A}}(f)\right)^* = (\lambda\, f)^* = \lambda f^*$, con $f^* \in L^2(X) \setminus \{0\}$. Por lo tanto, $\lambda \in Spec(\mathscr{A})$. ■

Proposición 3.4.4 Sean $X = (V, E), Y = (V', E')$ grafos finitos d-regulares tales que X cubre a Y, entonces $\lambda_2(X) \geq \lambda_2(Y)$.

Demostración.

Sea $\lambda_2(Y)$ el segundo valor propio más grande de Y, por el Lema 3.4.3 tenemos que $\lambda_2(Y)$ es un valor propio de X. Como $\lambda_2(X)$ es el segundo valor propio más grande de X tenemos que $\lambda_2(Y) \leq \lambda_2(X)$. ■

Definición 3.4.5 Sea G un grupo finito, S un conjunto simétrico de generadores de G y $H \leq G$. Definimos el *grafo cociente* $Cos(G/H, S)$ como el grafo orientado cuyos vértices son las clases laterales izquierdas de H en G y las aristas son de la forma $\{xH, sxH\}$ para cada $s \in S$.

Observación 3.4.6 G/H denota el conjunto de las clases laterales izquierdas de H en G, cuando H es un subgrupo normal de G entonces G/H es el grupo cociente.

Proposición 3.4.7 $Cos(G/H, S)$ es un grafo $|S|$-regular.

Demostración.

Supongamos que $S = \{s_1, \ldots, s_n\}$, sea xH un vértice de $Cos(G/H, S)$, por la definición de grafo cociente tenemos que las aristas que genera el vértice xH son $\{xH, s_1xH\}, \{xH, s_2xH\}, \ldots, \{xH, s_nxH\}$, así que el grado de el vértice xH es $n = |S|$. Por lo tanto, $Cos(G/H, S)$ es $|S|$-regular. ■

Ejemplo 3.4.8 Consideremos el grupo $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, $S = \{(12), (23), (123), (132)\}$ un conjunto simétrico de generadores de S_3 y el subgrupo $H = \{(1), (23)\}$. Tenemos que $G/H = \{H, (12)H, (13)H\}$ ya que

$$(12)H = \{(12), (12)(23)\} = \{(12), (123)\} = \{(123)(23), (123)\} = (123)H$$

$$(13)H = \{(13), (13)(23)\} = \{(13), (132)\} = \{(132)(23), (132)\} = (132)H.$$

Construyamos el grafo cociente $Cos(G/H, S\}$, para ello recordemos que en los grafos cocientes las aristas tienen la siguiente forma $\{xH, sxH\}$ con $xH \in G/H$ y $s \in S$.

Vértice	Vecinos			
xH	$(12)xH$	$(23)xH$	$(123)xH$	$(132)xH$
H	$(12)H$	H	$(12)H$	$(13)H$
$(12)H$	H	$(13)H$	$(13)H$	H
$(13)H$	$(13)H$	$(12)H$	H	$(12)H$

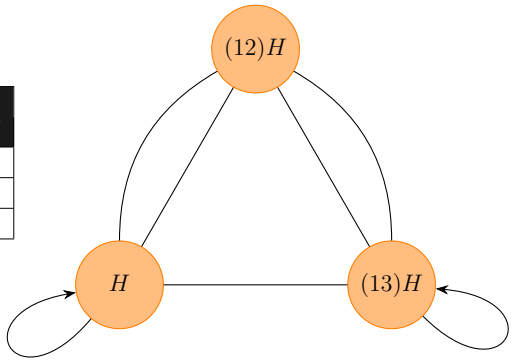


Figura 3.7: $Cos(S_3/H, S)$.

Lema 3.4.9 Sea G un grupo finito. Sea $H \leq G$ y S un conjunto simétrico de generadores. Entonces $Cay(G, S)$ cubre a $Cos(G/H, S)$.

Demostración.

Consideremos la función $\phi\colon G \to G/H$ dada por $\phi(a) = aH$. Probemos que ϕ es un homomorfismo de grafos (Definición 1.2.9). Sea $\{a, b\}$ una arista de $Cay(G, S)$, por la Definición 1.2.46 de grafo de Cayley tenemos que $ab^{-1} \in S$. Notemos que $ab^{-1}bH = aH$, entonces por la Definición 3.4.5 de grafo cociente $\{aH, bH\} = \{\phi(a), \phi(b)\}$ es una arista de $Cos(G/H, S)$, así que ϕ preserva la adyacencia de vértices. Por lo tanto, ϕ es un homomorfismo de grafos. Ahora probemos que ϕ es una cubierta (Definición 1.2.17) para ello solo basta probar que $\phi\colon E_a \to E_{\phi(a)}$ es biyectiva para cada $a \in G$, ya que la sobreyectividad de $\phi\colon G \to G/H$ es clara. Sea $a \in G$ y $s \in S$, denotaremos por $e(a, s)$ la arista $\{a, sa\}$ de $Cay(G, S)$ inducida por s y $\overline{e}(aH, s)$ la arista $\{aH, saH\}$ de $Cos(G/H, S)$ inducida por s. Sea $\overline{e}(\phi(a), s)$ una arista incidente en $\phi(a)$, si nos tomamos $e(a, s) \in E_a$ tenemos que $\phi(e(a, s)) = \{\phi(a), \phi(sa)\} = \{aH, saH\} = \{\phi(a), s\phi(a)\} = \overline{e}(\phi(a), s)$, es decir, para cada $\overline{e}(\phi(a), s) \in E_{\phi(a)}$ existe $e(a, s) \in E_a$ tal que $\phi(e(a, s)) = \overline{e}(\phi(a), s)$, así que $\phi\colon E_a \to E_{\phi(a)}$ es sobreyectiva, además por el Teorema 1.2.52 y la Proposición 3.4.7 el grado de a y $\phi(a)$ es igual a $|S|$, es decir, $|E_a| = |S| = |E_{\phi(a)}|$, por consiguiente $\phi\colon E_a \to E_{\phi(a)}$ es biyectiva para cada $a \in G$. Entonces ϕ es una cubierta de $Cay(G, S)$ a $Cos(G/H, S)$. Por lo tanto, $Cay(G, S)$ cubre a $Cos(G/H, S)$. ■

Ejemplo 3.4.10 Consideremos al grupo $D_6 = \{1, a, a^2, ab, a^2b, b\}$ y $S = \{a, a^2, b\}$ un conjunto simétrico de generadores de D_6. Construyamos el grafo de Cayley $Cay(D_6, S)$. Recordemos que en los grafos de Cayley las aristas tienen la siguiente forma $\{x, sx\}$ con $x \in D_6$ y $s \in S$, para hacer más énfasis en la forma de estas aristas denotaremos por $e(x, s)$ al arista de $Cay(D_6, S)$ incidente en x e inducida por s, es decir, $\{x, sx\} = e(x, s)$.

Vértice	Vecinos		
x	ax	a^2x	bx
1	a	a^2	b
a	a^2	1	a^2b
a^2	1	a	ab
ab	a^2b	b	a^2
a^2b	b	ab	a
b	ab	a^2b	1

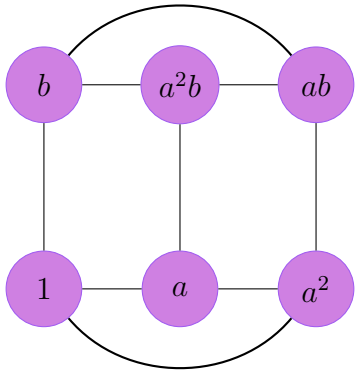


Figura 3.8: $Cay(D_6, S)$.

$$E_1 = \Big\{\{1, a\},\ \{1, a^2\},\ \{1, b\}\Big\} = \Big\{e(1, a),\ e(1, a^2),\ e(1, b)\Big\}.$$

$$E_a = \Big\{\{a,a^2\},\ \{a,1\},\ \{a,a^2b\}\Big\} = \Big\{e(a,a),\ e(a,a^2),\ e(a,b)\Big\}.$$
$$E_{a^2} = \Big\{\{a^2,1\},\ \{a^2,a\},\ \{a^2,ab\}\Big\} = \Big\{e(a^2,a),\ e(a^2,a^2),\ e(a^2,b)\Big\}.$$
$$E_{ab} = \Big\{\{ab,a^2b\},\ \{a,b\},\ \{ab,a^2\}\Big\} = \Big\{e(ab,a),\ e(ab,a^2),\ e(ab,b)\Big\}.$$
$$E_{a^2b} = \Big\{\{a^2b,b\},\ \{a^2b,b\},\ \{a^2b,a\}\Big\} = \Big\{e(a^2b,a),\ e(a^2b,a^2),\ e(a^2b,b)\Big\}.$$
$$E_b = \Big\{\{b,ab\},\ \{b,a^2b\},\ \{b,1\}\Big\} = \Big\{e(b,a),\ e(b,a^2),\ e(b,b)\Big\}.$$

Consideremos el grupo $H = \{1, b\}$, tenemos que $G/H = \{H, aH, a^2H\}$. Construyamos el grafo cociente $Cos(G/H, S\}$, para ello recordemos que en los grafos cocientes las aristas tienen la siguiente forma $\{xH, sxH\}$ con $xH \in G/H$ y $s \in S$, para hacer más énfasis en la forma de estas aristas denotaremos por $\overline{e}(xH, s)$ al arista de $Cos(D_6/H, S)$ incidente en xH e inducida por s, es decir, $\{xH, sxH\} = \overline{e}(xH, s)$.

Vértice	Vecinos		
xH	axH	a^2xH	bxH
H	aH	a^2H	H
aH	a^2H	H	a^2H
a^2H	H	aH	aH

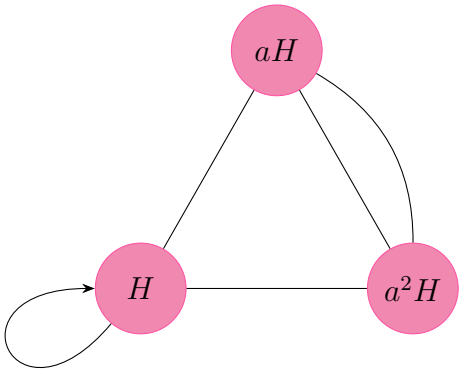


Figura 3.9: $Cos(D_6/H, S)$.

$$E_H = \Big\{\{H,aH\},\ \{H,a^2H\},\ \{H,H\}\Big\} = \Big\{\overline{e}(H,a),\ \overline{e}(H,a^2),\ \overline{e}(H,b)\Big\}.$$
$$E_{aH} = \Big\{\{aH,a^2H\},\ \{aH,H\},\ \{aH,a^2H\}\Big\} = \Big\{\overline{e}(aH,a),\ \overline{e}(aH,a^2),\ \overline{e}(aH,b)\Big\}.$$
$$E_{a^2H} = \Big\{\{a^2H,H\},\ \{a^2H,aH\},\ \{a^2H,aH\}\Big\} = \Big\{\overline{e}(a^2H,a),\ \overline{e}(a^2H,a^2),\ \overline{e}(a^2H,b)\Big\}.$$

Comparemos,

$$E_a = \Big\{\{a,a^2\},\ \{a,1\},\ \{a,a^2b\}\Big\} = \Big\{(a,a),\ e(a,a^2),\ e(a,b)\Big\}.$$
$$E_{aH} = \Big\{\{aH,a^2H\},\ \{aH,H\},\ \{aH,a^2H\},\Big\} = \Big\{\overline{e}(aH,a),\ \overline{e}(aH,a^2),\ \overline{e}(aH,b)\Big\}.$$

Dado que ambos conjuntos tienen la misma cantidad de elementos y que estos se pueden relacionar a través del elemento en S que induce cada arista, tenemos que la siguiente función es biyectiva

$$\begin{aligned}\phi_{E_a}\colon E_a &\longrightarrow E_{aH}\\ e(a,a) &\longmapsto \overline{e}(aH,a)\\ e(a,a^2) &\longmapsto \overline{e}(aH,a^2)\\ e(a,b) &\longmapsto \overline{e}(aH,b).\end{aligned}$$

Haciendo el mismo análisis con los conjuntos E_1 con E_H y E_{a^2} con E_{a^2H} tenemos que ϕ_{E_1} y $\phi_{E_{a^2}}$ son biyectivas. Entonces, $\phi\colon D_6 \to D_6/H$ dada por $\phi(x) = xH$ para cada $x \in D_6$ es una cubierta. Por lo tanto, $Cay(D_6, S)$ cubre a $Cos(D_6/H, S)$.

Corolario 3.4.11 Sea G un grupo finito. Sea $H \leq G$ y S un conjunto simétrico de generadores de G. Entonces $\lambda_2(Cay(G,S)) \geq \lambda_2(Cos(G/H,S))$.

Demostración.

Por el Lema 3.4.9 tenemos que $Cay(G,S)$ cubre a $Cos(G/H,S)$, entonces por la Proposición 3.4.4 tenemos que $\lambda_2(Cay(G,S)) \geq \lambda_2(Cos(G/H,S))$. ■

Observación 3.4.12 Si $H \triangleleft G$ entonces las clases laterales izquierdas coinciden con las derechas y si $\overline{S} = \{sH \mid s \in S\}$, entonces $Cos(G/H,S) = Cay(G/H,\overline{S})$.

Definición 3.4.13 Sean (G_n) y (Q_n) sucesiones de grupos finitos. Decimos que (G_n) admite a (Q_n) como una sucesión de cocientes si para cada $n \in \mathbb{N}$ existe $H_n \triangleleft G_n$ tal que $G_n/H_n \cong Q_n$.

Observación 3.4.14 Si para cada $n \in \mathbb{N}$, S_n es un conjunto simétrico de generadores de G_n, H_n es un subgrupo normal de G_n y ϕ_n es un isomorfismo entre G_n/H_n y Q_n, entonces los grafos $Cay(G/H,\overline{S})$ y $(Cay(Q_n,\phi_n(\overline{S_n})))$ son isomorfos.

Definición 3.4.15 Sea (G_n) una sucesión de grupos finitos, decimos que (G_n) forma una familia de grafos expanders si para algún entero positivo d existe una sucesión (S_n) donde para cada $n \in \mathbb{N}$ tenemos que S_n es un conjunto simétrico de generadores de G_n con cardinalidad d, la sucesión de grafos de Cayley $(Cay(G_n,S_n))$ es una familia de grafos expander.

Proposición 3.4.16 (Principio de no expansión de cocientes) Sea (G_n) una sucesión de grupos finitos. Si (G_n) admite a (Q_n) como una sucesión de cocientes y (Q_n) no forma una familia de grafos expanders, entonces (G_n) tampoco forma una familia de grafos expanders.

Demostración.

Supongamos que (G_n) forma una familia de grafos expanders, entonces para algún entero positivo d existe una sucesión (S_n) con S_n un conjunto simétrico de generadores de G_n y $|S_n| = d$ para cada $n \in \mathbb{N}$ tal que $(Cay(G_n,S_n))$ es una familia de grafos expander, así que por el Teorema 2.3.18 $(d - \lambda_2(Cay(G_n,S_n)))$ es una sucesión acotada lejos de cero, es decir, existe $\varepsilon > 0$ tal que $d - \lambda_2(Cay(G_n,S_n)) \geq \varepsilon$ para cada $n \in \mathbb{N}$. Dado que (G_n) admite a (Q_n) como una sucesión de cocientes,

entonces para cada $n \in \mathbb{N}$ existe un isomorfismo $\phi_n \colon G_n/H_n \to Q_n$ con $H_n \triangleleft G_n$. Entonces por las Observaciones 3.4.12 y 3.4.14

$$\lambda_2(Cos(G_n/H_n, S_n)) = \lambda_2(Cay(G_n/H_n, \overline{S_n})) = \lambda_2(Cay(Q_n, \phi_n(\overline{S}))).$$

Luego por el Corolario 3.4.11 tenemos que

$$\lambda_2(Cay(G_n, S_n)) \geq \lambda_2(Cos(G_n/H_n, S_n)),$$

así que $(Cay(G_n, S_n)) \geq \lambda_2(Cay(Q_n, \phi_n(\overline{S})))$. Entonces $d - \lambda_2(Cay(Q_n, \phi_n(\overline{S}))) \geq d - \lambda_2(Cay(G_n, S_n)) \geq \varepsilon$, por lo que $(d - \lambda_2(Cay(Q_n, \phi_n(\overline{S}))))$ esta acotada lejos de cero, pero por el Teorema 2.3.18 esto implicaria que$(Cay(Q_n, \phi_n(\overline{S})))$ es una familia de grafos expanders, contradicciendo el hecho de que (Q_n) no forma una familia de grafos expanders. Por lo tanto, (G_n) no forma una familia de grafos expanders.

■

Observación 3.4.17 Otra forma de probar de la Proposición 3.4.16 es mediante el uso de la constante isoperimétrica (ver [45] pág 52-54).

3.4.2. Los grupos abelianos finitos no forman una familia de grafos expanders

Los grupos abelianos finitos son grupos fáciles de trabajar, así que al tratar de construir una familia de grafos expanders es natural que se trate de utilizar grupos abelianos finitos. Sin embargo estos grupos no funcionan. En esta subsección, probaremos que los grupos abelianos finitos no forman familias de grafos expanders utilizando la constante de Kazhdan (ver Definición 2.4.6).

La prueba es un corolario de la Proposición 3.4.19 que nos establece una cota para la constante de Kazhdan de grupos abelianos finitos. Para probar tal proposición haremos uso del siguiente Lema.

Lema 3.4.18 Sea θ un número real. Entonces $|e^{i\theta} - 1| \leq |\theta|$.

Demostración.

Sea $f(x) = \cos(x) - 1 + \frac{x^2}{2}$. Veamos que $f(x) \geq 0$ para cada $x \in \mathbb{R}$. Tenemos que

$$\begin{aligned} f(0) &= \cos(0) - 1 + \tfrac{0^2}{2} = 0 \\ f'(x) &= -\sin(x) + x \\ f'(0) &= -\sin(0) + 0 = 0 \\ f''(x) &= -\cos(x) + 1. \end{aligned}$$

Recordemos que si una función real g es continua en $[a, b]$, diferenciable en (a, b) y $g'(x) \geq 0$ para todo $x \in (a, b)$ entonces g es creciente en (a, b). Entonces para $x > 0$ tomemos $b \in (0, x)$, dado que $\cos(b) \leq 1$ entonces $1 - \cos(b) \geq 0$, así que

$f''(b) \geq 0$ para todo $b \in (0, x)$, de ahí que $f'(x) \geq 0$ y por consiguiente, $f(x) \geq 0$ para cada $x > 0$. Luego, como f es una función par tenemos que $f(x) \geq 0$ para cada $x \in \mathbb{R}$. Entonces para toda $x \in \mathbb{R}$, $cos(x) \geq 1 - \frac{x^2}{2}$. Luego

$$\begin{aligned} |e^{i\theta} - 1|^2 = |\cos(\theta) - 1 + i\sin(\theta)|^2 &= (\cos(\theta) - 1)^2 + (\sin(\theta))^2 \\ &= \cos^2(\theta) - 2\cos(\theta) + 1 + \sin^2(\theta) \\ &= 2 - 2\cos(\theta) \\ &\leq 2 - 2(1 - \tfrac{\theta^2}{2}) \\ &= 2 - 2 + \theta^2, \end{aligned}$$

es decir, $|e^{i\theta} - 1|^2 \leq \theta^2$. Por lo tanto, $|e^{i\theta} - 1| \leq |\theta|$ para cada $\theta \in \mathbb{R}$. ■

Proposición 3.4.19 Sea G un grupo abeliano finito no trivial y $S \subseteq G$ con $|S| = d$. Entonces $\kappa(G, S) \leq \dfrac{2\pi}{|G|^{1/d} - 1}$.

Demostración.

Sea $\kappa = \kappa(G, S)$. Si $\kappa = 0$ la proposición es verdadera. Supongamos que $\kappa > 0$. Sea $C = \left\lceil \frac{2\pi}{\kappa} \right\rceil$, es decir C es el menor entero que es mayor o igual a $\frac{2\pi}{\kappa}$. Supongamos que $|G| > C^d$. Por el Teorema Fundamental de los grupos abelianos finitos tenemos que G es isomorfo a un producto de la siguiente forma $\frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \frac{\mathbb{Z}}{n_2\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{n_r\mathbb{Z}}$. Sea A el conjunto de todas las representaciones irreducibles de G, el cual fue determinado en el Corolario 1.3.39, entonces si ρ es una representación irreducible de G y $g \in G$ tenemos que $\rho(g)$ es de la forma $\exp(i\theta)$ para algún $\theta \in [0, 2\pi)$, así que para cada $g \in G$, $\rho(g)$ es un número complejo distinto de cero con módulo 1. Luego para cualquier $z \in \mathbb{C}$ en el círculo unitario, denotaremos por $l(z)$ al único elemento en $[0, 2\pi)$ que satisface $\exp(il(z)) = z$. Consideremos nuestro conjunto simétrico generadores de G como $S = \{s_1, \ldots, s_d\}$, a cada representación de G le asignaremos una $d-$tuple en $[0, 2\pi)^d$ mediante la siguiente función

$$\begin{aligned} \Gamma \colon A &\longrightarrow [0, 2\pi)^d \\ \rho &\longmapsto (l(\rho(s_1)), l(\rho(s_2)), \ldots, l(\rho(s_d))). \end{aligned}$$

Luego, sean $a_1, \ldots, a_d \in \mathbb{Z}$ con $1 \leq a_j \leq C$ para toda $j \in \{1, \ldots, d\}$ y sea $a = (a_1, \ldots, a_d)$, definimos

$$B_a := \left\{ r = (r_1, \ldots, r_d) \in [0, 2\pi)^d : \frac{2\pi(a_j - 1)}{C} \leq r_j < \frac{2\pi a_j}{C} \right\}$$

Probemos que $[0, 2\pi)^d$ es una unión disjunta de C^d conjuntos B_a, para ello primero nos tomaremos dos $d-$tuples distintas, digamos $a = (a_1, \ldots, a_d)$ y $a' = (a'_1, \ldots, a'_d)$ y probaremos que $B_a \cap B_{a'} = \emptyset$. Procederemos por contradicción, supongamos que existe $r = (r_1 \ldots, r_d) \in B_a \cap B_{a'}$, como $a \neq a'$ existe $j \in \{1, \ldots d\}$ tal que $a_j \neq a'_j$. Sin pérdida de la generalidad supongamos que $a_j < a'_j$, como ambos son enteros tenemos que $a_j \leq a'_j - 1$, multiplicando esta desigualdad

por $\frac{2\pi}{C}$ tenemos que $\frac{2\pi a_j}{C} \leq \frac{2\pi(a'_j-1)}{C}$. Por definición de los conjuntos B_a y $B_{a'}$ tenemos que $r_j \leq \frac{2\pi a_j}{C}$ y $\frac{2\pi(a'_j-1)}{C} < r_j$, entonces $r_j \leq \frac{2\pi a_j}{C} \leq \frac{2\pi(a'_j-1)}{C} < r_j$, es decir, $r_j < r_j$ lo cual es una contradicción, por lo tanto $B_a \cap B_{a'} = \emptyset$. Sea $\mathcal{A} = \{(a_1, \ldots, a_d) \in \mathbb{Z}^d : 1 \leq a_j \leq C \text{ para toda } j \in \{1, \ldots, d\}\}$ probaremos que $\bigcup_{a\in\mathcal{A}} B_a = [0, 2\pi)^d$. Si nos tomamos $r \in \bigcup_{a\in\mathcal{A}} B_a$, entonces existe $a \in \mathcal{A}$ tal que $r \in B_a$ y por definición de $B_a, r \in [0, 2\pi)^d$, así que $\bigcup_{a\in\mathcal{A}} B_a \subseteq [0, 2\pi)^d$. Ahora sea $r' = (r'_1, \ldots, r'_d) \in [0, 2\pi)^d$, para cada $j \in \{1, \ldots, d\}$ definimos el siguiente entero $a_j = \text{mín}\{C, \lfloor \frac{Cr'_j}{2\pi} + 1 \rfloor\}$. Dado que $1 \leq C$ y $1 \leq \lfloor \frac{Cr'_j}{2\pi} + 1 \rfloor$ tenemos que $1 \leq a_j$ y por la definición de cada a_j tenemos que $a_j \leq C$, así que para cada $j \in \{1, \ldots, d\}$, $1 \leq a_j \leq C$. Sea $a = (a_1, \ldots, a_d)$ veamos que $r' \in B_a$, para ello primero probaremos que para cada $j \in \{1, \ldots, d\}$ $r'_j < \frac{2\pi a_j}{C}$. Si $a_j = C$, entonces $\frac{2\pi a_j}{C} = 2\pi$ y como $r' \in [0, 2\pi)^d$, se satisface que $r'_j < 2\pi$, así que $r'_j < \frac{2\pi a_j}{C}$. Si $a_j = \lfloor \frac{Cr'_j}{2\pi} + 1 \rfloor$, supongamos que $a_j \leq \frac{Cr'_j}{2\pi}$, entonces por la propiedad de la función piso tenemos que $\lfloor \frac{Cr'_j}{2\pi} + 1 \rfloor \leq \lfloor \frac{Cr'_j}{2\pi} \rfloor$ lo cual es una contradicción, entonces $\frac{Cr'_j}{2\pi} < a_j$, de ahí que $r'_j < \frac{2\pi a_j}{C}$. Por otra parte, como a_j es un entero que es menor o igual a $\lfloor \frac{Cr'_j}{2\pi} + 1 \rfloor$, tenemos que $a_j \leq \frac{Cr'_j}{2\pi} + 1$, de ahí que $\frac{2\pi(a_j-1)}{C} \leq r'_j$. Entonces para cada $j \in \{1, \ldots, d\}$ se cumple que $\frac{2\pi(a_j-1)}{C} \leq r'_j < \frac{2\pi a_j}{C}$, así que $r' = (r'_1, \ldots, r'_d) \in B_a$ con $a \in \mathcal{A}$, es decir $r' \in \bigcup_{a\in\mathcal{A}} B_a$. Entonces $[0, 2\pi)^d \subseteq \bigcup_{a\in\mathcal{A}} B_a$. Por lo tanto $[0, 2\pi)^d = \bigcup_{a\in\mathcal{A}} B_a$.

Luego, por el Corolario 1.3.39 $|A| = |G|$ así que hay $|G|$ representaciones irreducibles y como $|G| > C^d$, tenemos que por el principio del palomar (o el principio de cajas) debe haber dos representaciones irreducibles ρ_1, ρ_2 tales que $\Gamma(\rho_1), \Gamma(\rho_2) \in B_a$ para alguna $d-$tuple a. Definimos

$$\begin{aligned} \widehat{\rho}\colon G &\longrightarrow GL(\mathbb{C}) \\ g &\longmapsto \widehat{\rho}(g) = \frac{\rho_1(g)}{\rho_2(g)}. \end{aligned}$$

Notemos que $\widehat{\rho}$ es una representación de G ya que para cada $g, h \in G$

$$\widehat{\rho}(g+h) = \frac{\rho_1(g+h)}{\rho_2(g+h)} = \frac{\rho_1(g)\rho_1(h)}{\rho_2(g)\rho_2(h)} = \frac{\rho_1(g)}{\rho_2(g)}\frac{\rho_1(h)}{\rho_2(h)} = \widehat{\rho}(g)\widehat{\rho}(h).$$

Más aún, como ρ_1 y ρ_2 son distintas y de grado 1 tenemos que $\widehat{\rho}$ es no trivial y es irreducible. Dado que $\Gamma(\rho_1), \Gamma(\rho_2) \in B_a$ para alguna $d-$tuple $a = (a_1, a_2, \ldots, a_d)$, es decir, $(l(\rho_1(s_1)), l(\rho_1(s_2)), \ldots, l(\rho_1(s_d)))$, $(l(\rho_2(s_1)), l(\rho_2(s_2)), \ldots, l(\rho_2(s_d))) \in B_a$ tenemos que para cada $j \in \{1, \ldots, d\}$

$$\frac{2\pi(a_j - 1)}{C} \leq l(\rho_1(s_j) < \frac{2\pi a_j}{C}$$

$$\frac{2\pi(a_j-1)}{C} \leq l(\rho_2(s_j) < \frac{2\pi a_j}{C},$$

así que

$$\frac{2\pi(a_j-1)}{C} - \frac{2\pi a_j}{C} < l(\rho_1(s_j) - l(\rho_2(s_j) < \frac{2\pi a_j}{C} - \frac{2\pi(a_j-1)}{C},$$

es decir,

$$-\frac{2\pi}{C} < l(\rho_1(s_j) - l(\rho_2(s_j) < \frac{2\pi}{C},$$

entonces

$$|l(\rho_1(s_j)) - l(\rho_2(s_j))| < \frac{2\pi}{C}. \tag{3.3}$$

Recordemos que para cada $j \in \{1,\ldots,d\}$ tenemos que $\rho_1(s_j) = \exp(i\ l(\rho_1(s_j))\ )$ y $\rho_2(s_j) = \exp(i\ l(\rho_2(s_j))\ )$. Entonces

$$\widehat{\rho}(s_j) = \frac{\rho_1(s_j)}{\rho_2(s_j)} = \frac{\exp(i\ l(\rho_1(s_j))\ )}{\exp(i\ l(\rho_2(s_j))\ )} = \exp(i\ [l(\rho_1(s_j)) - l(\rho_2(s_j))]\ ).$$

De la igualdad anterior, el Lema 3.4.18 y la desigualdad (3.3) tenemos que

$$\begin{aligned} |\widehat{\rho}(s_j) - 1| &= |\exp(i\ [l(\rho_1(s_j)) - l(\rho_2(s_j))]\ ) - 1| \\ &\leq |l(\rho_1(s_j)) - l(\rho_2(s_j))| \\ &< \tfrac{2\pi}{C}, \end{aligned}$$

es decir, $|\widehat{\rho}(s_j) - 1| < \frac{2\pi}{C}$ para toda $j \in \{1,\ldots,d\}$. Sea v un vector unitario de $\mathbb{C}^{\mathbb{C}}$ tenemos que $\|\widehat{\rho}(s_j)v - v\| = |\rho(s_j) - 1||v| < \frac{2\pi}{C}$, entonces $\kappa'(G,S,\widehat{\rho}) < \frac{2\pi}{C}$ de ahí que $\kappa = \kappa(G,S) < \frac{2\pi}{C}$, así que $C < \frac{2\pi}{\kappa}$ pero esto contradice el hecho de que $C \geq \frac{2\pi}{\kappa}$. Por lo tanto, $|G| \leq C^d$.

Luego, dado que C es el menor entero tal que $\frac{2\pi}{\kappa} \leq C$ tenemos que $C \leq \frac{2\pi}{\kappa} + 1$, así que $|G| \leq C^d \leq (\frac{2\pi}{\kappa} + 1)^d$ entonces

$$|G|^{\frac{1}{d}} \leq \frac{2\pi}{\kappa} + 1 \tag{3.4}$$

Despejando κ de (3.4) tenemos que $\kappa \leq \frac{2\pi}{|G|^{1/d}-1}$. Por lo tanto, $\kappa(G,S) \leq \frac{2\pi}{|G|^{1/d}-1}$. ■

Corolario 3.4.20 Si (G_n) es una sucesión de grupos abelianos finitos tales que $|G_n| \to \infty$ cuando $n \to \infty$ y sea S_n un conjunto simétrico de generadores de G_n para cada $n \in \mathbb{N}$ con $|S_n| = d$ donde d es un entero no negativo fijo. Entonces (G_n) no forma una familia de grafos expanders.

Demostración.

Por la Proposición 3.4.19 tenemos que para cada G_n con $n \in \mathbb{N}$

$$0 \leq \kappa(G_n, S_n) \leq \frac{2\pi}{|G_n|^{1/d} - 1}.$$

Como $\lim_{n\to\infty} \frac{2\pi}{|G_n|^{1/d}-1} = 0$ tenemos que $\lim_{n\to\infty} \kappa(G_n, S_n) = 0$, así que $\kappa(G_n, S_n)$ no esta acotada lejos de cero. Entonces por el Teorema 2.4.16 (G_n) no forma una familia de grafos expanders. ■

Observación 3.4.21 Otra forma de probar que los grupos abelianos no forman familias de grafos expanders es exhibiendo que sus grafos de Cayley no tienen diámetro logarítmico, para ello es necesario ocupar resultados de combinatoria (ver [45] pág 102-104).

Capítulo 4
Códigos

Si bien un grafo por si solo tiene una infinidad de aplicaciones, el hecho de que tenga la propiedad de ser altamente conectado lo vuelve muy útil en áreas como lo es la teoría de la información. Por ejemplo, es posible construir familias de buenos códigos correctores de errores utilizando familias de grafos expanders.

En este capítulo estudiaremos algunos conceptos básicos sobre la teoría de códigos y su relación con las familias de grafos expanders. Los textos base para su desarrollo son [52], [5], [55], [39], [31], [41], [46] y [18].

Los códigos detectores-correctores de errores fueron inventados para detectar y corregir errores producidos por el ruido en los canales de comunicación. Supóngase que un mensaje u se codifica en una palabra-código x la cual es enviada por el canal, debido al ruido del canal se recibe el vector y el cual puede ser diferente de x, esto es $y = x + e$ donde e es un vector error. La decodificación debe determinar, a partir del vector y, que mensaje u o estimado de u fue transmitido. En la Figura 4.1 se muestra un sistema general de transmisión de información como el que se acaba de describir.

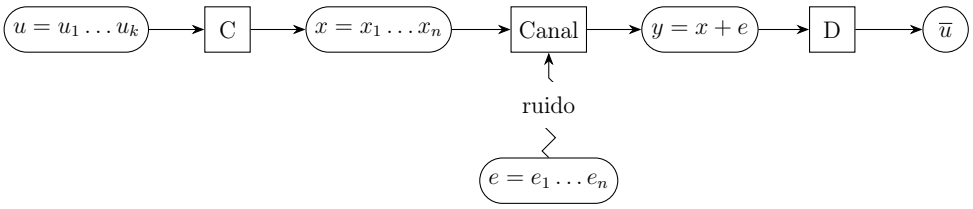


Figura 4.1: Sistema general de transmisión de información.

Definición 4.0.1 Sea $A = \{a_1, a_3, \dots, a_q\}$ un conjunto de tamaño q al que llamaremos *alfabeto* y sea A^n el conjunto de $n-$tuplas de elementos de A. Un *código* $\mathcal{C}$ *de longitud* n *sobre* A es un subconjunto no vacío de A^n. Los elementos de $\mathcal{C}$ se denominan *palabras-código.*

Definición 4.0.2 Sea $\mathcal{C}$ un código de longitud n tal que $|\mathcal{C}| = M$, decimos que $\mathcal{C}$ es un $(n, M)-$código.

Observación 4.0.3 En la práctica, el alfabeto de un código es un campo finito $\mathbb{F}_q$ donde q es la potencia de un primo o un anillo finito R. Un código sobre el alfabeto $\mathbb{F}_2$ se llama *código binario.* En este capítulo se trabajará solo con este tipo de códigos.

Definición 4.0.4 Sean $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$. La *distancia de Hamming* de x a y, denotada por $d(x, y)$, es definida como

$$d(x, y) = |\{i : 1 \leq i \leq n, x_i \neq y_i\}|.$$

Definición 4.0.5 El *peso de Hamming* de $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, denotado por $wt(x)$, se define como

$$wt(x) = |\{i : 1 \leq i \leq n, x_i \neq 0\}|.$$

Observación 4.0.6 A partir de las definiciones 4.0.4 y 4.0.5 se tiene que $d(x, y) = wt(x-y)$, ya que si $d(x, y) = s$, entonces hay s coordenadas en las que x y y difieren y $n - s$ coordenadas en las que coinciden, así que en la diferencia $x - y$ hay $n - s$ ceros y s coordenadas distintas de cero, por lo tanto $wt(x - y) = s$.

Los siguientes tres Teoremas son resultados conocidos en la teoría de códigos y su pruebas pueden consultarse en [5].

Teorema 4.0.7 la función $d\colon \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbf{N} \cup \{0\}$ dada por $d(x, y)$ satisface las siguientes propiedades para toda $x, y, z \in \mathbb{F}_2^n$.

1) $d(x, y) \geq 0$ y $d(x, y) = 0$ sí y sólo si $x = y$,

2) $d(x, y) = d(y, x)$,

3) $d(x, y) \leq d(x, z) + d(z, y)$.

Por lo tanto, $(\mathbb{F}_2^n, d)$ es un espacio métrico.

Teorema 4.0.8 La *distancia mínima* de un código $\mathcal{C}$, la cual se denota por $d(\mathcal{C})$, es el peso mínimo de cada palabra-código diferente de cero.

Definición 4.0.9 Sea $\mathcal{C}$ un código de longitud n y distancia mínima $d(\mathcal{C})$. La *distancia mínima relativa* de $\mathcal{C}$ es $\frac{d(\mathcal{C})}{n}$.

La distancia mínima del código juega un papel esencial en la respuesta a la pregunta ¿cuántos errores puede corregir un código?

Teorema 4.0.10 Un código $\mathcal{C}$ con distancia mínima d puede corregir $\lfloor \frac{1}{2}(d-1) \rfloor$

Observación 4.0.11 En base al Teorema 4.0.10, nosotros consideraremos a un código como *bueno* si tiene una distancia mínima grande y consideraremos a una familia de códigos *asintóticamente buena* si sus distancias mínimas relativas, permanecen constantes a medida que la longitud de los códigos crece.

4.1. Códigos lineales

Definición 4.1.1 Un *código lineal* $\mathcal{C}$ de longitud n sobre $\mathbb{F}_2$ es un subespacio de $\mathbb{F}_2^n$.

Definición 4.1.2 Sea $\mathcal{C}$ un código lineal en $\mathbb{F}_2^n$.

- El *código dual* de $\mathcal{C}$, denotado por $\mathcal{C}^\perp$, es el complemento ortogonal de $\mathcal{C}$ como subespacio de $\mathbb{F}_2^n$.
- La *dimensión* de un código lineal $\mathcal{C}$ es la dimensión de $\mathcal{C}$ como subespacio de $\mathbb{F}_2^n$.

Observación 4.1.3 Un código lineal $\mathcal{C}$ de longitud n y dimensión k sobre $\mathbb{F}_2$ es llamado un $[n,k]-$código lineal. Si la distancia mínima d es conocida, decimos que $\mathcal{C}$ es un $[n,k,d]-$código lineal binario.

Definición 4.1.4 Una *matriz generadora* para un código lineal $\mathcal{C}$ es una matriz G cuyas filas forman una base para $\mathcal{C}$.

Definición 4.1.5 Una *matriz verificadora de paridad* H para un código lineal $\mathcal{C}$ es una matriz generadora para el código dual $\mathcal{C}^\perp$.

Observaciones 4.1.6 ([46], Observaciones 4.5.2)

- Si $\mathcal{C}$ es un $[n,k]-$código lineal, entonces su matriz generadora G es una matriz de tamaño $k \times n$ y su matriz verificadora de paridad H es una matriz de tamaño $(n-k) \times n$.
- Dado que existe más de una base para un espacio vectorial, tenemos que existe más de una matriz generadora para un código lineal. Además, aun cuando la base sea fija, una permutación (distinta de la identidad) de las filas de una matriz generadora también conduce a una matriz generadora diferente.
- Las filas de una matriz generadora son linealmente independientes. Lo mismo sucede para las filas de una matriz verificadora de paridad. De hecho para mostrar que una matriz G de tamaño $k \times n$ es una matriz generadora para un $[n,k]-$código lineal dado, basta con mostrar que las filas de G son palabras-código de $\mathcal{C}$ y que son linealmente independientes. Alternativamente, esto se puede hacer mostrando que $\mathcal{C}$ está contenido en el espacio de filas de G.

Definición 4.1.7 Sea $\mathcal{C}$ un $[n,k]-$código lineal.

- Si la matriz generadora de $\mathcal{C}$ es de la forma $(I_k|X)$ se dice que está en su forma estándar.

- Si la matriz verificadora de paridad de $\mathcal{C}$ es de la forma $(Y|I_{n-k})$ se dice que está en su forma estándar.

Teorema 4.1.8 Sea $\mathcal{C}$ un $[n,k]-$código lineal con matriz generadora G. Sea $v \in \mathbb{F}_2^n$, entonces $v \in \mathcal{C}^\perp$ si y solo si v es ortogonal a cada fila de G, es decir, $v \in \mathcal{C}^\perp$ si y solo si $Gv^T = 0$. En particular, dada una matriz H de tamaño $(n-k) \times n$, tenemos que H es la matriz de verificadora de paridad de $\mathcal{C}$ si y solo si las filas de H son linealmente independientes y $GH^T = 0$. (c.f [46])

Observación 4.1.9 Una formulación equivalente del Teorema 4.1.8 es la siguiente:

Sea $\mathcal{C}$ un $[n,k]-$código lineal con matriz verificadora de paridad H. Sea $v \in \mathbb{F}_2^n$, entonces $v \in \mathcal{C}$ si y solo si v es ortogonal a cada fila de H, es decir, $v \in \mathcal{C}$ si y solo si $Hv^T = 0$. En particular, dada una matriz G de tamaño $k \times n$, tenemos que G es la matriz generadora de $\mathcal{C}$ si y solo si las filas de G son linealmente independientes y $HG^T = 0$.

Corolario 4.1.10 ([46], Teorema 4.5.9) Si $G = (I_k|X)$ es la forma estándar de una matriz generadora de un $[n,k]-$código lineal $\mathcal{C}$, entonces la matriz verificadora de paridad de $\mathcal{C}$ es $H = (-X^T|I_{n-k})$.

Ejemplo 4.1.11 Sea $\mathcal{C}$ el $[n,1]-$código lineal que sólo contiene las palabras código $(0\ldots0)$ y $(1\ldots1)$, el cual es llamado *código binario de repetición de longitud* n, cuya matriz generadora es

$$G = (1 \mid 1\ldots1)$$

la cual está en su forma estándar. Así que su matriz verificadora de paridad es

$$H = \left(\begin{array}{c|c} 1 & \\ \vdots & I_{(n-1)} \\ 1 & \end{array}\right).$$

Un dato importante del código binario de repetición de longitud n es que su código dual consiste en todas las $n-$tuplas que tienen peso par, es decir, $\mathcal{C}^\perp = \{(x_1\ldots x_n) \in \mathbb{F}_2^n | x_1 + \cdots + x_n \equiv 0 \mod 2\}$. Este código tomará relevancia en la sección 4.2 por lo que le llamaremos el *código dual del código binario de repetición* y lo denotaremos por $\mathcal{P}$.

Como ya hemos visto podemos obtener un código lineal mediante su matriz generadora o su matriz verificadora de paridad, pero puede que el código no satisfaga algún parámetro que necesitemos, para estos casos existen técnicas que nos ayudan a obtener nuevos códigos a partir de códigos ya conocidos. A nosotros en particular nos va a interesar la longitud del código, dos técnicas que modifican este parámetro es la extensión y perforación del código.

Definición 4.1.12 El proceso de agregar una o más coordenadas a las palabras-código de un código se conoce como *extender* el código. La forma más común

de extender un código es agregando una verificación de paridad general, que se realiza de la siguiente manera. Si $\mathcal{C}$ un $[n,k,d]-$código lineal binario. Definimos el *código extendido* $\widehat{\mathcal{C}}$ como

$$\widehat{\mathcal{C}} = \left\{ (x_1x_2\dots x_nx_{n+1}) \in \mathbb{F}_2^n \middle| (x_1x_2\dots x_n) \in \mathcal{C} \text{ y } \sum_{i=1}^{n+1} x_i = 0 \right\}$$

Observaciones 4.1.13 ([39])

- Todas las palabras-código de $\widehat{\mathcal{C}}$ son de peso par.
- $\widehat{\mathcal{C}}$ es un $[n+1,k,\widehat{d}]-$código lineal donde $\widehat{d} = d$ si d es par y $\widehat{d} = d+1$ si d es impar.
- Si G es matriz generadora de $\mathcal{C}$, entonces la matriz generadora de $\widehat{\mathcal{C}}$ se obtiene agregando una columna a G de tal forma que la suma de las coordenadas de cada fila sea cero.
- Si H es la matriz verificadora de paridad de $\mathcal{C}$, entonces una matriz verificadora de paridad para $\widehat{\mathcal{C}}$ es la matriz

$$\widehat{H} = \left(\begin{array}{ccc|c} 1 & \dots & 1 & 1 \\ \hline & & & 0 \\ & H & & \vdots \\ & & & 0 \end{array}\right).$$

Ejemplo 4.1.14 Sea H la matriz verificadora de paridad del $[7,4,3]-$código de Hamming $\mathcal{H}_3$ (Ver 4.1.1).

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

Al extender $\mathcal{H}_3$ obtenemos un $[8,4,4]-$código lineal con matriz verificadora de paridad

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

Definición 4.1.15 Sea $\mathcal{C}$ un $[n,k,d]-$código lineal binario. *Perforar* el código $\mathcal{C}$ consiste en eliminar una o más coordenadas de cada palabra-código de $\mathcal{C}$, estás palabras-código perforadas forman un nuevo código lineal llamado *código perforado* y que suele ser denotado por $\mathcal{C}^*$.

Observaciones 4.1.16

- Si eliminamos r coordenadas entonces $\mathcal{C}^*$ es un código de longitud $n-r$.
- Si G es la matriz generadora de $\mathcal{C}$, entonces la matriz generadora de $\mathcal{C}^*$ se obtiene a partir de la eliminación de las columnas correspondientes a las coordenadas que se desean eliminar [39].
- El software *SageMath* nos permite hacer uso de esta técnica, pero hay que tener cuidado ya que el software comienza a contar todo desde cero, es decir, la primera coordenada en *SageMath* será la coordenada cero.

Teorema 4.1.17 Sea $\mathcal{C}$ un $[n,k,d]-$código lineal binario con $d>1$ y sea $\mathcal{C}^*$ el código $\mathcal{C}$ perforado en la $i-$ésima coordenada. Entonces $\mathcal{C}^*$ es un $[n,k,d^*]$ código lineal, donde $d^*=d-1$ si la palabra-código de $\mathcal{C}$ cuyo peso es d, tiene la $i-$ésima coordenada distinta cero, en otro caso $d^*=d$.(c.f [39])

Ejemplo 4.1.18 Sea $\mathcal{C}=\{00000,11000,00111,11111\}$ un $[5,2,2]-$código lineal binario, donde 11000 es la palabra-código con menor peso. Si perforamos a $\mathcal{C}$ en la primera coordenada, $\mathcal{C}_1^*=\{0000,1000,0111,1111\}$ el cual es un $[4,2,1]-$código lineal. Si ahora perforamos a $\mathcal{C}$ en la coordenada 5, $\mathcal{C}_5^*=\{0000,1100,0011,1111\}$ el cual es un $[4,2,2]-$código lineal.

4.1.1. Códigos de Hamming

Los códigos de Hamming son probablemente los códigos correctores de errores más famosos. Fueron descubiertos de forma independiente por Marcel Golay en 1949 y Richard Hamming en 1950. Son códigos correctores de un solo error, muy faciles de códificar y decodificar. [5]

Si bien los códigos de Hamming se definen sobre todos los campos finitos $\mathbb{F}_q$, únicamente trabajaremos con los códigos binarios de Hamming. Si el lector quisiera abordar más sobre esta familia de códigos recomendamos revisar [5] y [52].

Sean $r\geq 2, n=2^r-1$ y $\mathbb{F}_2^r$, como $|\mathbb{F}_2^r\setminus\{0\}|=2^r-1$, hay 2^r-1 $r-$tuples binarios distintos de cero.

Definición 4.1.19 Definimos la $r\times(2^r-1)$ matriz de chequeo de paridad H_r cuyas columnas en orden son los bits de las representaciones binarias de los números $1,2,\ldots,2^r-1$ (es decir, H_r está formada por el conjunto de todos los $r-$tuples binarios distintos de cero como sus columnas). El *código lineal binario de Hamming* $\mathcal{H}_r$ de longitud $n=2^r-1$ $(r\geq 2)$ es el espacio de soluciones del sistema lineal homogéneo dado por la matriz H_r.

Teorema 4.1.20 $\mathcal{H}_r$ es un $[n=2^r-1,k=2^r-1-r,3]-$código lineal binario. (c.f [5])

Ejemplo 4.1.21 Sea $r=3$, $\mathcal{H}_3$ es un $[7,4,3]-$código lineal binario de Hamming con matriz de verificadora de paridad

$$H=\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}.$$

4.1.2. Códigos LDPC

Los códigos de verificación de paridad de baja densidad conocidos como códigos LDPC por sus siglas en ingles Low Density Parity Check, o también como Códigos de Gallager, fueron inventados por Gallager [33] en 1960 pero fueron olvidados durante casi 30 años porque la complejidad de su decodificación estaba más allá de las capacidades del hardware de la época. En 1981, Tanner [59] los generalizó e introdujo su representación gráfica, los famosos grafos de Tanner. Finalmente en 1997, Mackay y Neal [51] redescubrieron estos códigos y provocaron una intensa investigación al respecto. Desde entonces, los códigos LDPC se han convertido en un área activa de investigación en las aplicaciones en la comunicación digital.

Definición 4.1.22 Un *código LDPC* es un código lineal cuya matriz verificadora de paridad H contiene en su mayoría $0'$s y relativamente pocos $1'$s, es decir, su matriz verificadora de paridad H es dispersa o de baja densidad.

Observación 4.1.23 Decimos que un código LDPC es *regular* si en su matriz verificadora de paridad H, todas las columnas tienen el mismo peso w_c y todas las filas tienen el mismo peso w_r. Por el contrario, si todas las columnas y/o filas de H no tienen el mismo peso decimos que el código LDPC es *irregular.*

Una característica peculiar de los códigos LDPC, es la correspondencia que hay entre la matriz verificadora de paridad H y la matriz de biadyacencia de un grafo bipartito. En base a ésto es posible a representar los códigos LDPC como grafos bipartitos y a su vez construir códigos LDPC a base de grafos bipartitos.

Los grafos que representan los códigos LDPC son llamados *grafos de Tanner*, estos son grafos bipartitos $Z = (X \cup C, E)$ donde los vértices de X reciben el nombre de *vértices de variable* y los vértices de C reciben el nombre de *vértices de restricción o de verificación.* Luego si $H = (h_{ij})$ es la matriz verificadora de un código LDPC, cada columna de H será representada en el grafo como un vértice de variable mientras que cada fila de H será un vértice de restricción, además conectaremos mediante un arista al vértice de variable x_j con el vértice de restricción c_i si y solo si $h_{ij} = 1$.

Observaciones 4.1.24

- Los vértices de variable reciben este nombre ya que estarán relacionados con los bits de las palabras-código. En ocasiones se suele omitir la palabra vértice y solo se les llama variable.
- Los vértices de restricción reciben este nombre ya que tales vértices representan una ecuación de verificación de paridad. En ocasiones se suele abreviar vértice de restricción y solo se les llama restricción.
- La matriz verificadora de paridad H es la matriz de biadyacencia de Z.

- Se suelen usar vértices circulares para los vértices de variable y vértices cuadrados para los vértices de restricción.
- Si $\mathcal{C}$ es un código LDPC $(w_c, w_r)-$regular entonces $Z = (X \cup C, E)$ será un grafo bipartito $(d_X, d_C)-$regular en el cual $w_c = d_X$ y $w_r = d_C$. Por otro lado, si $\mathcal{C}$ es un código LDPC irregular entonces Z será un grafo bipartito irregular.

En la Figura 4.2 se muestra un ejemplo pictórico de la construcción del grafo bipartito para un código LDPC muy simple.

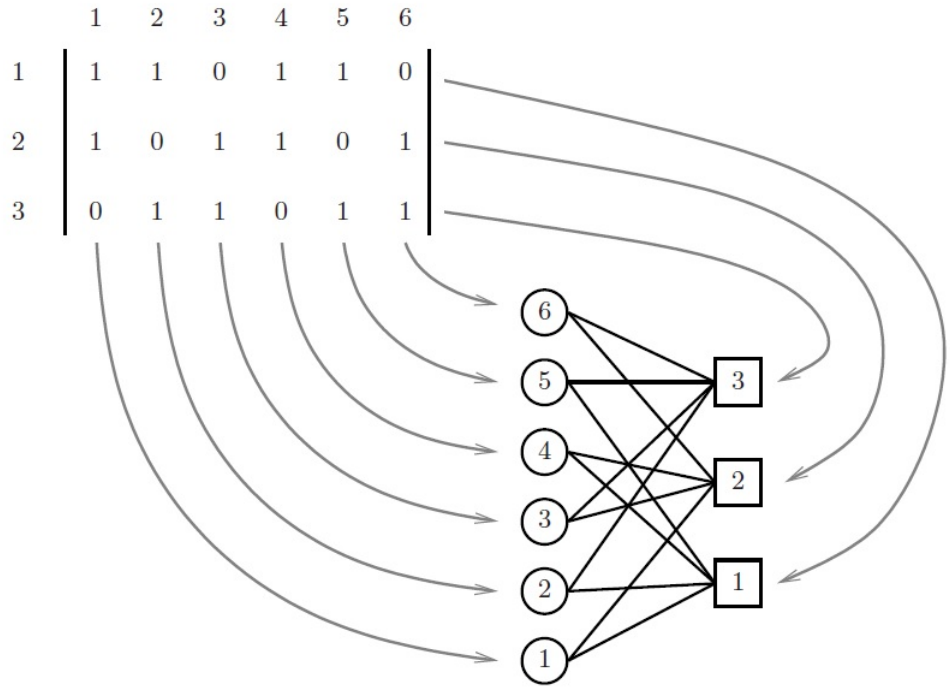


Figura 4.2

Ahora, a partir un grafo bipartito construiremos un código LDPC.

Definición 4.1.25 Sea $Z = (X \cup C, E)$ un grafo bipartito (d_X, d_C)-regular donde X es un conjunto de m vértices de variable, C es un conjunto de n vértices de restricción y $m > n$. Un código $\mathcal{C}(Z)$ de verificación de paridad de baja densidad o simplemente un código LDPC de longitud m es

$$\mathcal{C}(Z) = \{x = (x_1, \ldots, x_m) \in \mathbb{F}_2^m | x_{z(i,1)} + x_{z(i,2)} + \cdots + x_{z(i,d_C)} = 0,\ 1 \leq i \leq n\},$$

donde $z(i, j)$ es una función tal que para cada vértice de restricción c_i, las variables vecinas a c_i son $x_{z(i,1)}, \ldots, x_{z(i,d_C)}$.

Observación 4.1.26 Una forma rápida de definir la función $z(i, j)$ es mediante la matriz de biadyacencia B del grafo $Z = (X \cup C, E)$ ya que para cada $i \in \{1, \ldots n\}$ tenemos que $\{z(i, 1), \ldots, z(i, d_C)\} = \{k \in \{1, \ldots m\} | b_{ki} = 1\}$.

Observación 4.1.27 Desarrollando a fondo la Definición 4.1.25 tenemos que

$$\mathcal{C}(Z) = \left\{ (x_1, x_2, \dots x_m) \in \mathbb{F}_2^m \;\middle|\; \begin{array}{ccc} x_{z(1,1)} + & \dots & +x_{z(1,d_C)} = 0 \\ x_{z(2,1)} + & \dots & +x_{z(2,d_C)} = 0 \\ \vdots & \ddots & \vdots \\ x_{z(i,1)} + & \dots & +x_{z(i,d_C)} = 0 \\ \vdots & \ddots & \vdots \\ x_{z(n,1)} + & \dots & +x_{z(n,d_C)} = 0 \end{array} \right\}.$$

Es decir, obtenemos un sistema de n ecuaciones lineales, donde la $i-$ésima ecuación lineal va a ser la suma de los vértices de variable que son vecinos del vértice de restricción c_i. Luego, la matriz asociada con este sistema de ecuaciones es una matriz verificadora de paridad H de tamaño $n \times m$ para $\mathcal{C}(Z)$. Así que $\mathcal{C}(Z) = \{x \in \mathbb{F}_2^m | Hx^T = 0\}$.

Observación 4.1.28 Es posible generalizar la Definición 4.1.25, introduciendo condiciones más complejas a los vértices. El código resultante se le denomina código LDPC generalizado (o GLDPC). Tanner fue el primero en definir esta clase de códigos, agregando como nueva condición que todos los vértices de restricción estén asociados a un código denominado *código interno* cuya longitud sea igual a d_C. Por lo que ahora una palabra es una palabra-código si y solo si los bits conectados a cada vértice restricción forman una palabra-código del código interno.

Por último, un factor importante para la construcción de buenos códigos LDPC es la cintura de su grafo de Tanner. Recordemos que la cintura de un grafo es la longitud de su ciclo más corto. Chaohui, et.al [34] plantean la importancia de que un código LDPC tenga una cintura grande y cito: "Al decodificar, la circulación de información entre diferentes nodos es provechosa para la corrección de errores. Sin embargo, la circulación de la información se ve obstaculizada por la existencia de ciclos, por lo que la información errónea en los ciclos no puede ser actualizada por información extrínseca en el tiempo y hace que los errores sean difíciles de corregir. A medida que se acorta la longitud de los ciclos, aumenta la frecuencia de reciclaje de información incorrecta y aumenta la dificultad de la corrección de errores.[...] En vista del daño de los ciclos cortos, muchos algoritmos de construcción de códigos LDPC están diseñados para maximizar la cintura de los códigos LDPC, es decir, tratando de evitar generar o eliminar ciclos cortos, y mejorar la conectividad de los ciclos cortos cuando no puedan ser evitados o eliminados."

4.2. Códigos expanders

En 1996, Sipser y Spielman [56] propusieron nuevas familias de códigos detectores correctores de errores asintóticamente buenas mediante familias de grafos expanders. Si un código pertenece a una de estas familias se les denominará código expander, el cual pertenece a la clase de los códigos LDPC generalizados.

En esta sección mostraremos la construcción original de Sipser y Spielman de códigos expanders, así como algunas de sus propiedades y ejemplos.

Definición 4.2.1 Sea $Z = (X \cup C, E)$ un grafo $(d_X, d_C)-$regular donde X es el conjunto de m vértices de variable y C es el conjunto de n vértices de restricción con $n < m$ y $d_X < d_C$. Sea $z(i,j)$ una función diseñada de modo que para cada restricción c_i, las variables vecinas de c_i son $x_{z(i,1)}, \ldots, x_{z(i,d_C)}$. Sea $\mathcal{S}$ un código detector-corrector de errores de longitud d_C. El *código expander* $\mathcal{C}(Z, \mathcal{S})$ es un código de longitud m donde $(y_1 \ldots y_m) \in \mathbb{F}_2^m$ es una palabra código de $\mathcal{C}(Z, \mathcal{S})$ si para cada $1 \leq i \leq n$ $(y_{z(i,1)} \ldots y_{z(i,d_C)})$ es una palabra-código de $\mathcal{S}$.

Observación 4.2.2 En 2001 Zémor [64] redefinió los códigos expander, asignando un código $\mathcal{C}_0$ a X y un código $\mathcal{C}_1$ a C, mejorando propiedades de distancia y decodificación. Para conocer más sobre estos códigos invitamos al lector a revisar [64], [9] [8].

Observación 4.2.3 El hecho de que se utilice la palabra *expander* en estos códigos es por que los mejores grafos que se pueden utilizar para construir estos códigos son los grafos con una buena constante de expansión, para ser más específicos estos deben ser grafos biexpander no balanceados (ver Definición 2.2.15). A lo largo de está sección mencionaremos las propiedades que obtienen estos códigos en base a la expansión del grafo.

Observación 4.2.4 Si $\mathcal{S}$ es un $[d_C, k]-$código lineal con matriz verificadora de paridad H tenemos que $(y_1 \ldots y_m) \in \mathcal{C}(Z, \mathcal{S})$ si y solo si para cada $1 \leq i \leq n$ $H(y_{z(i,1)} \ldots y_{z(i,d_C)})^T = 0$. Entonces,

$$\mathcal{C}(Z,\mathcal{S}) = \left\{ (y_1 \ldots y_m) \in \mathbb{F}_2^m \;\middle|\; \begin{array}{ccccc}
h_{1,1}\, y_{z(1,1)} & + & \ldots & + & h_{1,d_C}\, y_{z(1,d_C)} = 0 \\
h_{2,1}\, y_{z(1,1)} & + & \ldots & + & h_{2,d_C}\, y_{z(1,d_C)} = 0 \\
\vdots & & \ddots & & \vdots \\
h_{d_C-k,1}\, y_{z(1,1)} & + & \ldots & + & h_{d_C-k,d_C}\, y_{z(1,d_C)} = 0 \\
h_{1,1}\, y_{z(2,1)} & + & \ldots & + & h_{1,d_C}\, y_{z(2,d_C)} = 0 \\
\vdots & & \ddots & & \vdots \\
h_{d_C-k,1}\, y_{z(1,1)} & + & \ldots & + & h_{d_C-k,d_C}\, y_{z(2,d_C)} = 0 \\
\vdots & & \ddots & & \vdots \\
h_{1,1}\, y_{z(i,1)} & + & \ldots & + & h_{1,d_C}\, y_{z(i,d_C)} = 0 \\
\vdots & & \ddots & & \vdots \\
h_{d_C-k,1}\, y_{z(i,1)} & + & \ldots & + & h_{d_C-k,d_C}\, y_{z(i,d_C)} = 0 \\
\vdots & & \ddots & & \vdots \\
h_{1,1}\, y_{z(n,1)} & + & \ldots & + & h_{1,d_C}\, y_{z(n,d_C)} = 0 \\
\vdots & & \ddots & & \vdots \\
h_{d_C-k,1}\, y_{z(n,1)} & + & \ldots & + & h_{d_C-k,d_C}\, y_{z(n,d_C)} = 0
\end{array} \right\}$$

Es decir, obtenemos un sistema de $(d_C - k)n$ ecuaciones lineales, donde la matriz asociada a este sistema de ecuaciones es una matriz verificadora de paridad $\widehat{H}$ de tamaño $d_C \times (d_C - k)n$ para $\mathcal{C}(Z, \mathcal{S})$. Por lo tanto, $\mathcal{C}(Z, \mathcal{S}) = \{y \in \mathbb{F}_2^m | \widehat{H} y^T = 0\}$.

Ejemplo 4.2.5 Consideremos el siguiente grafo bipartito $Z_1 = (X \cup C, E)$.

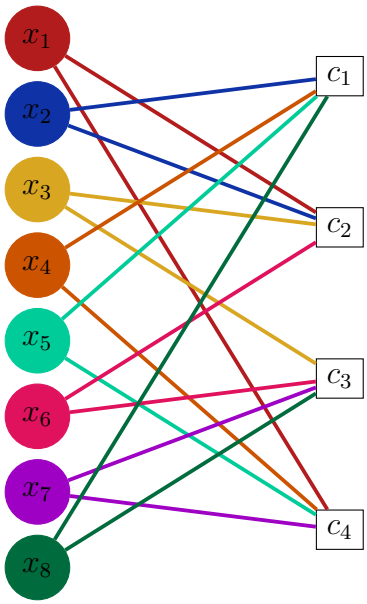


Figura 4.3: Grafo bipartito $(2,4)-$regular Z_1 con 8 vértices de variable y 4 vértices de restricción.

Recordemos que una forma rápida para definir la función $z(i,j)$ es mediante la matriz de biadyacencia del grafo Z_1 (ver observación 4.1.26). Sea B la matriz de biayacencia de Z_1

$$B = \begin{array}{c} \begin{matrix} c_1 & c_2 & c_3 & c_4 \end{matrix} \\ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \end{array} \begin{matrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{matrix}.$$

Para cada $1 \leq i \leq 4$ tenemos que $\{z(i,1), \ldots, z(i,4)\} = \{1 \leq k \leq 8 | b_{ki} = 1\}$. Entonces

$$\begin{pmatrix} z(1,1) & z(1,2) & z(1,3) & z(1,4) \\ z(2,1) & z(2,2) & z(2,3) & z(2,4) \\ z(3,1) & z(3,2) & z(3,3) & z(3,4) \\ z(4,1) & z(4,2) & z(4,3) & z(4,4) \end{pmatrix} = \begin{pmatrix} 2 & 4 & 5 & 8 \\ 1 & 2 & 3 & 6 \\ 3 & 6 & 7 & 8 \\ 1 & 4 & 5 & 7 \end{pmatrix}.$$

Luego, consideremos como código interno a $\mathcal{S} = \{0000, 0100, 1011, 1111\}$ un $[4,2]-$código lineal con matriz verificadora de paridad

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Por definición tenemos que $(y_1 \dots y_8) \in \mathcal{C}(Z_1, \mathcal{S})$ si y solo si para cada $1 \leq i \leq 4$ se cumple que

$$H \begin{pmatrix} y_{z(i,1)} \\ y_{z(i,2)} \\ y_{z(i,3)} \\ y_{z(i,4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

- Para i=1

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = H \begin{pmatrix} y_{z(i,1)} \\ y_{z(i,2)} \\ y_{z(i,3)} \\ y_{z(i,4)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_2 \\ y_4 \\ y_5 \\ y_8 \end{pmatrix} = \begin{pmatrix} y_2 + y_8 \\ y_5 + y_8 \end{pmatrix}.$$

  Así que

$$y_2 + y_8 = 0 \tag{4.1}$$
$$y_5 + y_8 = 0 \tag{4.2}$$

- Para i=2

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = H \begin{pmatrix} y_{z(i,1)} \\ y_{z(i,2)} \\ y_{z(i,3)} \\ y_{z(i,4)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_6 \end{pmatrix} = \begin{pmatrix} y_1 + y_6 \\ y_3 + y_6 \end{pmatrix}.$$

  Así que

$$y_1 + y_6 = 0 \tag{4.3}$$
$$y_3 + y_6 = 0 \tag{4.4}$$

- Para i=3

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = H \begin{pmatrix} y_{z(i,1)} \\ y_{z(i,2)} \\ y_{z(i,3)} \\ y_{z(i,4)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_3 \\ y_6 \\ y_7 \\ y_8 \end{pmatrix} = \begin{pmatrix} y_3 + y_8 \\ y_7 + y_8 \end{pmatrix}.$$

  Así que

$$y_3 + y_8 = 0 \tag{4.5}$$
$$y_7 + y_8 = 0 \tag{4.6}$$

- Para i=4

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = H \begin{pmatrix} y_{z(i,1)} \\ y_{z(i,2)} \\ y_{z(i,3)} \\ y_{z(i,4)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_4 \\ y_5 \\ y_7 \end{pmatrix} = \begin{pmatrix} y_1 + y_7 \\ y_5 + y_7 \end{pmatrix}.$$

Así que

$$y_1 + y_7 = 0 \tag{4.7}$$
$$y_5 + y_7 = 0 \tag{4.8}$$

Las ecuaciones lineales 4.1,4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8 forman un sistema de 8 ecuaciones lineales de donde se obtiene la siguiente matriz

$$\widetilde{H_1} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

la cual es una matriz verificadora del código $\mathcal{C}(Z_1, S)$ y para obtener todas sus palabras-código haremos uso del software *SageMath* V.10.0 [61].

```
[1]: H1=Matrix(GF(2), [[0,1,0,0,0,0,0,1],\
                       [0,0,0,0,1,0,0,1],\
                       [1,0,0,0,0,1,0,0],\
                       [0,0,1,0,0,1,0,0],\
                       [0,0,1,0,0,0,0,1],\
                       [0,0,0,0,0,0,1,1],\
                       [1,0,0,0,0,0,1,0],\
                       [0,0,0,0,1,0,1,0]])
     ExpanderCode1=codes.from_parity_check_matrix(H1)
     ExpanderCode1
```

```
[1]: [8, 2] linear code over GF(2)
```

```
[2]: ExpanderCode1.list()
```

```
[2]: [(0, 0, 0, 0, 0, 0, 0, 0),
      (1, 1, 1, 0, 1, 1, 1, 1),
      (0, 0, 0, 1, 0, 0, 0, 0),
      (1, 1, 1, 1, 1, 1, 1, 1)]
```

Por último, verificaremos que al restringir las palabras-código de $\mathcal{C}(Z_1, \mathcal{S})$ en las posiciones $z(i,1), z(i,1), z(i,3), z(i,4)$ con $i \in \{1, \ldots 4\}$ obtenemos palabras-

código de $\mathcal{S}$. A continuación se muestra el caso $i = 1$

$$\begin{array}{l}
(0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0) = (0000) \in \mathcal{S} \\
(1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1) = (1011) \in \mathcal{S} \\
(0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0) = (0100) \in \mathcal{S} \\
(1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1) = (1111) \in \mathcal{S}
\end{array}$$

Para los demás casos, decidimos perforar $\mathcal{C}(Z_1, \mathcal{S})$ (ver Definición 4.1.15) con ayuda del software *SageMath* V.10.0 [61]. Los códigos de *SageMath* se pueden consultar en B.2.

Observación 4.2.6 Un ejemplo simple de códigos expander se obtiene utilizando un grafo biexpander Z y el código dual del código de repetición $\mathcal{P}$ (ver Ejemplo 4.1.11). La matriz de chequeo de paridad del código expander $\mathcal{C}(Z, \mathcal{P})$ es la matriz transpuesta de la matriz de biadyacencia del grafo Z. [56]

Ejemplo 4.2.7 Consideremos el siguiente grafo bipartito $Z_2 = (X \cup C, E)$

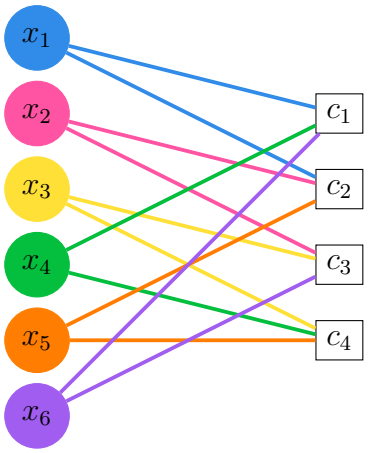


Figura 4.4: Grafo bipartito $(2, 3)-$regular Z_2 con 6 vértices de variable y 4 vértices de restricción.

A igual que en el Ejemplo 4.2.5 definiremos la función $z(i, j)$ mediante la matriz de biadyacencia del grafo Z_2 (ver observación 4.1.26). Sea B la matriz transpuesta de la matriz de biadyacencia de Z_2.

$$B = \begin{array}{c} \begin{array}{cccc} c_1 & c_2 & c_3 & c_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \end{array} \begin{array}{l} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{array}$$

Para cada $1 \leq i \leq 4$ tenemos que $\{z(i,1), \ldots, z(i,3)\} = \{1 \leq k \leq 6 | b_{ki} = 1\}$. Entonces

$$\begin{pmatrix} z(1,1) & z(1,2) & z(1,3) \\ z(2,1) & z(2,2) & z(2,3) \\ z(3,1) & z(3,2) & z(3,3) \\ z(4,1) & z(4,2) & z(4,3) \end{pmatrix} = \begin{pmatrix} 1 & 4 & 6 \\ 1 & 2 & 5 \\ 2 & 3 & 6 \\ 3 & 4 & 5 \end{pmatrix}.$$

Consideremos como código interno a $\mathcal{P} = \{000, 101, 011, 110\}$ el código dual del código de repetición de longitud 3. Por el Ejemplo 4.1.11 tenemos que $H = (111)$ es una matriz verificadora para $\mathcal{P}$. De acuerdo con la definición de código expander tenemos que $(y_1 \ldots y_6) \in \mathcal{C}(Z_2, \mathcal{P})$ si y solo si para cada $1 \leq i \leq 4$ se cumple que

$$H \begin{pmatrix} y_{z(i,1)} \\ y_{z(i,2)} \\ y_{z(i,3)} \end{pmatrix} = 0 \tag{4.9}$$

Pero como $H = (111)$, la ecuación 4.9 nos va a arrojar que $y_{z(i,1)} + y_{z(i,2)} + y_{z(i,3)} = 0$ para cada $1 \leq i \leq 4$. Formando así el sistema de 4 ecuaciones 4.10.

$$\begin{cases} y_1 + y_4 + y_6 = 0 \\ y_1 + y_2 + y_5 = 0 \\ y_2 + y_3 + y_6 = 0 \\ y_3 + y_4 + y_5 = 0 \end{cases} \tag{4.10}$$

Notemos que al determinar la matriz $\widetilde{H}_2$ asociada al sistema obtenemos la matriz transpuesta de la matriz de biadyacencia B del grafo Z_2, debido a que para cada $1 \leq i \leq 4$ definimos $\{z(i,1), z(i,2), z(i,3)\} = \{1 \leq k \leq 6 | b_{ki} = 1\}$.

$$\widetilde{H}_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}^T = B^T$$

Dado que $\widetilde{H}_2$ es una matriz verificadora del código $\mathcal{C}(Z_2, \mathcal{P})$, obtendremos las palabras-código del código expander con ayuda del software *SageMath* V.10.0 [61].

```
[1]: H2=Matrix(GF(2), [[1, 0, 0, 1, 0, 1],\
                       [1, 1, 0, 0, 1, 0],\
                       [0, 1, 1, 0, 0, 1],\
                       [0, 0, 1, 1, 1, 0]])
     ExpanderCode2=codes.from_parity_check_matrix(H2)
     ExpanderCode2
```

```
[1]: [6, 3] linear code over GF(2)
```

```
[2]: ExpanderCode2.list()
```

```
[2]: [(0, 0, 0, 0, 0, 0),
      (1, 0, 0, 1, 1, 0),
      (0, 1, 0, 1, 1, 1),
      (1, 1, 0, 0, 0, 1),
      (0, 0, 1, 1, 0, 1),
      (1, 0, 1, 0, 1, 1),
      (0, 1, 1, 0, 1, 0),
      (1, 1, 1, 1, 0, 0)]
```

Para que el código expander $\mathcal{C}(Z, \mathcal{S})$ sea un buen código necesitamos que Z sea un grafo biexpander no balanceado (ver Definición 2.2.15) con constante de expansión grande y que el código interno $\mathcal{S}$ tenga buena distancia mínima. En la siguiente proposición se refleja la necesidad de estas dos condiciones para obtener una cota para la distancia mínima del código expander.

Teorema 4.2.8 ([56], Teorema 7) Sea $Z = (X \cup C, E)$ un $(m, n, d_X, d_C, \frac{d_X}{d(\mathcal{S})})-$ biexpander y $\mathcal{S}$ un código detector-corrector de errores con longitud d_C y distancia mínima $d(\mathcal{S})$. Entonces la distancia mínima del código expander $\mathcal{C}(Z, \mathcal{S})$ es por lo menos $\frac{m}{2}$.

Demostración.

Supongamos que $d(\mathcal{C}(Z, \mathcal{S})) < \frac{m}{2}$. Entonces existe una palabra-código distinta de cero, digamos w tal que $wt(w) < m/2$. Sea V el conjunto de vértices de variable que son distintas de cero en w, entonces $|V| < m/2$. Como Z es biexpander no balanceado tenemos que $|\partial V| \geq \frac{d_X}{d(\mathcal{S})}|V|$, es decir, V tiene más de $\frac{d_X}{d(\mathcal{S})}|V|$ vértices de restricción como vecinos. Por otro lado como los elementos de X tienen grado d_X tenemos que salen $d_X|V|$ aristas de V. Entonces si calculamos el número de aristas que inciden en promedio en cada restricción vecina de V tenemos que

$$\frac{d_X|V|}{|\partial V|} < \frac{d_X|V|}{\frac{d_X}{d(\mathcal{S})}|V|} = d(\mathcal{S}),$$

por lo que debe existir un vértice de restricción, digamos c', que tenga menos de $d(\mathcal{S})$ vecinos en V, pero como las variables vecinas de c' forman una palabra-código de $\mathcal{S}$ debe tener al menos $d(\mathcal{S})$ variables vecinas distintas de cero, por lo que w no puede ser una palabra código de $\mathcal{C}(Z, \mathcal{S})$. Así que $d(\mathcal{C}(Z, \mathcal{S})) \geq m/2$. ■

Ejemplo 4.2.9 En el Ejemplo 4.2.7 el grafo Z_2 es un $(6, 4, 2, 3, 1)-$biexpander (para ver los cálculos de su constante de expansión consulte B.3). Y $\mathcal{P}$ es un código con distancia mínima igual a 2. Entonces $\frac{d_X}{d(\mathcal{P})} = \frac{2}{2} = 1$ que es precisamente la expansión de Z_2, así que en base al Teorema 4.2.8 la distancia de $\mathcal{C}(Z_2, \mathcal{P})$ debe ser por lo menos 3 y al observar las palabras-código obtenidas en el ejemplo podemos comprobar que en efecto la distancia mínima de $\mathcal{C}(Z_2, \mathcal{P})$ es igual a 3.

En el caso del Ejemplo 4.2.5 el grafo Z_1 es un $(8, 4, 2, 4, \frac{3}{4})-$biexpander (para ver los cálculos de su constante de expansión consulte B.1). Y $\mathcal{S}$ es un código con distancia mínima igual a 1. Entonces $\frac{d_X}{d(\mathcal{S})} = \frac{2}{1} = 2 > \frac{3}{4}$ por lo que $\mathcal{C}(Z_1, \mathcal{S})$ no satisface el Teorema 4.2.8, es decir, la distancia $\mathcal{C}(Z_1, \mathcal{S})$ no es a lo más 4, de hecho al observar sus palabras-código tenemos que su distancia es 1.

4.2.1. Decodificación: Algoritmo de decodificación secuencial

Una ventaja de los códigos expanders es su decodificación. Sipser y Spielman dan un algoritmo de decodificación secuencial basado en el bit-flipping para la decodificación de estos códigos.

Definición 4.2.10 Decimos que una restricción c_i es *satisfecha* si

$$x_{z(i,1)} + x_{z(i,2)} + \ldots x_{z(i,d_C)} \equiv 0 \mod 2,$$

es decir, si la suma de las variables vecinas a c_i es congruente a 0 mód 2. De lo contrario, decimos que c_i es una restricción *insatisfecha*.

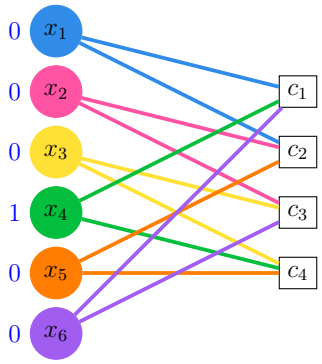
Supongamos que recibimos una palabra $w = (w_1, \ldots, w_n)$, asignamos el valor w_i al vértice de variable x_i para cada $i \in \{1, \ldots, n\}$. Luego determinemos si las restricciones se satisfacen o no y localicemos a la variable que este conectada a más restricciones insatisfechas, a esta variable le vamos a cambiar su valor, es decir, si la variable tenia asignada el valor 1 lo cambiaremos a 0 y viceversa. Después volvemos a determinar si las restricciones se satisfacen o no, si aún hay restricciones insatisfechas buscamos nuevamente la variable con más restricciones insatisfechas y cambiamos su valor. Repetimos este proceso hasta que todas las restricciones queden satisfechas. Y los valores obtenidos en las variables son los bit de nuestra palabra decodificada.

Algoritmo de decodificación secuencial simple.

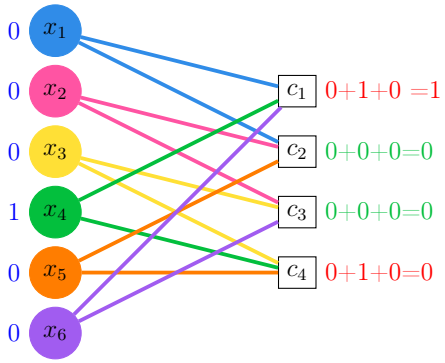
- Si hay una variable que tiene más restricciones insatisfechas que satisfechas, invierta su valor.

- Repita hasta que no quede ninguna variable de ese tipo.

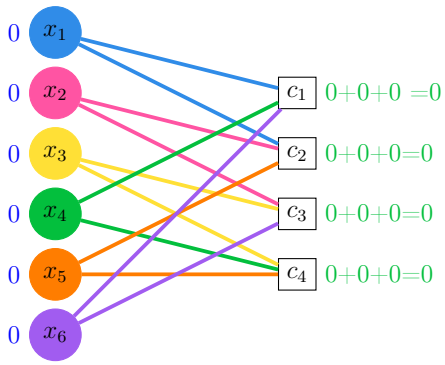
Ejemplo 4.2.11 Consideremos el código expander generado en el Ejemplo 4.2.7. Supongamos que enviamos la palabra (000000) y recibimos la palabra (000100). Así que procedemos a asignar a cada bit de la palabra a un vértice de variable como se muestra en la siguiente figura.



Al determinar el estatus de las restricciones tenemos que c_1 y c_4 son insatisfechas.



La variable que está conectada a ambas restricciones c_1 y c_4 es x_4 así que cambiaremos su valor a 0. Y volvemos a determinar el estatus de todas las restricciones.



Esta vez tenemos que todas se satisfacen. Por lo tanto la palabra que fue enviada es (000000).

La siguiente implementación del algoritmo de decodificación simple es dada por Sipser y Spielman en [56] y a partir de ella se dan los Teoremas 4.2.12 y 4.2.14.

Entrada: Un grafo bipartito no balanceado $(d_X, d_C)-$regular $B = (X \cup C, E)$ con n vértices variables, m vértices de restricción y una asignación de valores a las variables.

Fase de configuración

Para cada restricción determine si es satisfecha o no por las variables.

Inicializar los conjuntos $S_0, \ldots, S_{d_X}$ a conjuntos vacíos.

Para cada variable cuente el número de restricciones insatisfechas en las que aparece. Si el número es i, entonces coloque esa variable en el conjunto S_i.

Bucle
  Mientras los conjuntos $S_{\lceil d_X/2 \rceil}, \ldots, S_{d_X}$ estén vacíos **hacer**
    Encontrar el mayor i tal que si S_i no este vacío.
    Elegir una variable v del conjunto S_i.
    Cambiar el valor de la variable v
    Para cada restricción c que sea vecina de v **hacer**
      Actualice el estatus de la restricción c.
      Para cada variable w vecina de la restricción c **hacer**
        Vuelva a calcular el número de restricciones insatisfechas en las que aparece w.
        Mueva w al conjunto indexado por este número.
      Fin Para
    Fin Para
  Fin Mientras
Fin Bucle
Si todas las variables están en S_0 **entonces**
  emita los valores de las variables
si no
  informe "fallo al decodificar".
Fin Si

Teorema 4.2.12 ([56], Teorema 10) Sea Z un $(m, n, d_X, d_C, \frac{3d_X}{4})-$expander. Sea $\mathcal{P}$ el código dual del código de repetición de longitud d_X. Entonces el algoritmo de decodificación secuencial simple corregirá $m/4$ errores del código $\mathcal{C}(Z, \mathcal{P})$.

Observación 4.2.13 Una característica importante de la decodificación de códigos expanders es que esta se puede hacer en tiempo lineal, nosotros no abordaremos esta característica pero si el lector quisiera indagar más en ello lo invitamos a leer [56] y [57] .

El Teorema 4.2.12 nos dice que dado un grafo con cierta expansión, el algoritmo de decodificación simple corregirá ciertos errores, así que la expansión del grafo es muy importante para el funcionamiento del algoritmo, es más el algoritmo solo funcionará si el grafo que utilizamos tiene buena expansión, es decir, es expander. El siguiente Teorema prueba lo anterior.

Teorema 4.2.14 ([56],Teorema 24) Sea $Z = (X \cup C)$ un grafo bipartito $(d_X, d_C)-$regular con m vértices de variable y n vértices de restricción y $d_X < d_C$ tal que el algoritmo de decodificación secuencial simple decodifica con éxito conjuntos de a lo más αm errores en el código $\mathcal{C}(Z, \mathcal{P})$. Entonces todos los conjuntos de αm variables deben tener por lo menos

$$\alpha m \left(1 + \frac{2\frac{d_X - 1}{2d_C}}{3 + \frac{d_X - 1}{2d_C}} \right)$$

vecinos.

Actualmente se siguen desarrollando mejores algoritmos de decodificación para estos códigos. En la siguiente tabla se muestran los avances que se han tenido.

Algoritmo de decodificación para $\mathcal{C}(Z, \mathcal{S})$ con Z un $(m, n, d_X, d_C, \varepsilon)-$biexpander				
	Expansión necesaria	**Condiciones sobre $\mathcal{S}$**	**Número de errores corregidos**	**Tiempo**
Sipser y Spielman 1996 [56]	$\varepsilon > \frac{3d_X}{4}$	Código dual del código de repetición de longitud d_X	$\frac{m}{4}$	Lineal
Feldman et.al 2007 [30]	$\varepsilon > \frac{2}{3} + \frac{1}{3d_X}$	Lineal	$\left(\frac{3\varepsilon - 2}{2\varepsilon - 1}\right)\frac{m}{2}$	Polinomial
Chilppagari 2010 [21]	$\varepsilon > \frac{l+2}{2(l+1)}$	$d(\mathcal{S}) \geq 2l - 1$ con $l > 1$	$\frac{m}{2}$	Lineal
Viderman 2013 [62]	$\varepsilon > \frac{2}{3} - \frac{1}{6d_X}$	Lineal	$\frac{m}{2}$	Lineal
Dowling y Gao 2018 [27]	$\varepsilon > 0$	$d(\mathcal{S}) \geq 2t + d_x(t-1)^2 - 1$ con $t > \frac{1}{\varepsilon}$	$\frac{m}{2}$	Lineal
Chen et.al 2023 [20]	$\varepsilon > \frac{3}{4}$	Lineal	$\left(\frac{3\varepsilon d_X}{16(1-\varepsilon)} - \eta\right) m$ con $\eta > 0$	Lineal

4.2.2. Construcción explícita

Los grafos biexpanders no balanceados con buena expansión son construidos de manera aleatoria. A pesar de ello existe un método para obtener grafos bipartitos no balanceados mediante un grafo de incidencia arista-vértice obtenido de un grafo $d-$regular Y. Recordemos que si Y tiene una constante de expansión espectral pequeña (Definición 2.3.21) entonces Y será un buen expander. Así que ahora nos enfocaremos en la constante de expansión espectral de Y, y a partir de esta daremos una nueva cota para la distancia mínima de códigos expanders construidos mediante grafos de incidencia arista-vértice.

Definición 4.2.15 Sea $Y = (V, E)$ un grafo, el *grafo de incidencia arista-vértice* Z es un grafo bipartito con conjunto de vértices $E \cup V$ y con conjunto de aristas $\{(e, v) \in E \times V : v \text{ es incidente con } e\}$.

Proposición 4.2.16 Sea $Y = (V, E)$ un grafo $d-$regular con n vértices, entonces el grafo de incidencia vértice-arista obtenido de Y es un grafo bipartito Z $(d, 2)-$regular en el que su partición izquierda tiene $\frac{nd}{2}$ vértices y su partición derecha tiene n vértices.

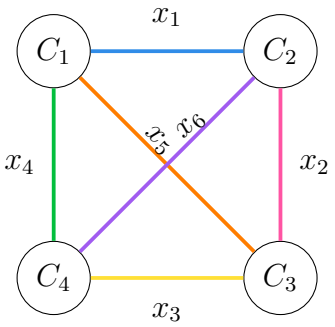
Demostración.

Dado que la partición derecha de Z son los vértices de Y entonces hay n vértices en la partición y como salen d aristas de cada vértice de Y tenemos que el grado de los vértices de la partición derecha es d. Luego para obtener el número de elementos de la partición izquierda hay que calcular el número total de aristas de Y, para ello notemos que cada arista incidente a $v \in V$ se cuenta dos veces en el grado de v que denotamos por $d_Y(v)$ entonces la suma $\sum_{v \in V} d_Y(v)$ cuenta $2|E|$, por lo que

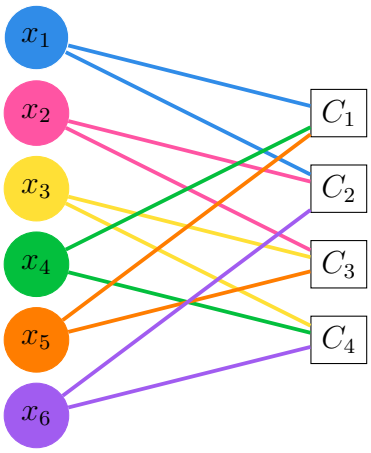
$$|E| = \tfrac{1}{2} \sum_{v \in V} d_Y(v) = \tfrac{1}{2} \sum_{v \in V} d = \tfrac{1}{2}|V|d = \frac{nd}{2},$$

así que la partición izquierda de Z tiene $\frac{nd}{2}$ vértices. Por último como cada arista de Y es incidente a dos vértices, tenemos que el grado de cada vértice en la partición izquierda de Z es 2. ■

Ejemplo 4.2.17 Consideremos el grafo completo K^4 el cual es $3-$regular. Para construir su grafo de incidencia arista-vértice debemos considerar a las aristas de K^4 como los elementos de la partición izquierda y a los vértices de K^4 como los elementos de la partición derecha. Luego para conectar un elemento x_i de la partición izquierda con los elementos de la partición derecha debemos fijarnos en aquellos vértices c_j que son incidentes a x_i en K^4. Por ejemplo x_1 solo va a estar conectado a c_1 y c_2 ya que son los únicos vértices de K^4 que inciden en x_1. Siguiendo de esta manera obtenemos un grafo bipartito $(2, 3)-$regular, el cual es precisamente Z_2 del Ejemplo 4.2.7.



(a) K^4.



(b) Grafo de incidencia arista-vértice obtenido de K^4.

Proposición 4.2.18 Sea Y un grafo $d-$regular con matriz de incidencia M y sea Z el grafo de incidencia arista-vértice de Y con matriz de biadyacencia B. Entonces $M = B^T$.

Demostración.

Sea $Y = (V, E)$ un grafo $d-$regular con n vértices y sea Z el grafo de incidencia arista-vértice de Y. Por la proposición 4.2.16 tenemos que Z es un grafo bipartito donde su partición izquierda es el conjunto E con $\frac{nd}{2}$ elementos y su partición derecha es el conjunto V con n elementos. Al ser Z bipartito tenemos que su matriz de biadyacencia B es una matriz de tamaño $\frac{nd}{2} \times n$ donde

$$b_{ij} = \begin{cases} 1 & \text{si } \{e_i, v_j\} \text{ es una arista de } Z \\ 0 & \text{otro caso.} \end{cases}$$

Entonces la matriz transpuesta de B es una matriz de tamaño $n \times \frac{nd}{2}$ donde

$$b_{ji} = \begin{cases} 1 & \text{si } \{e_i, v_j\} \text{ es un arista de Z} \\ 0 & \text{otro caso.} \end{cases}$$

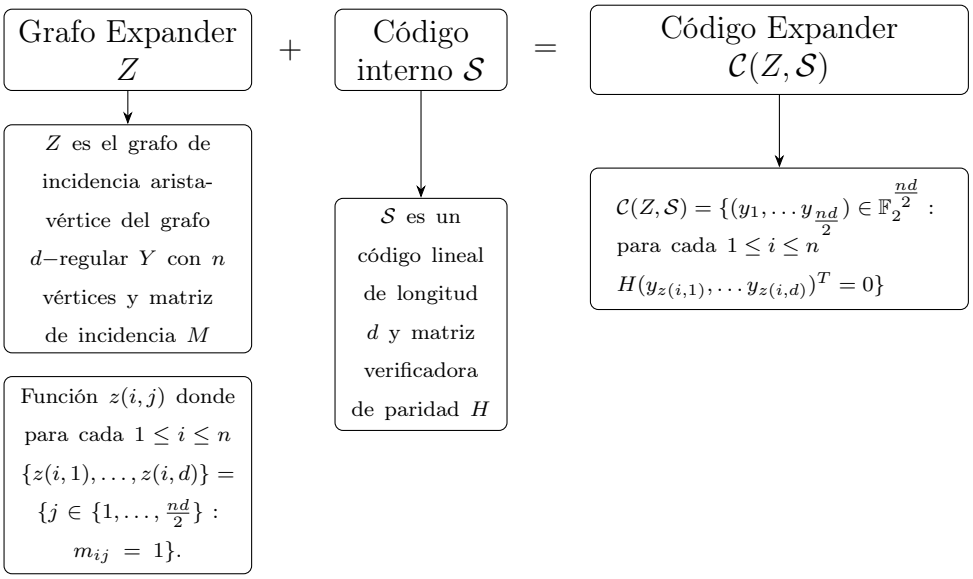
El hecho de que $\{e_i, v_j\}$ sea una arista de Z implica que v_j sea incidente con e_i, así que

$$b_{ji} = \begin{cases} 1 & \text{si } v_j \text{ es incidente con } e_i \\ 0 & \text{otro caso.} \end{cases}$$

Pero esto mismo es lo que deben satisfacer las entradas de la matriz de incidencia M del grafo Y que también es de tamaño $n \times \frac{nd}{2}$. Por lo tanto $M = B^T$. ■

Observación 4.2.19 Con la Proposición 4.2.18 tenemos una forma aun más fácil, que la de la Observación 4.1.26, para obtener la función $z(i, j)$. Si M es la matriz de incidencia de un grafo $d-$regular Y con n vértices, entonces para cada $1 \leq i \leq n$, $\{z(i, 1), \ldots, z(i, d)\} = \{j \in \{1, \ldots, \frac{nd}{2}\} | m_{ij} = 1\}$.

Más aún, si nosotros tenemos un grafo $d-$regular Y con n vértices del cual conocemos su matriz de incidencia M ya no es necesario obtener gráficamente su grafo de incidencia arista-vértice Z ya que la Proposición 4.2.16 y la Observación 4.2.19 nos dan la información de Z que es necesaria para la construcción de un código expander. En el siguiente diagrama se muestran los elementos para construir un código expander a base de grafos regulares con buena constante de expansión espectral.



Ya que para calcular la expansión de un grafo estamos usando la constante de expansión espectral, veamos como influye en la distancia del código expander mediante el siguiente ejemplo.

Ejemplo 4.2.20 Consideremos el grafo de Petersen $P10$ y el grafo de Cayley $Cay(D_{10},\{a,a^4,b\})$, los cuales se muestran en las Figuras 4.6 y 4.7 respectivamente.

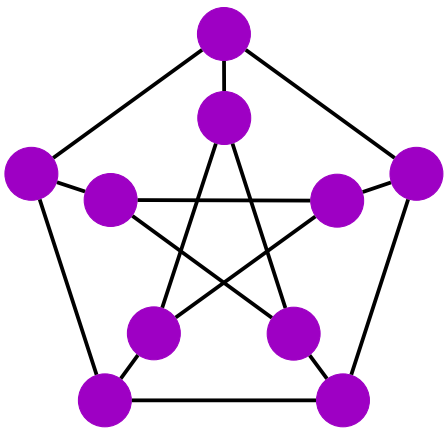


Figura 4.6: Grafo de Petersen $P10$.

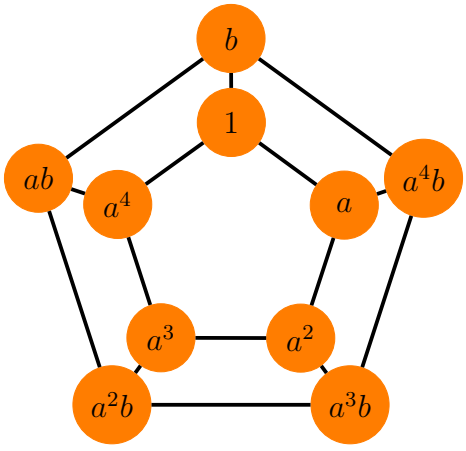


Figura 4.7: $Cay(D_{10},\{a,a^4,b\})$.

Notemos que cada grafo tiene 10 vértices y es 3−regular así que los códigos expanders que pueden generar son de longitud $\frac{10\times 3}{2} = 15$. Pero cada grafo tiene distinta constante de expansión espectral ya que al calcular sus espectros mediante el software *SageMath* V.10.0 [61].

```
[1]: P10= graphs.PetersenGraph()
     P10.spectrum()
```

```
[1]: [3, 1, 1, 1, 1, 1, -2, -2, -2, -2]
```

```
[2]: D = groups.presentation.Dihedral(5)
     Elementos=D.list()
     Generadores = D.gens()
     a=Generadores[0]
     b=Generadores[1]
     a4=a*a*a*a
     S= [a, b, a4]
     D10 = Graph([ Elementos, lambda x, y : x*y^(-1) in␣
      ↪S])
     D10.spectrum()
```

```
[2]: [3, 1.6180339887498895?, 1.6180339887498895?, 1, -0.
      ↪3819660112501051?,
     -0.3819660112501051?, -0.6180339887498895?, -0.
      ↪6180339887498895?,
     -2.6180339887498895?, -2.6180339887498895?]
```

Tenemos que $\lambda(P10) = 2$ y $\lambda(Cay(D_{10}, \{a, a^4, b\})) = 2{,}61$. Entonces $P10$ tiene mejor constante de expansión espectral ya que es más pequeña. Veamos como influye esto en la distancia de sus códigos expanders. Para ello elegiremos de nuevo el código dual del código de repetición $\mathcal{P} = \{000, 101, 011, 110\}$ como nuestro código interno. Sean Z_{P10} y Z_{D10} los grafos de incidencia arista-vértice de $P10$ y $Cay(D_{10}, \{a, a^4, b\})$ respectivamente, por la Observación 4.2.6 tenemos que las matrices verificadoras de paridad de los códigos expanders $\mathcal{C}(Z_{P10}, \mathcal{P})$ y $\mathcal{C}(Z_{D10}, \mathcal{P})$ son las transpuestas de la matrices de biadyacencia de Z_{P10} y Z_{D10} respectivamente, pero gracias a la Proposición 4.2.18 estas matrices son sus matrices de incidencia de $P10$ y $Cay(D_{10}, \{a, a^4, b\})$. Así que con ayuda del software *SageMath* V.10.0 [61] obtendremos cada código expander y sus respectivas distancias.

[3]:
```
MatrizDeIncidenciaP10=P10.incidence_matrix()
MatrizDeIncidenciaP10
```

[3]:
```
[1 1 1 0 0 0 0 0 0 0 0 0 0 0 0]
[1 0 0 1 1 0 0 0 0 0 0 0 0 0 0]
[0 0 0 1 0 1 1 0 0 0 0 0 0 0 0]

[0 0 0 0 0 1 0 1 1 0 0 0 0 0 0]
[0 1 0 0 0 0 0 1 0 1 0 0 0 0 0]
[0 0 1 0 0 0 0 0 0 0 1 1 0 0 0]

[0 0 0 0 1 0 0 0 0 0 0 0 1 1 0]
[0 0 0 0 0 0 1 0 0 0 1 0 0 0 1]
[0 0 0 0 0 0 0 0 1 0 0 1 1 0 0]

[0 0 0 0 0 0 0 0 0 1 0 0 0 1 1]
```

[4]:
```
H3 = Matrix(GF(2), MatrizDeIncidenciaP10)
CEP10=codes.from_parity_check_matrix(H3)
CEP10
```

[4]:
```
[15, 6] linear code over GF(2)
```

[5]:
```
CEP10.minimum_distance()
```

[5]:
```
5
```

[6]:
```
MatrizDeIncidenciaD10=D10.incidence_matrix()
MatrizDeIncidenciaD10
```

[6]:
```
[1 1 1 0 0 0 0 0 0 0 0 0 0 0 0]
[1 0 0 1 1 0 0 0 0 0 0 0 0 0 0]
[0 1 0 0 0 1 1 0 0 0 0 0 0 0 0]
[0 0 1 0 0 0 0 1 1 0 0 0 0 0 0]
[0 0 0 1 0 0 0 0 0 1 1 0 0 0 0]
[0 0 0 0 0 1 0 1 0 0 0 1 0 0 0]
[0 0 0 0 0 0 1 0 0 1 0 0 1 0 0]
[0 0 0 0 1 0 0 0 1 0 0 0 0 1 0]
[0 0 0 0 0 0 0 0 0 0 0 1 1 0 1]
[0 0 0 0 0 0 0 0 0 0 1 0 0 1 1]
```

```
[7]: H4 = Matrix(GF(2), MatrizDeIncidenciaD10)
     CED10=codes.from_parity_check_matrix(H4)
     CED10

[7]: [15, 6] linear code over GF(2)

[8]: CED10.minimum_distance()

[8]: 4
```

Entonces el código expander $\mathcal{C}(Z_{P10}, \mathcal{P})$ tiene distancia 5 y el código expander $\mathcal{C}(Z_{D10}, \mathcal{P})$ tiene distancia 4, así que entre más pequeña sea la constante de expansión espectral mejor distancia mínima tendrá el código expander.

De hecho, el siguiente Teorema nos reafirma la importancia de tener un grafo con constante de expansión espectral pequeña, es decir, un grafo con buena expansión y un código interno con una distancia mínima grande para la construcción de un buen código expander. Dado que estamos trabajando con la constante de expansión espectral, haremos del Lema 2.3.25 dado por Alon y Chung , para la demostración del Teorema.

Teorema 4.2.21 ([56], Lema 15) Sea $\mathcal{S}$ es un código lineal de longitud d y distancia mínima $d(\mathcal{S})$. Sea Z un grafo de incidencia arista-vértice de un grafo $d-$regular Y con constante de expansión espectral $\lambda(Y)$, entonces

$$d(\mathcal{C}(Z, \mathcal{S})) > \frac{nd}{2}\left(\frac{d(\mathcal{S}) - \lambda(Y)}{d - \lambda(Y)}\right)^2.$$

Demostración.

Sea Y un grafo $d-$regular con n vértices del cual Z es generado. Por la Proposición 4.2.16 tenemos que Z tiene $\frac{nd}{2}$ vértices de variable y n vértices de restricción. Luego por el Lema 2.3.25 tenemos que cualquier conjunto de $\frac{nd}{2}(\gamma^2 + \frac{\lambda(Y)}{d}\gamma(1-\gamma))$ variables puede tener a lo menos γn restricciones como vecinos, es decir, si existe una palabra código distinta de cero, digamos w, tal que

$$wt(w) \leq \tfrac{nd}{2}(\gamma^2 + \tfrac{\lambda(Y)}{d}\gamma(1-\gamma)).$$

Y denotamos por V al conjunto de variables distintas de cero de w, $|V| \leq \frac{nd}{2}(\gamma^2 + \frac{\lambda(Y)}{d}\gamma(1-\gamma))$, el Lema 2.3.25 nos asegura que V puede tener a lo menos γn vértices de restricción como vecinos. Como cada variable tiene dos vértices de restricción como vecinos, tenemos que salen $2|V|$ aristas de V entonces el promedio de aristas que tiene cada restricción vecina de V es

$$\frac{2|V|}{\gamma n} < \frac{2(\frac{nd}{2}(\gamma^2 + \frac{\lambda(Y)}{d}\gamma(1-\gamma)))}{\gamma n} = d(\gamma + \tfrac{\lambda(Y)}{d}(1-\gamma)).$$

Si $d(\gamma + \frac{\lambda(Y)}{d}(1-\gamma)) < d(\mathcal{S})$. Entonces debe haber una restricción con menos de $d(\gamma+\frac{\lambda(Y)}{d}(1-\gamma))$ variables vecinas distintas de cero, pero esto no es posible por que cada restricción es una palabra-código de $\mathcal{S}$, así que su distancia debe ser mayor o igual $d(\mathcal{S})$. Entonces $d(\mathcal{C}(Z,\mathcal{S})) > \frac{nd}{2}(\gamma^2+\frac{\lambda(Y)}{d}\gamma(1-\gamma))$ y $d(\gamma+\frac{\lambda(Y)}{d}(1-\gamma)) \geq d(\mathcal{S})$. De esta última desigualdad tenemos que $\gamma \geq \frac{d(\mathcal{S})-\lambda(Y)}{d-\lambda(Y)}$ y como

$$\frac{nd}{2}(\gamma^2 + \frac{\lambda(Y)}{d}\gamma(1-\gamma)) > \frac{nd}{2}\gamma^2 \geq \frac{nd}{2}\left(\frac{d(\mathcal{S})-\lambda(Y)}{d-\lambda(Y)}\right)^2.$$

Entonces $d(\mathcal{C}(Z,\mathcal{S})) > \frac{nd}{2}\left(\frac{d(\mathcal{S})-\lambda(Y)}{d-\lambda(Y)}\right)^2$. ■

Ejemplo 4.2.22 Consideremos el grafo completo K^9 que se muestra en la Figura 4.8 y denotemos por Z_{K^9} su grafo de incidencia arista-vértice.

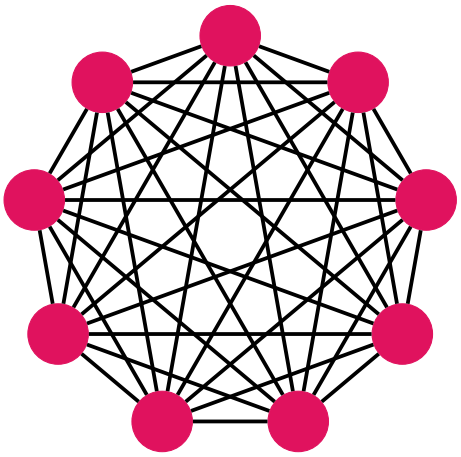


Figura 4.8: K^9.

El grafo K^9 tiene muy buena constante de expansión espectral ya que al calcular su espectro con ayuda de *SageMath* V 10.0 [61].

```
[1]: K9= graphs.CompleteGraph(9)
     K9.spectrum()
```

```
[1]: [8, -1, -1, -1, -1, -1, -1, -1, -1]
```

Tenemos que $\lambda(K^9) = 1$. Como K^9 es $8-$regular tomemos el código extendido $\widehat{\mathcal{H}_3}$ del $[7,4,3]-$código de Hamming $\mathcal{H}_3$, el cual tiene distancia mínima igual a 4 (ver Observación 4.1.13), como código interno. Entonces en base al Teorema 4.2.21

$$d(\mathcal{C}(Z_{K^9}, \widehat{\mathcal{H}_3})) > \frac{9\times 8}{2}\left(\frac{4-1}{8-1}\right)^2 = 6{,}61.$$

Lo cual es cierto ya que al calcular el código expander $\mathcal{C}(Z_{K^9}, \widehat{\mathcal{H}_3})$ (ver B.4) obtenemos que este tiene distancia mínima igual a 10.

Hasta ahora hemos mostrado ejemplos con grafos relativamente sencillos que tienen buena expansión para poder comprender la definición de código expander y su distancia. No obstante, ninguno de ellos pertenece a una familia de grafos expanders. Así que para finalizar el capítulo utilizaremos una de las familias de grafos expander que fueron construidas por Lubotzky, Philips y Sarnak [49], las cuales fueron descritas en la subsección 3.3.1, para construir una familia de códigos expanders.

Ejemplo 4.2.23 Sea $p = 13$, tenemos que existe una infinidad de números primos q que son congruentes a 1 mód 4 y que son residuos cuadráticos de 13, así que (X^{13q}) es una familia de grafos expanders donde cada grafo es $14-$regular, sus constantes de expansión espectral son menores a $2\sqrt{13}$. y cuentan con $\frac{q(q^2-1)}{2}$ vértices. A los grafos de incidencia arista-vértice de los grafos de la familia (X^{13q}) los estaremos denotando por Z_{13q}. Luego, como código interno nos tomaremos el código perforado en la primera entrada del $[15, 11, 3]-$código de Hamming H_4, es decir, $(H_4)_1^*$. Con ayuda del software *SageMath* V.10.0 [61] calcularemos su distancia mínima.

```
[1]: CH1511 = codes.HammingCode(GF(2), 4)
     CpCH1511= codes.PuncturedCode(CH1511, 0)
     CpCH1511.minimum_distance()
```

```
[1]: 2
```

Entonces por el Teorema 4.2.21 tenemos que las distancias mínimas relativas (Definición 4.0.9) de los miembros de la familia de códigos expanders $(\mathcal{C}(Z_{13q}, (H_4)_1^*)$ son mayores que $(\frac{2-2\sqrt{13}}{14-2\sqrt{13}})^2 \approx 0{,}58$. Así que $(\mathcal{C}(Z_{13q}, (H_4)_1^*)$ es una familia de códigos expanders asintóticamente buena. Adicionalmente cada código expander de la familia $(\mathcal{C}(Z_{13q}, (H_4)_1^*)$ es un buen código LDPC generalizado ya que cada grafo X^{13q} tiene una cintura mayor o igual a $2\log_{13} q$.

Conclusiones

Durante este trabajo se estudiaron cinco constantes que pueden definir a una familia de grafos expanders, las constantes de carácter más algebraico (la brecha espectral, la constante de expansión espectral y la constante de Kazhdan) se utilizan actualmente en la construcción de familias de grafos expanders, debido a que se sigue estudiando grupos que satisfagan la propiedad (T) y en el caso de los grafos de Ramanujan se tiene como un problema abierto la construcción de familias de grafos de Ramanujan $d-$regulares no bipartitos para cada $d \geq 3$ [45].

Además, mediante estas constantes de carácter algebraico, se exhibieron resultados que nos ayudan a saber por donde no buscar familias de grafos expanders, tales resultados son el principio de no expansión de cocientes y que los grupos abelianos finitos no forman familias de grafos expanders.

Se hizo la conexión entre familias de grafos expanders con los códigos detectores-correctores de errores mediante los códigos expanders, en donde se ilustró la importancia de usar un grafo con buena expansión y se presentó una familia de códigos expanders. La construcción de los códigos expanders presentados se hicieron con la ayuda de grafos de incidencia arista-vértice de grafos no bipartitos con buena constante de expansión espectral, ya que la construcción explícita de grafos biexpanders no balanceados sigue siendo un problema abierto, pero esta constante no es tan práctica para la decodificación de estos códigos como lo es la constante de expansión de vértices, por lo que sería interesante establecer una relación entre las constantes de expansión espectral de un grafo regular y su grafo de incidencia arista-vértice y mediante la desigualdad de Cheeger tener una aproximación de la constante de expansión de vértices del grafo de incidencia arista-vértice, o bien encontrar directamente una relación entre las constantes de expansión de vértices del grafo regular y su grafo de incidencia arista-vértice.

Apéndice A
Teoría de números

Definición A.0.1 Sean a y n dos enteros positivos coprimos. Decimos que a es un *residuo cuadrático* módulo n si la congruencia $x^2 \equiv a \mod n$ tiene solución. Si la congruencia no tiene solución decimos que a no es un residuo cuadrático módulo n.

Ejemplo A.0.2 Calculemos todos los residuos cuadráticos módulo 17. Como 17 es primo elevaremos al cuadrado todos los números del 1 al 16 y después obtendremos sus congruencias módulo 17.

$$\begin{array}{llll} 1^2 = 1 \equiv 1 & 5^2 = 25 \equiv 8 & 9^2 = 81 \equiv 13 & 13^2 = 169 \equiv 16 \\ 2^2 = 4 \equiv 4 & 6^2 = 36 \equiv 2 & 10^2 = 100 \equiv 15 & 14^2 = 196 \equiv 9 \\ 3^2 = 9 \equiv 9 & 7^2 = 49 \equiv 15 & 11^2 = 121 \equiv 2 & 15^2 = 225 \equiv 4 \\ 4^2 = 16 \equiv 16 & 8^2 = 64 \equiv 13 & 12^2 = 144 \equiv 8 & 16^2 = 256 \equiv 1 \end{array}$$

Entonces $1, 2, 4, 8, 9, 13, 15$ y 16 son los residuos cuadráticos módulo 17.

Definición A.0.3 Sean p un primo impar y m un entero. El *símbolo de Legendre* $\left(\frac{m}{p}\right)$ se define como

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divide a } m \\ 1 & \text{si } a \text{ es residuo cuadrático módulo } p \\ -1 & \text{si } a \text{ no es residuo cuadrático módulo } p. \end{cases}$$

Teorema A.0.4 (Teorema de los cuatro cuadrados de Jacobi) Sea $r_4(n)$ el número de formas en las que se puede expresar el entero n como la suma de cuatro cuadrados. Entonces

$$r_4(n) = \begin{cases} 8 \sum_{m|n} m & \text{si } n \text{ es impar} \\ 24 \sum_{\substack{m|n \\ m \text{ impar}}} m & \text{si } n \text{ es par.} \end{cases}$$

Ejemplo A.0.5 Para $n = 1$, tenemos que $r_4(1) = 8\sum_{m|1} m = 8(1) = 8$, así que existen 8 formas de expresar a 1 como la suma de cuatro cuadrados. A continuación presentamos las 8 formas.

$$\begin{aligned} 1^2+0^2+0^2+0^2 &= 1 & (-1)^2+0^2+0^2+0^2 &= 1 \\ 0^2+1^2+0^2+0^2 &= 1 & 0^2+(-1)^2+0^2+0^2 &= 1 \\ 0^2+0^2+1^2+0^2 &= 1 & 0^2+0^2+(-1)^2+0^2 &= 1 \\ 0^2+0^2+0^2+1^2 &= 1 & 0^2+0^2+0^2+(-1)^2 &= 1 \end{aligned}$$

Para $n = p$ con p un primo, tenemos que $r_4(p) = 8\sum_{m|p} m = 8(p+1)$.

Teorema A.0.6 ([22], Teorema 2.2.7) Sea p un primo impar. Los siguientes argumentos son equivalentes:

a) $p \equiv 1 \mod 4$.

b) La congruencia $x^2 \equiv -1 \mod p$ tiene solución en $\mathbb{Z}$.

c) p es la suma de dos cuadrados.

Proposición A.0.7 Existe una infinidad de números primos congruentes a 1 mód 4.

Demostración.

Supongamos $p_1, p_2, \ldots, p_n$ son todos los primos congruentes a 1 mód 4. Consideremos $N = (2p_1p_2\cdots p_n)^2 + 1$, es claro que $N \equiv 1 \mod 4$ y que $N \neq p_i$ con $i \in \{1, \ldots n\}$, así que N no puede ser primo. Dado que N es impar tenemos que 2 no puede dividir a N, entonces existe un primo impar p que divide a N, es decir, $N = (2p_1p_2\cdots p_n)^2 + 1 \equiv 0 \mod p$, de ahí que $(2p_1p_2\cdots p_n)^2 \equiv -1 \mod p$, entonces por el Teorema A.0.6 $p \equiv 1 \mod 4$. Si $p = p_i$ para algún $i \in \{1, \ldots n\}$ tenemos que $p|N$ y $p|(2p_1p_2\cdots p_n)^2$, así que $p|N - (2p_1p_2\cdots p_n)^2 = 1$, es decir, $p|1$ lo cual es una contradicción. De ahí que p es un primo impar congruente a 1 mód 4 distinto de p_i con $i \in \{1, \ldots, n\}$, contradiciendo la afirmación al inicio de la prueba. Por lo tanto, existe una infinidad de números primos congruentes a 1 mód 4. ■

Apéndice B
Cálculos para códigos expanders

B.1. Cálculos de la constante de expansión de Z_1

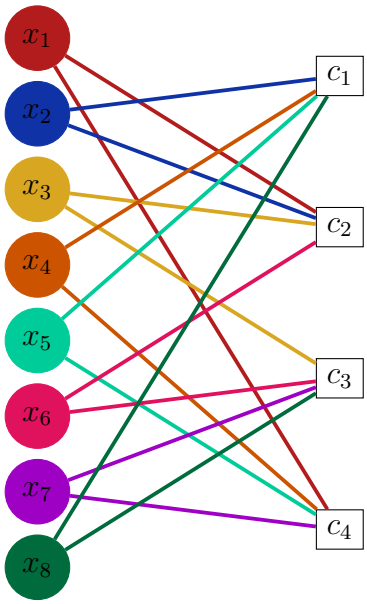


Figura B.1: Grafo Z_1.

Calculemos su constante de expansión. Para ello tomemos un subconjunto A de X con $|A| \leq \frac{8}{2} = 4$ y veamos que ocurre con ∂A.

- Caso $|A| = 1$

A	∂A	$\lvert\partial A\rvert$
$\{x_1\}$	$\{c_2, c_4\}$	2
$\{x_2\}$	$\{c_1, c_2\}$	2
$\{x_3\}$	$\{c_2, c_3\}$	2
$\{x_4\}$	$\{c_1, c_4\}$	2
$\{x_5\}$	$\{c_1, c_4\}$	2
$\{x_6\}$	$\{c_2, c_3\}$	2
$\{x_7\}$	$\{c_3, c_4\}$	2
$\{x_8\}$	$\{c_1, c_3\}$	2

Estimemos el valor de ε que satisface que la Definición 2.2.15 de biexpander no balanceado.

$$2 = |\partial A| \geq \varepsilon |A| = \varepsilon,$$

así que $\varepsilon \leq 2$.

- Caso $|A| = 2$.

  Para tomar 2 elementos de un conjunto de 8 elementos hay 28 posibles formas.

A	∂A	$\lvert\partial A\rvert$
$\{x_1, x_2\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_3\}$	$\{c_2, c_3, c_4\}$	3
$\{x_1, x_4\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_6\}$	$\{c_2, c_3, c_4\}$	3
$\{x_1, x_7\}$	$\{c_2, c_3, c_4\}$	3
$\{x_1, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3\}$	$\{c_1, c_2, c_3\}$	3
$\{x_2, x_4\}$	$\{c_1, c_2, c_4\}$	3
$\{x_2, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_2, x_6\}$	$\{c_1, c_2, c_3\}$	3
$\{x_2, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_8\}$	$\{c_1, c_2, c_3\}$	3
$\{x_3, x_4\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_6\}$	$\{c_2, c_3\}$	2
$\{x_3, x_7\}$	$\{c_2, c_3, c_4\}$	3
$\{x_3, x_8\}$	$\{c_1, c_2, c_3\}$	3
$\{x_4, x_5\}$	$\{c_1, c_4\}$	2

Sigue en la página siguiente.

A	∂A	$\lvert\partial A\rvert$
$\{x_4, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_7\}$	$\{c_1, c_3, c_4\}$	3
$\{x_4, x_8\}$	$\{c_1, c_3, c_4\}$	3
$\{x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_5, x_7\}$	$\{c_1, c_3, c_4\}$	3
$\{x_5, x_8\}$	$\{c_1, c_3, c_4\}$	3
$\{x_6, x_7\}$	$\{c_2, c_3, c_4\}$	3
$\{x_6, x_8\}$	$\{c_1, c_2, c_3\}$	3
$\{x_7, x_8\}$	$\{c_1, c_3, c_4\}$	3

Estimemos el valor de ε que satisface que la Definición 2.2.15 de biexpander no balanceado.

- Si $|\partial A| = 2$,
$$2 = |\partial A| \geq \varepsilon |A| = 2\varepsilon,$$
así que $\varepsilon \leq 1$.
- Si $|\partial A| = 3$,
$$3 = |\partial A| \varepsilon |A| = 2\varepsilon,$$
así que $\varepsilon \leq \frac{3}{2}$.
- Si $|\partial A| = 4$,
$$4 = |\partial A| \geq \varepsilon |A| = 2\varepsilon,$$
así que $\varepsilon \leq \frac{4}{2} = 2$.

- Caso $|A| = 3$.

Para tomar 3 elementos de un conjunto de 8 elementos hay 56 posibles formas.

A	∂A	$\lvert\partial A\rvert$
$\{x_1, x_2, x_3\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_4\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_2, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_2, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_4\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_6\}$	$\{c_2, c_3, c_4\}$	3
$\{x_1, x_3, x_7\}$	$\{c_2, c_3, c_4\}$	3
$\{x_1, x_3, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4

Sigue en la página siguiente.

A	∂A	$\lvert\partial A\rvert$
$\{x_1, x_4, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_4, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_6, x_7\}$	$\{c_2, c_3, c_4\}$	3
$\{x_1, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_4\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_6\}$	$\{c_1, c_2, c_3\}$	3
$\{x_2, x_3, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_8\}$	$\{c_1, c_2, c_3\}$	3
$\{x_2, x_4, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_2, x_4, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_6, x_7\}$	$\{c_2, c_3, c_4\}$	3
$\{x_3, x_6, x_8\}$	$\{c_1, c_2, c_3\}$	3
$\{x_3, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_5, x_7\}$	$\{c_1, c_3, c_4\}$	3
$\{x_4, x_5, x_8\}$	$\{c_1, c_3, c_4\}$	3
$\{x_4, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_7, x_8\}$	$\{c_1, c_3, c_4\}$	3

Sigue en la página siguiente.

A	∂A	$\lvert\partial A\rvert$
$\{x_5, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_5, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_5, x_7, x_8\}$	$\{c_1, c_3, c_4\}$	3
$\{x_6, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4

Estimemos el valor de ε que satisface que la Definición 2.2.15 de biexpander no balanceado.

- Si $|\partial A| = 3$,
$$3 = |\partial A| \geq \varepsilon |A| = 3\varepsilon,$$
así que $\varepsilon \leq 1$.
- Si $|\partial A| = 4$,
$$4 = |\partial A| \geq \varepsilon |A| = 3\varepsilon,$$
así que $\varepsilon \leq \frac{4}{3}$.

- Caso $|A| = 4$.

Para tomar 4 elementos de un conjunto de 8 elementos hay 70 posibles formas.

A	∂A	$\lvert\partial A\rvert$
$\{x_1, x_2, x_3, x_4\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_3, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_3, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_3, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_3, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_4, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_2, x_4, x_6, \}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_4, x_7, \}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_4, x_8, \}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_4, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_4, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_4, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_4, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4

Sigue en la página siguiente.

A	∂A	$\lvert\partial A\rvert$
$\{x_1, x_3, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_6, x_7\}$	$\{c_2, c_3, c_4\}$	3
$\{x_1, x_3, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_5, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_5, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_5, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_6, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_4, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_4, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_4, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_4, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_6, x_8\}$	$\{c_1, c_2, c_3\}$	3
$\{x_2, x_3, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_5, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_5, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_5, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_6, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_5, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_5, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4

Sigue en la página siguiente.

A	∂A	$\lvert\partial A\rvert$
$\{x_3, x_5, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_5, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_5, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_6, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_5, x_6, x_7\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_5, x_6, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_5, x_7, x_8\}$	$\{c_1, c_3, c_4\}$	3
$\{x_4, x_6, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_5, x_6, x_7, x_8\}$	$\{c_1, c_2, c_3, c_4\}$	4

Estimemos el valor de ε que satisface que la Definición 2.2.15 de biexpander no balanceado.

- Si $|\partial A| = 4$,
$$3 = |\partial A| \geq \varepsilon |A| = 4\varepsilon,$$
así que $\varepsilon \leq \frac{3}{4}$.
- Si $|\partial A| = 4$,
$$4 = |\partial A| \geq \varepsilon |A| = 4\varepsilon,$$
así que $\varepsilon \leq 1$.

Entonces $\varepsilon = \text{mín}\{2, 1, \frac{3}{2}, \frac{4}{3}, \frac{3}{4}\} = \frac{3}{4}$. Por lo tanto Z_1 es un $(8, 4, 2, 4, \frac{3}{4})-$biexpander.

B.2. Perforación de $\mathcal{C}(Z_1, \mathcal{S})$

En el software *SageMath* V.10 [61] llamamos a $\mathcal{C}(Z_1, \mathcal{S})$ como `ExpanderCode1`. La función `punctured` perforará el código en las posiciones que se indiquen dentro de los corchetes. Cabe destacar que *SageMath* empieza a contar las posiciones desde cero, así que la última posición es 7 y no 8.

```
[2]: ExpanderCode1.list()
```

```
[2]: [(0, 0, 0, 0, 0, 0, 0, 0),
      (1, 1, 1, 0, 1, 1, 1, 1),
      (0, 0, 0, 1, 0, 0, 0, 0),
      (1, 1, 1, 1, 1, 1, 1, 1)]
```

```
[3]: CpEC1=ExpanderCode1.punctured([0,2,5,6])
     CpEC1.list()
```

```
[3]: [(0, 0, 0, 0), (1, 0, 1, 1), (0, 1, 0, 0), (1, 1,␣
     ↪1, 1)]
```

```
[4]: CpEC2=ExpanderCode1.punctured([3,4,6,7])
     CpEC2.list()

[4]: [(0, 0, 0, 0), (1, 1, 1, 1)]

[5]: CpEC3=ExpanderCode1.punctured([0,1,3,4])
     CpEC3.list()

[5]: [(0, 0, 0, 0), (1, 1, 1, 1)]

[6]: CpEC4=ExpanderCode1.punctured([1,2,4,7])
     CpEC4.list()

[6]:
     [(0, 0, 0, 0), (1, 0, 1, 1), (0, 1, 0, 0), (1, 1,␣
      ↪1, 1)]
```

B.3. Cálculos de la constante de expansión de Z_2

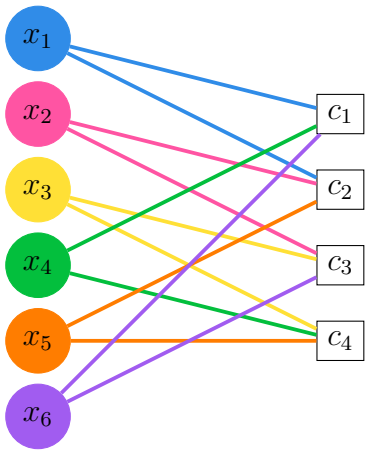


Figura B.2: Grafo bipartito Z_2.

Calculemos su constante de expansión. Para ello tomemos un subconjunto A de X con $|A| \leq \frac{6}{2} = 3$ y veamos que ocurre con ∂A.

- Caso $|A| = 1$

A	∂A	$\lvert\partial A\rvert$
$\{x_1\}$	$\{c_1, c_2\}$	2
$\{x_2\}$	$\{c_2, c_3\}$	2
$\{x_3\}$	$\{c_3, c_4\}$	2
$\{x_4\}$	$\{c_1, c_4\}$	2
$\{x_5\}$	$\{c_2, c_4\}$	2
$\{x_6\}$	$\{c_1, c_3\}$	2

Estimemos el valor de ε que satisface que la Definición 2.2.15 de biexpander no balanceado .

$$2 = |\partial A| \geq \varepsilon |A| = \varepsilon,$$

así que $\varepsilon \leq 2$.

- Caso $|A| = 2$

  Para tomar 2 elementos de un conjunto de 6 elementos hay 15 posibles formas.

A	∂A	$\lvert\partial A\rvert$
$\{x_1, x_2\}$	$\{c_1, c_2, c_3\}$	3
$\{x_1, x_3\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_6\}$	$\{c_1, c_2, c_3\}$	3
$\{x_2, x_3\}$	$\{c_2, c_3, c_4\}$	3
$\{x_2, x_4\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_5\}$	$\{c_2, c_3, c_4\}$	3
$\{x_2, x_6\}$	$\{c_1, c_2, c_3\}$	3
$\{x_3, x_4\}$	$\{c_1, c_3, c_4\}$	3
$\{x_3, x_5\}$	$\{c_2, c_3, c_4\}$	2
$\{x_3, x_6\}$	$\{c_1, c_3, c_4\}$	3
$\{x_4, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_4, x_6\}$	$\{c_1, c_3, c_4\}$	3
$\{x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4

Estimemos el valor de ε que satisface que la Definición 2.2.15 de biexpander no balanceado.

- Si $|\partial A| = 3$

$$3 = |\partial A| \geq \varepsilon |A| = 2\varepsilon,$$

  así que $\varepsilon \leq \frac{3}{2}$.

- Si $|\partial A| = 4$

$$4 = |\partial A| \geq \varepsilon |A| = 2\varepsilon,$$

así que $\varepsilon \leq \frac{4}{2} = 2$.

- Caso $|A| = 3$

Para tomar 3 elementos de un conjunto de 6 elementos hay 20 posibles formas.

A	∂A	$\lvert\partial A\rvert$
$\{x_1, x_2, x_3\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_4\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_2, x_6\}$	$\{c_1, c_2, c_3\}$	3
$\{x_1, x_3, x_4\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_3, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_4, x_5\}$	$\{c_1, c_2, c_4\}$	3
$\{x_1, x_4, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_1, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_4\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_3, x_5\}$	$\{c_2, c_3, c_4\}$	3
$\{x_2, x_3, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_4, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_2, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_5\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_3, x_4, x_6\}$	$\{c_1, c_3, c_4\}$	3
$\{x_3, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4
$\{x_4, x_5, x_6\}$	$\{c_1, c_2, c_3, c_4\}$	4

Estimemos el valor de ε que satisface que la Definición 2.2.15 de biexpander no balanceado .

- Si $|\partial A| = 3$

$$3 = |\partial A| \geq \varepsilon |A| = 3\varepsilon,$$

así que $\varepsilon \leq 1$.

- Si $|\partial A| = 4$

$$4 = |\partial A| \geq \varepsilon |A| = 3\varepsilon,$$

así que $\varepsilon \leq \frac{4}{3}$.

Entonces $\varepsilon = \text{mín}\{2, \frac{3}{2}, 1, \frac{4}{3}\} = 1$. Por lo tanto, Z_2 es un $(6, 4, 2, 3, 1)-$biexpander.

B.4. Código expander $\mathcal{C}(Z_{K^9}, \widehat{\mathcal{H}_3})$

A continuación presentamos el código realizado en *SageMath* V.10.0 [61] para obtener el código expander $\mathcal{C}(Z_{K^9}, \widehat{\mathcal{H}_3})$.

[1]:
```
import sympy as sp
import numpy as np

#Declaramos las variables y1,y2,...,y36
nombres_variables = []
for i in range(0,36):
    nombres_variables.append('y{}'.format(i+1))
    Y=sp.symbols(nombres_variables)
```

[2]:
```
#Usaremos el código extendido del [7,3]-código de␣
 ↪Hamming como nuestro código interno y lo␣
 ↪denotaremos por Ce
CH = codes.HammingCode(GF(2), 3)
Ce=codes.ExtendedCode(CH)
Ce
```

[2]:
```
Extension of [7, 4] Hamming Code over GF(2)
```

[3]:
```
#Introducimos manualmente la matriz verificadora de␣
 ↪paridad del código  interno

H = [[1, 1, 1, 1, 1, 1, 1, 1],
    [0, 0, 0, 1, 1, 1, 1, 0],
    [0, 1, 1, 0, 0, 1, 1, 0],
    [1, 0, 1, 0, 1, 0, 1, 0]]

#Convertimos a una matriz simbólica de sympy

H1 = sp.Matrix(H)
```

[4]:
```
#Usaremos el grafo completo de 9 vértices
K9=graphs.CompleteGraph(9)
M= K9.incidence_matrix()
M
```

[4]:

```
[1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[1 0 0 0 0 0 0 0 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 1 1 1 1␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0␣
 ↪1 1 1 1 0 0 0 0 0 0]
[0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0␣
 ↪1 0 0 0 1 1 1 0 0 0]
[0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0␣
 ↪0 1 0 0 1 0 0 1 1 0]
[0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0␣
 ↪0 0 1 0 0 1 0 1 0 1]
[0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1␣
 ↪0 0 0 1 0 0 1 0 1 1]
```

[5]:

```
#Procedimiento para obtener la función Z
Z = []
for i in range(0, 9):
    Mrow1= M.row(i) #Tomamos la i-ésima fila de M
    x = np.array([Mrow1])
    fila_de_Z=np.flatnonzero(x == 1) #Pedimos que␣
 ↪elija las entradas que tienen 1 en la fila␣
 ↪seleccionada
    print(fila_de_Z+1)#La i-ésima fila contiene las␣
 ↪posiciones de las variables vecinas a la␣
 ↪restricción c_{i}
    Z.append(fila_de_Z)
```

```
[1 2 3 4 5 6 7 8]
[ 1  9 10 11 12 13 14 15]
[ 2  9 16 17 18 19 20 21]
[ 3 10 16 22 23 24 25 26]
[ 4 11 17 22 27 28 29 30]
[ 5 12 18 23 27 31 32 33]
[ 6 13 19 24 28 31 34 35]
[ 7 14 20 25 29 32 34 36]
[ 8 15 21 26 30 33 35 36]
```

[6]:
```
#Función que multiplica la matriz verificadora de paridad H1 del código interno con el vector columna que contiene las variables cuyos indices son los valores de una fila de Z, devolviendo sistemas de ecuaciones.
def multiplicacion(fila_de_Z):
    nombres_variables = [] #Borrón y cuenta nueva
    for indice in fila_de_Z:
        nombres_variables.append('y{}'.format(indice)) #Guardamos en un array los nombres de las variables cuyos índices son los valores de una fila de Z
    y=sp.symbols(nombres_variables) #Volvemos a símbolos de sympy los nombres de las variables
    y_restriccion = sp.Matrix([y]) #Colocamos en un vector fila todas las variables cuyos indices son los valores de una fila de ZT=y_restriccion.T #Transponemos el vector fila
    return H1*T # Multiplicamos por la matriz verificadora de paridad y se nos devuelve un sistema de ecuaciones
```

[7]:
```
#Procedimiento para guardar en un sólo arreglo todas las ecuaciones
eqns = []
for fila_de_Z in Z:
    resultado_de_multiplicacion = multiplicacion(fila_de_Z+1)

    for j in range(0, resultado_de_multiplicacion.shape[0]): #Ciclo para formar las expresiones de las filas de la matriz resultado_de_multiplicacion igualadas a cero, pasamos el resultado a sage y guardamos dicha expresión en un arreglo llamado eqns
        eqns.append(sp.Eq(resultado_de_multiplicacion[j],0)._sage_())
```

[8]:
```
eqns
```

```
[8]: [y1 + y2 + y3 + y4 + y5 + y6 + y7 + y8 == 0,
      y4 + y5 + y6 + y7 == 0,
      y2 + y3 + y6 + y7 == 0,
      y1 + y3 + y5 + y7 == 0,
      y1 + y10 + y11 + y12 + y13 + y14 + y15 + y9 == 0,
      y11 + y12 + y13 + y14 == 0,
      y10 + y13 + y14 + y9 == 0,
      y1 + y10 + y12 + y14 == 0,
      y16 + y17 + y18 + y19 + y2 + y20 + y21 + y9 == 0,
      y17 + y18 + y19 + y20 == 0,
      y16 + y19 + y20 + y9 == 0,
      y16 + y18 + y2 + y20 == 0,
      y10 + y16 + y22 + y23 + y24 + y25 + y26 + y3 == 0,
      y22 + y23 + y24 + y25 == 0,
      y10 + y16 + y24 + y25 == 0,
      y16 + y23 + y25 + y3 == 0,
      y11 + y17 + y22 + y27 + y28 + y29 + y30 + y4 == 0,
      y22 + y27 + y28 + y29 == 0,
      y11 + y17 + y28 + y29 == 0,
      y17 + y27 + y29 + y4 == 0,
      y12 + y18 + y23 + y27 + y31 + y32 + y33 + y5 == 0,
      y23 + y27 + y31 + y32 == 0,
      y12 + y18 + y31 + y32 == 0,
      y18 + y27 + y32 + y5 == 0,
      y13 + y19 + y24 + y28 + y31 + y34 + y35 + y6 == 0,
      y24 + y28 + y31 + y34 == 0,
      y13 + y19 + y31 + y34 == 0,
      y19 + y28 + y34 + y6 == 0,
      y14 + y20 + y25 + y29 + y32 + y34 + y36 + y7 == 0,
      y25 + y29 + y32 + y34 == 0,
      y14 + y20 + y32 + y34 == 0,
      y20 + y29 + y34 + y7 == 0,
```

```
y15 + y21 + y26 + y30 + y33 + y35 + y36 + y8 == 0,
y26 + y30 + y33 + y35 == 0,
y15 + y21 + y33 + y35 == 0,
y21 + y30 + y35 + y8 == 0]
```

[9]:
```
#Construcción de la matriz asociada al sistema de␣
 ↪ecuaciones eqs
matriz_asociada_al_sistema = matrix([[lhs.
 ↪coefficient(u) for u in Y] for eq in eqns for␣
 ↪lhs in [eq.lhs()]])
print(matriz_asociada_al_sistema.str())
```

```
[1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 1 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[1 0 0 0 0 0 0 0 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[1 0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
[0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0]
```

```
[0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0␣
↪1 1 1 1 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0␣
↪1 1 1 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0␣
↪0 1 1 0 0 0 0 0 0 0]
[0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0␣
↪1 0 1 0 0 0 0 0 0 0]
[0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0␣
↪1 0 0 0 1 1 1 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0␣
↪1 0 0 0 1 1 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0␣
↪0 0 0 0 1 1 0 0 0 0]
[0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0␣
↪1 0 0 0 0 1 0 0 0 0]
[0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0␣
↪0 1 0 0 1 0 0 1 1 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0␣
↪0 1 0 0 1 0 0 1 0 0]
[0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0␣
↪0 0 0 0 1 0 0 1 0 0]
[0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0␣
↪0 1 0 0 0 0 0 1 0 0]
[0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0␣
↪0 0 1 0 0 1 0 1 0 1]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0␣
↪0 0 1 0 0 1 0 1 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0␣
↪0 0 0 0 0 1 0 1 0 0]
[0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
↪0 0 1 0 0 0 0 1 0 0]
[0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1␣
↪0 0 0 1 0 0 1 0 1 1]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1␣
↪0 0 0 1 0 0 1 0 1 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0␣
↪0 0 0 0 0 0 1 0 1 0]
[0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0␣
↪0 0 0 1 0 0 0 0 1 0]
```

[10]:
```
#Generamos el código expander a través de la matriz␣
 ↪asociada al sistema
H3=matrix(GF(2),matriz_asociada_al_sistema)
ExpanderCodeK9 = codes.from_parity_check_matrix(H3)
ExpanderCodeK9
```

[10]:
```
[36, 4] linear code over GF(2)
```

[11]:
```
Codewords=ExpanderCodeK9.list()
print(np.array(Codewords))
```

```
[[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0␣
 ↪0 0 0 0 0 0 0 0 0 0 0 0]
 [1 0 0 1 1 0 0 1 0 1 1 0 1 0 0 0 1 1 1 1 0 0 1 0 1␣
 ↪1 0 0 0 1 1 0 0 1 0 1]
 [0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 0 0 1 0 1 1 0␣
 ↪0 0 1 1 0 0 1 1 0 1 0]
 [1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 0 0 0 1 1 1 0 0 1 1␣
 ↪1 0 1 1 1 1 1 1 1 1 1]
 [0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 1 1 1 0 0 0 0 0 1 1␣
 ↪0 0 1 1 0 1 1 0 1 0 0]
 [1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 1 0 0 1 1 0␣
 ↪1 0 1 1 1 0 1 0 0 0 1]
 [0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 1 0 0 0 0 1 0 1 0 1␣
 ↪0 0 0 0 0 1 0 1 1 1 0]
 [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0␣
 ↪1 0 0 0 1 0 0 1 0 1 1]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1␣
 ↪0 1 1 1 0 1 1 0 1 0 0]
 [1 0 0 1 1 0 0 1 0 1 1 0 1 0 0 0 1 1 1 1 0 1 0 1 0␣
 ↪1 1 1 1 1 0 1 0 0 0 1]
 [0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 0 0 1 1 0 0 1␣
 ↪0 1 0 0 0 1 0 1 1 1 0]
 [1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 0 0 0 1 1 1 1 1 0 0␣
 ↪1 1 0 0 1 0 0 1 0 1 1]
 [0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 1 1 1 0 0 0 1 1 0 0␣
 ↪0 1 0 0 0 0 0 0 0 0 0]
 [1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 1 0 1 0 0 1␣
 ↪1 1 0 0 1 1 0 0 1 0 1]
```

```
[0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 1 0 0 0 0 1 1 0 1 0␣
↪0 1 1 1 0 0 1 1 0 1 0]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1␣
↪1 1 1 1 1 1 1 1 1 1 1]]
```

[12]:
```
ExpanderCodeK9.minimum_distance()
```

[12]:
```
10
```

[13]:
```
print(ExpanderCodeK9.weight_distribution())
```

```
[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 1, 0, 1,␣
 ↪0, 6, 0, 1, 0, 1, 0, 0, 0,
2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]
```

[14]:
```
#Comprobación:
#Calculamos los complementos de las filas de Z
Z_complemento = []
indices_0_35 = {i for i in range(0,36)} #Indices␣
 ↪del 0 al 35 en forma de conjunto
for fila_de_Z in Z:
    Z_complemento.append(list(indices_0_35.
 ↪difference(set(fila_de_Z)))) #Calculamos la␣
 ↪diferencia de conjuntos y lo volvemos lista
```

[15]:
```
#Perforaremos el código expander  en los␣
 ↪complementos de las filas de Z  y verificamos␣
 ↪que las palabras-código del código perforado␣
 ↪estén en el código interno

for complemento in Z_complemento:
    Cp=ExpanderCodeK9.punctured(complemento)
    print('*'*80+'\n')
    print('Código perforado en las entradas\n {}'.
 ↪format(complemento))
    for palabra in Cp.list():
        if palabra not in Ce.list():
            print('La palabra {} no está en el␣
 ↪código interno'.format(palabra))
        else:
            print('La palabra {} está en el código␣
 ↪interno'.format(palabra))
    print('\n')
```

```
************************************************************

Código perforado en las entradas
 [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23,␣
 ↪24, 25, 26, 27,
28, 29, 30, 31, 32, 33, 34, 35]
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 0, 0, 1, 1, 0, 0, 1) está en el código interno
La palabra (0, 1, 1, 0, 0, 1, 1, 0) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno


************************************************************

Código perforado en las entradas
 [1, 2, 3, 4, 5, 6, 7, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25,␣
 ↪26, 27, 28,
29, 30, 31, 32, 33, 34, 35]
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 0, 0, 0, 0, 1, 1, 1) está en el código interno
La palabra (0, 1, 0, 0, 1, 0, 1, 1) está en el código interno
La palabra (1, 1, 0, 0, 1, 1, 0, 0) está en el código interno
La palabra (0, 0, 1, 1, 0, 0, 1, 1) está en el código interno
La palabra (1, 0, 1, 1, 0, 1, 0, 0) está en el código interno
La palabra (0, 1, 1, 1, 1, 0, 0, 0) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno


************************************************************

Código perforado en las entradas
 [0, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 21, 22, 23, 24, 25,␣
 ↪26, 27, 28,
29, 30, 31, 32, 33, 34, 35]
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 0, 0, 0, 0, 1, 1, 1) está en el código interno
La palabra (0, 1, 1, 0, 0, 1, 1, 0) está en el código interno
La palabra (1, 1, 1, 0, 0, 0, 0, 1) está en el código interno
La palabra (0, 0, 0, 1, 1, 1, 1, 0) está en el código interno
La palabra (1, 0, 0, 1, 1, 0, 0, 1) está en el código interno
La palabra (0, 1, 1, 1, 1, 0, 0, 0) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno
```

```
************************************************************

Código perforado en las entradas
 [0, 1, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20,␣
 ↪26, 27, 28,
29, 30, 31, 32, 33, 34, 35]
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 0, 0, 0, 0, 1, 1, 1) está en el código interno
La palabra (0, 1, 0, 0, 1, 0, 1, 1) está en el código interno
La palabra (1, 1, 0, 0, 1, 1, 0, 0) está en el código interno
La palabra (0, 0, 1, 0, 1, 1, 0, 1) está en el código interno
La palabra (1, 0, 1, 0, 1, 0, 1, 0) está en el código interno
La palabra (0, 1, 1, 0, 0, 1, 1, 0) está en el código interno
La palabra (1, 1, 1, 0, 0, 0, 0, 1) está en el código interno
La palabra (0, 0, 0, 1, 1, 1, 1, 0) está en el código interno
La palabra (1, 0, 0, 1, 1, 0, 0, 1) está en el código interno
La palabra (0, 1, 0, 1, 0, 1, 0, 1) está en el código interno
La palabra (1, 1, 0, 1, 0, 0, 1, 0) está en el código interno
La palabra (0, 0, 1, 1, 0, 0, 1, 1) está en el código interno
La palabra (1, 0, 1, 1, 0, 1, 0, 0) está en el código interno
La palabra (0, 1, 1, 1, 1, 0, 0, 0) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno


************************************************************

Código perforado en las entradas
 [0, 1, 2, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 17, 18, 19, 20,␣
 ↪22, 23, 24, 25,
30, 31, 32, 33, 34, 35]
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 0, 0, 0, 0, 1, 1, 1) está en el código interno
La palabra (0, 1, 1, 0, 0, 1, 1, 0) está en el código interno
La palabra (1, 1, 1, 0, 0, 0, 0, 1) está en el código interno
La palabra (0, 0, 0, 1, 1, 1, 1, 0) está en el código interno
La palabra (1, 0, 0, 1, 1, 0, 0, 1) está en el código interno
La palabra (0, 1, 1, 1, 1, 0, 0, 0) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno


************************************************************

Código perforado en las entradas
```

```
 [0, 1, 2, 3, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 18, 19, 20,␣
 ↪21, 23, 24, 25,
27, 28, 29, 33, 34, 35]
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 0, 0, 0, 0, 1, 1, 1) está en el código interno
La palabra (0, 1, 0, 0, 1, 0, 1, 1) está en el código interno
La palabra (1, 1, 0, 0, 1, 1, 0, 0) está en el código interno
La palabra (0, 0, 1, 0, 1, 1, 0, 1) está en el código interno
La palabra (1, 0, 1, 0, 1, 0, 1, 0) está en el código interno
La palabra (0, 1, 1, 0, 0, 1, 1, 0) está en el código interno
La palabra (1, 1, 1, 0, 0, 0, 0, 1) está en el código interno
La palabra (0, 0, 0, 1, 1, 1, 1, 0) está en el código interno
La palabra (1, 0, 0, 1, 1, 0, 0, 1) está en el código interno
La palabra (0, 1, 0, 1, 0, 1, 0, 1) está en el código interno
La palabra (1, 1, 0, 1, 0, 0, 1, 0) está en el código interno
La palabra (0, 0, 1, 1, 0, 0, 1, 1) está en el código interno
La palabra (1, 0, 1, 1, 0, 1, 0, 0) está en el código interno
La palabra (0, 1, 1, 1, 1, 0, 0, 0) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno


**********************************************************

Código perforado en las entradas
 [0, 1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 19, 20,␣
 ↪21, 22, 24, 25,
26, 28, 29, 31, 32, 35]
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 0, 0, 0, 0, 1, 1, 1) está en el código interno
La palabra (0, 1, 1, 0, 0, 1, 1, 0) está en el código interno
La palabra (1, 1, 1, 0, 0, 0, 0, 1) está en el código interno
La palabra (0, 0, 0, 1, 1, 1, 1, 0) está en el código interno
La palabra (1, 0, 0, 1, 1, 0, 0, 1) está en el código interno
La palabra (0, 1, 1, 1, 1, 0, 0, 0) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno


**********************************************************

Código perforado en las entradas
 [0, 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 20,␣
 ↪21, 22, 23, 25,
26, 27, 29, 30, 32, 34]
```

```
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 1, 0, 0, 1, 1, 0, 0) está en el código interno
La palabra (0, 0, 1, 0, 1, 1, 0, 1) está en el código interno
La palabra (1, 1, 1, 0, 0, 0, 0, 1) está en el código interno
La palabra (0, 0, 0, 1, 1, 1, 1, 0) está en el código interno
La palabra (1, 1, 0, 1, 0, 0, 1, 0) está en el código interno
La palabra (0, 0, 1, 1, 0, 0, 1, 1) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno


**********************************************************

Código perforado en las entradas
 [0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19,␣
 ↪21, 22, 23, 24,
26, 27, 28, 30, 31, 33]
La palabra (0, 0, 0, 0, 0, 0, 0, 0) está en el código interno
La palabra (1, 0, 0, 1, 1, 0, 0, 1) está en el código interno
La palabra (0, 1, 1, 0, 0, 1, 1, 0) está en el código interno
La palabra (1, 1, 1, 1, 1, 1, 1, 1) está en el código interno
```

Índice alfabético

Índice simbólico

Símbolo	Descripción	Página
$(L^2(G), L)$	Representación regular.	23
(V, ρ)	Representación de dimensión finita de un grupo finito.	16
$(\alpha, c)-$concentrador		73
$(m, n, d_{V^-}, d_{V^+}, \varepsilon)$	Grafo bipartito con conjunto de vértices $V^- \cup V^+$ donde $\lvert V^-\rvert = m$, $\lvert V^+\rvert = n$, con $n > n$, $(d_{V^-}, d_{V^+})-$regular y con la constante de expansión de vértices ε.	38
$(n, d, c)-$biexpander	Grafo bipartito $d-$regular donde cada partición tiene n vértices y la constante de expansión de vértices del grafo es c.	37
$(n, d, c)-$expander	Grafo $d-$regular con n vértices y constante de expansión de vértices c.	33
C^k	Ciclo de longitud k.	5
$Cay(G, S)$	Grafo de Cayley del grupo G con conjunto simétrico de generadores S.	13
$Cos(G/H, S)$	Grafo cociente.	92
$E(F, V \setminus F)$	Frontera de aristas del subconjunto de vértices F.	29
$E_X(v)$	Conjunto de aristas que inciden en el vértice v en el grafo X.	3
$GL(V)$	Grupo de todas las transformaciones lineales invertibles del espacio vectorial de dimensión finita V a sí mismo.	16
$GL(n, \mathbb{C})$	Grupo de todas las matrices invertibles del espacio vectorial de tamaño $n \times n$ con coeficientes en $\mathbb{C}$.	18
H_z	Grupo multiplicativo de matrices con entradas enteras de la forma $\left(\begin{smallmatrix} a & b & u \\ c & d & v \\ 0 & 0 & 1 \end{smallmatrix}\right)$.	76
I_m	$\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$	74
K^n	Grafo completo de n vértices.	4
L	Representación regular izquierda.	23

Símbolo	Descripción	Página
$L^2(X)$	$\mathbb{C}$-espacio vectorial que consiste en las funciones que van del conjunto finito X a $\mathbb{C}$.	1
$L^2(X,\mathbb{R})$	Espacio vectorial cuyos elementos son funciones de $L^2(X)$, cuyo codominio es $\mathbb{R}$.	2
$L^2_1(X)$	Espacio vectorial cuyos elementos son funciones de $L^2(X)$, cuyo producto interno con la función constante 1 es igual a cero.	2
$L^2_1(X,\mathbb{R})$	Espacio vectorial cuyos elementos son funciones de $L^2(X,\mathbb{R})$, cuyo producto interno con la función constante 1 es igual a cero.	2
$N_X(v)$	Conjunto de vecinos del vértice v en el grafo X.	3
O_m	$\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$	74
P^k	Camino de longitud k.	5
S_z	Grupo multiplicativo de matrices con entradas enteras de la forma $\left(\begin{smallmatrix} 1 & 0 & u \\ 0 & 1 & v \\ 0 & 0 & 1 \end{smallmatrix}\right)$.	76
$Spec(X)$	Espectro del grafo X.	11
$X = (V, E)$	Grafo X con conjunto de vértices V y conjunto de aristas E.	2
$X = (V_1 \cup V_2, E)$	Grafo bipartito X con conjunto de vértices $V_1 \cup V_2$ y conjunto de aristas E.	7
X^{pq}	Grafo de Ramanujan construido por Lubotzky, Phillips y Sarnak.	90
$Z = (X \cup C, E)$	Grafo bipartito donde los vértices de X son llamados variables y los vértices de C son llamados restricciones.	107
$[n,k]-$código lineal	Código lineal binario de longitud n, y dimensión k.	103
Δ	Laplaciano discreto.	39
$\left(\frac{m}{p}\right)$	Símbolo de Legendre.	131
$\kappa(G,S)$	Constante de Kazhdan del par (G,S).	62
$\kappa(G,S,\widehat{L})$	$\min_{\|v\|=1} \max_{s\in S} \|\widehat{L}(s)v - v\|$.	66
$\kappa'(G,S,\rho,\langle\cdot,\cdot\rangle)$	$\min_{\|v\|=1} \max_{s\in S} \|\rho(s)v - v\|$.	58
$\lambda(X)$	Constante de expansión espectral del grafo X.	54
$\lambda_2(X)$	Segundo valor propio más grande asociado al grafo X.	40
$\mathcal{C}$	Código.	101
$\mathcal{C}(Z)$	Código LDPC construido apartir del grafo bipartito Z.	108
$\mathcal{C}(Z,\mathcal{S})$	Código expander construido a partir del grafo bipartito Z y el código interno $\mathcal{S}$.	110
$\mathcal{C}^*$	Código perforado.	105
$\mathcal{C}^\perp$	Código dual.	103

Símbolo	Descripción	Página
$\mathcal{D}$	Gradiente.	38
$\mathcal{D}^*$	Divergencia.	39
$\mathcal{H}_r$	Código de Hamming de longitud 2^r-1 y dimensión 2^r-1-r.	106
$\mathcal{P}$	Código dual del código binario de repetición.	104
$\mathscr{A}$	Operador de adyacencia.	9
∂A	Frontera de vértices del subconjunto de vértices A.	33
$\varepsilon-$biexpander	Grafo bipartito con constante de expansión de vértices compacta ε.	38
$\varepsilon-$expander	Grafo con constante de expansión de vértices compacta ε.	36
$\widehat{G}$	Conjunto de representaciones unitarias irreducibles no equivalentes de G.	20
$\widehat{L}$	Representación regular izquierda restringida a $L_1^2(G)$.	66
$\widehat{\mathcal{C}}$	Código extendido.	105
$\|X\|$	Número de aristas del grafo X.	3
c_i	$i-$ésima restricción.	107
$d(\mathcal{C})$	Disatncia mínima del código $\mathcal{C}$.	102
$d(x,y)$	Distancia de Hamming entre las palabras-código x y y.	102
$d-\lambda_2(X)$	Brecha espectral del grafo X.	52
$d_X(v)$	Grado del vértice v en el grafo X.	3
e^+	vértice final de la arista e.	38
e^-	vértice inicial de la arista e.	38
f_c	Función contante c en $L^2(X)$.	1
$g(X)$	Cintura del grafo X.	5
$h(X)$	Constante isoperimétrica.	30
$wt(x)$	Peso de Hamming de la palabra-código x.	102
x_j	$j-$ésima variable.	107
$z(i,j)$	Función donde para cada restricción c_i sus variables vecinas son $X_{z(i,1)},\ldots,X_{z(i,d_C)}$.	108
$\|X\|$	Número de vértices del grafo X.	3

Bibliografía

[1] Alon, N. Eigenvalues and expanders. *Combinatorica 6*, 2 (jun 1986), 83–96.

[2] Alon, N., and Chung, F. Explicit construction of linear sized tolerant networks. *Discrete Mathematics 72*, 1 (1988), 15–19.

[3] Alon, N., Galil, Z., and Milman, V. Better expanders and superconcentrators. *Journal of Algorithms 8*, 3 (sep 1987), 337–347.

[4] Alon, N., and Milman, V. λ, isoperimetric inequalities for graphs, and superconcentrators. *Journal of Combinatorial Theory, Series B 38*, 1 (feb 1985), 73–88.

[5] Andrade, C. A. L. *Códigos de Hamming, En F. Macías Romero (Ed.), Matemáticas y sus aplicaciones 4*. BUAP, Puebla, 2014, ch. Cap. 1, pp. 5–33.

[6] Angluin, D. A note on a construction of margulis. *Information Processing Letters 8*, 1 (jan 1979), 17–19.

[7] Asratian, A., Denley, T., and Häggkvist, R. *Bipartite Graphs and Their Applications*. Cambridge Tracts in Mathematics. Cambridge University Press, 1998.

[8] Barg, A., and Zémor, G. Error exponents of expander codes. *IEEE Transactions on Information Theory 48*, 6 (2002), 1725–1729.

[9] Barg, A., and Zemor, G. Distance properties of expander codes. *IEEE Transactions on Information Theory 52*, 1 (2005), 78–90.

[10] Barut, A., and Raczka, R. *Theory Of Group Representations And Applications*. World Scientific Publishing Company, 1986.

[11] Bassalygo, L. A., and Pinsker, M. S. The complexity of an optimal nonblocking commutation scheme without reorganization. *Problemy Peredachi Informatsii 9*, 1 (1973), 84–87.

[12] Bekka, B., de la Harpe, P., and Valette, A. *Kazhdan's Property (T)*. New Mathematical Monographs. Cambridge University Press, 2008.

[13] Bien., F. Constructions of telephone networks by group representations. *Notices A.M.S 36*, 1 (1979), 5–22.

[14] Bondy, J. A., and Murty, U. S. R. *Graph Theory*. Springer London, 2008.

[15] Brasseur, C., Grady, R. E., and Prassidis, S. Kazhdan's property (t) for graphs, 2006.

[16] Buser, P. A note on the isoperimetric constant. *Annales scientifiques de l'École normale supérieure 15*, 2 (1982), 213–230.

[17] Chandrasekharan, K. *A Course on Topological Groups*. Texts and readings in mathematics. Hindustan Book Agency, 2011.

[18] Chandrasetty, V., and Aziz, S. *Resource Efficient LDPC Decoders: From Algorithms to Hardware Architectures*. Elsevier Science, 2017.

[19] Cheeger., J. A lower bound for the smallest eigenvalue of the laplacian. In *In Problemsin analysis (Papers dedicated to Salomon Bochner, 1969)*. PrincetonUniv. Press, Princeton, 1970, pp. 195–199.

[20] Chen, X., Cheng, K., Li, X., and Ouyang, M. Improved decoding of expander codes. *IEEE Transactions on Information Theory* (2023).

[21] Chilappagari, S. K., Nguyen, D. V., Vasic, B., and Marcellin, M. W. On trapping sets and guaranteed error correction capability of LDPC codes and GLDPC codes. *IEEE Transactions on Information Theory 56*, 4 (2010), 1600–1611.

[22] Davidoff, G., Sarnak, P., and Valette, A. *Elementary Number Theory, Group Theory and Ramanujan Graphs*. Cambridge University Press, jan 2001.

[23] Diestel, J., Spalsbury, A., and Society, A. M. *The Joys of Haar Measure*. Graduate Studies in Mathematics. American Mathematical Society, 2014.

[24] Diestel, R. *Graph Theory*. Springer Berlin Heidelberg, 2017.

[25] Dodziuk, J. Difference equations, isoperimetric inequality and transience of certain random walks. *Transactions of the American Mathematical Society 284*, 2 (1984), 787–794.

[26] Dowling, M. Expander graphs and coding theory. Master's thesis, Clemson University, 2016.

[27] Dowling, M., and Gao, S. Fast decoding of expander codes. *IEEE Transactions on Information Theory 64*, 2 (2017), 972–978.

[28] Effinger, G., and Mullen, G. *Elementary Number Theory*. Textbooks in Mathematics. CRC Press, 2021.

[29] Ershov, M., Jaikin-Zapirain, A., Kassabov, M., and Zhang, Z. Groups graded by root systems and property (t). *Proceedings of the National Academy of Sciences 111*, 50 (nov 2014), 17759–17764.

[30] Feldman, J., Malkin, T., Servedio, R., Stein, C., and Wainwright, M. LP decoding corrects a constant fraction of errors. *IEEE Transactions on Information Theory 53*, 1 (jan 2007), 82–89.

[31] Franceschini, M., Ferrari, G., and Raheli, R. *LDPC Coded Modulations*. Signals and Communication Technology. Springer Berlin Heidelberg, 2009.

[32] Gabber, O., and Galil, Z. Explicit constructions of linear-sized superconcentrators. *Journal of Computer and System Sciences 22*, 3 (jun 1981), 407–420.

[33] Gallager, R. *Low Density Parity Check Codes*. PhD thesis, MIT Press, 1963.

[34] Gao, C., Liu, S., Jiang, D., and Chen, L. Constructing LDPC codes with any desired girth. *Sensors 21*, 6 (2021).

[35] Gardam, G. Expander graphs and kazhdan's property (t). Master's thesis, University of Sydney, 2012.

[36] Gómez Texco, L. A. Códigos LDPC: un acercamiento, 2017. Tesis de licenciatura.

[37] Hoory, S., Linial, N., and Wigderson, A. Expander graphs and their applications. *Bull. Amer. Math. Soc. 43*, 4 (2006), 439–561.

[38] Huerta, L., and López, C. La transformada discreta de fourier y grafos. Notas por publicar, 2020.

[39] Huffman, W., and Pless, V. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2010.

[40] James, G., and Liebeck, M. *Representations and Characters of Groups*. Cambridge University Press, oct 2001.

[41] Jiang, Y. *A Practical Guide to Error-control Coding Using Matlab*. Artech House, 2010.

[42] Jimbo, S., and Maruoka, A. Expanders obtained from affine transformations. *Combinatorica 7*, 4 (dec 1987), 343–355.

[43] Kassabov, M., Lubotzky, A., and Nikolov, N. Finite simple groups as expanders. *Proceedings of the National Academy of Sciences 103*, 16 (apr 2006), 6116–6119.

[44] Kelley, C. A. Minimum distance and pseudodistance lowerbounds for generalized LDPC codes. *Int. J. Inform. and Coding Theory X*, X (2009), XXX–XXX.

[45] Krebs, M., and Shaheen., A. *Expander Families and Cayley Graphs: A Beginner's Guide.* Oxford University Press, 2011.

[46] Ling, S., and Xing, C. *Coding Theory: A First Course.* Cambridge University Press, 2004.

[47] Lubotzky, A. *Discrete Groups, Expanding Graphs and Invariant Measures.* Birkhäuser Basel, 1994.

[48] Lubotzky, A. What is...property (tau)? *Notices of the AMS 52*, 6 (June 2005), 626–627.

[49] Lubotzky, A., Phillips, R., and Sarnak, P. Ramanujan graphs. *Combinatorica 8*, 3 (sep 1988), 261–277.

[50] Lubotzky, A., and Zuk, A. *On property* (τ). (versión preliminar), 2003.

[51] MacKay, D. J., and Neal, R. M. Good codes based on very sparse matrices. In *IMA International Conference on Cryptography and Coding* (1995), Springer, pp. 100–111.

[52] MacWilliams, F. J., and Sloane, N. J. A. *The Theory of Error-Correcting Codes.* Elsiever Science Publishers B.V., 1977.

[53] Margulis, G. A. Explicit constructions of expanders. *Problemy Peredachi Informatsii 9*, 4 (1973), 71–80.

[54] Morgenstern, M. Existence and explicit constructions of $q + 1$ regular ramanujan graphs for every prime power q. *Journal of Combinatorial Theory, Series B 62*, 1 (sep 1994), 44–62.

[55] Roman, S. *Coding and Information Theory.* Springer, 1992.

[56] Sipser, M., and Spielman, D. A. Expander codes. *IEEE transactions on Information Theory 42*, 6 (1996), 1710–1722.

[57] Spielman, D. A. Linear-time encodable and decodable error-correcting codes. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing* (1995), pp. 388–397.

[58] Sun, H. Lectures on algorithmic spectral graph theory. (Versión Revisada), Agosto 2017.

[59] Tanner, M. A recursive approach to low complexity codes. *IEEE Trans. Inform.Theory 27*, 5 (1981), 533–547.

[60] Terras, A. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press, mar 1999.

[61] The Sage Developers. *SageMath, The Sage Mathematics Software System (Version 10)*, 2023. `https://www.sagemath.org`.

[62] Viderman, M. Linear-time decoding of regular expander codes. *ACM Transactions on Computation Theory (TOCT) 5*, 3 (2013), 1–25.

[63] Wicker, S. *Fundamentals of Codes, Graphs, and Iterative Decoding*. Kluwer Academic Publishers, 2002.

[64] Zémor, G. On expander codes. *IEEE Transactions on Information Theory 47*, 2 (2001), 835–837.