An Introduction to Expander Families

Arnaud Girand

Internship Report, June–August 2011

Contents

Introduction

This document was written during the author's internship at the Oxford Mathematical Institute, from June 20 to August 19 2011, under the supervision of Dr. Cornelia Drutu. This internship was endorsed by both the École Normale Supérieure de Cachan and the University of Oxford.

Abstract

In this report we will look into a few properties of expander graphs. Expander families are collection of graphs whose "robustness" (i.e connectivity) we can accurately control as their number of vertices increases ; and as such may be used to conceive computers networks, amongst other applications.

We will begin our journey by examining two ways of defining graph expansion, namely using cardinality arguments and spectral theory. Then we will move on to some basic properties of expander families before trying to know whether or not the natural metrics on such graphs can be accurately represented by our standards, "nature–friendly" ℓ_2 metrics.

In a second part, we will present a well known example of expander family : the Margulis graphs. In order to do this, we will first need to dabble into Kazhdan's property (T) and more precisely try and find out whether the special linear groups $SL_n(\mathbb{Z})$ have this property or not.

In order to keep this report as self–inclusive as possible, we included a few appendices aiming to provide the reader with (almost) all the prerequisites needed to fully understand this document. Each appendix also provides a list of references for further reading on the associated topic.

Notations

Throughout this document, we will be using the following notations :

Generic Notations

- $[n]$ denotes the set $\{1, \ldots, n\} \subset \mathbb{N}$;
- $|A|$ denotes the cardinality of any finite set A ;
- e denotes the vector $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$.

Linear Algebra

- ${}^tU$ denotes the transpose of the matrix U ;
- $\mathcal{L}(V)$ denotes the set of all linear mappings on a vector space V ;
- $\mathcal{P}(V)$ denotes the set of all orthogonal projections on a vector space V ;
- $S_n(\mathbb{R})$ denotes the space of symmetric real $n \times n$ matrices ;
- $S_n^+(\mathbb{R})$ denotes the space of positive semidefinite symmetric real $n \times n$ matrices.

Topology and Measure Theory

- $\mathcal{B}(X)$ denotes the set of Borel sets on a topological space X ;
- $\mathcal{B}(x, r)$ denotes the open ball of center x and radius r for the relevant distance ;
- $\overline{\mathcal{B}}(x, r)$ denotes the closed ball of center x and radius r for the relevant distance ;
- $\overline{\mathrm{conv}}(X)$ denotes the closed convex hull of a set X ;
- the notation $K \subset\subset X$ mean that K is a compact subset of the topological space X.

Computational Complexity

- $\Omega(f(n))$ is the class of all functions $g : \mathbb{N} \to \mathbb{R}$ such that :

$$\exists N \in \mathbb{N},\ \exists C > 0,\ \forall n \geq N,\ g(n) \geq Cf(n)$$

- $\Theta(f(n))$ is the class of all functions $g : \mathbb{N} \to \mathbb{R}$ such that :

$$\exists N \in \mathbb{N},\ \exists C, D > 0,\ \forall n \geq N,\ Df(n) \leq g(n) \leq Cf(n)$$

Chapter 1

Expander Graphs

In this chapter, we consider a finite nonempty d–regular graph $G = (V, E)$. Let n be the cardinality of its vertex set V, which we identify to the set $[n]$ for practical reasons. If the reader is not really into graphs, we recommend that he'd check appendix A.1 beforehand.

1.1 Graph Expansion

In this section we lay out the fundamentals of graph expansion, in order to define an expander graph. Since the expander property is one of "robustness", we will need to give ourselves mean to evaluate how strongly connected a set of vertices is, relatively to its inner complexity.

Definition 1.1.1 (Restricted Edge Set)
Let $S, T \subset V$.
We denote the set of edges from S to T by :

$$E(S,T) := \{(u,v) \in E \mid u \in S,\, v \in T\}$$

Remark : We will simply denote $E(S,S)$ by $E(S)$.

Definition 1.1.2 (Edge Boundary, Expansion Ratio)
Let $S \subset V$.

(i) We define the edge boundary of S by :

$$\partial S := E(S, S^c)$$

(ii) We define the expansion ratio (also called Cheeger constant) of the graph G by :

$$h(G) := \min_{\substack{\emptyset \subsetneq S \subset V \\ |S| \leq \frac{n}{2}}} \frac{|\partial S|}{|S|}$$

The expansion ratio of a graph gives us a mean to estimate the robustness of the associated "network". More precisely, if given a subset $S \subset V$, having a high enough $\frac{|\partial S|}{|S|}$ ratio means that said subset is difficult to disconnect from the remainder of the graph in regard of its inner complexity.

Definition 1.1.3 (Expander Graph)
Let $c > 0$.
We say that the graph G is an (n, d, c)–expander graph if for every subset $S \subset V$, we have :

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

Remark : Plainly, any finite connected d–regular graph is an expander for some $c > 0$.

Example (with an infinite graph) : Let $L(a, b)$ denote the free group with two generators a and b, then consider its Cayley graph $G := \mathcal{C}(L(a, b), \{a, b, a^{-1}, b^{-1}\}$ (see[1.1] fig. 1.1). It is relatively easy to see that this graph doesn't make a "good" expander. Indeed, it suffices to "cut" one edge to completely disconnect any of the four major branches from the rest of the graph.

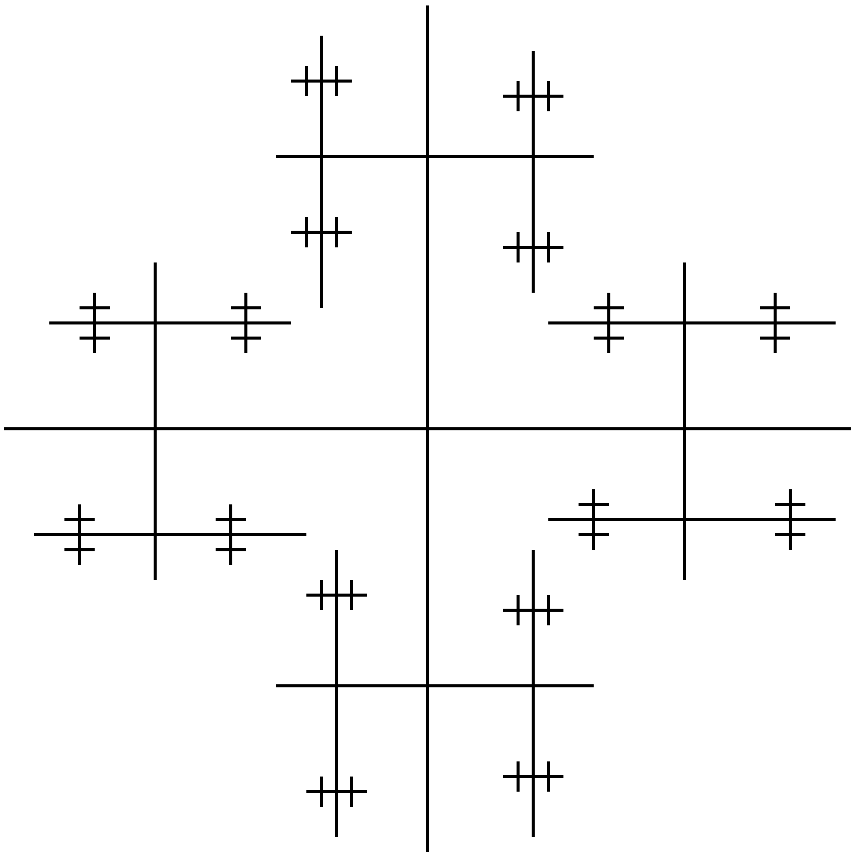

Figure 1.1: Cayley Graph of the Free Group (Rough Sketch)

We wish here to prove the existence of families of graphs whose "robustness" c we can control when their size increases. Such collections of graphs are called families of expanders.

Definition 1.1.4 (Family of Expander Graphs)
Let $(G_i)_{i\in\mathbb{N}}$ be a sequence of d–regular graphs.
We say that $(G_i)_i$ is a family of expander graphs if :

(i) the sequence $(|V(G_i)|)_i$ is increasing ;

(ii) there exists $c > 0$ such that $\forall i \geq 0$, $h(G_i) \geq c$.

Remark : There isn't any nontrivial example of "interesting" such families. We direct the reader to section 2.3 for an example construction method for families of expanders.

1.2 A Spectral Approach of Expanders

Spectral graph theory offers us another way to characterize graph expansion. Indeed, we will show in this section that the expansion ratio of a graph is fully determined by its spectral gap.

[1.1]The reader certainly did notice that this is only a finite "approximation" of the actual Cayley graph. Drawing infinite graph can indeed get quite painful.

1.2.1 Graph Spectrum

Definition 1.2.1 (Adjacency Matrix)
We call adjacency matrix of the graph G the matrix $A(G) = (a_{u,v})_{u,v\in[n]} \in \mathcal{M}_n(\mathbb{R})$ where $a_{u,v}$ is equal to one if $(u, v) \in E$ and else is zero.

Remark : $A(G) \in S_n(\mathbb{R})$, therefore has n real eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$, to which we associate an orthonormal system of eigenvectors $v_1, \ldots, v_n$ so that $\forall 1 \leq i \leq n$ we have $A(G)v_i = \lambda_i v_i$. Note that when need be we will denote these eigenvalues (resp. eigenvectors) by $\lambda_i(G)$ (resp. $v_i(G)$) to avoid any ambiguity. We also denote by $\lambda := \max(|\lambda_2|, |\lambda_n|)$ the largest absolute value of an eigenvalue of G that isn't λ_1.

Definition 1.2.2 (Graph Spectrum)
We call spectrum of the graph G the set $\mathrm{Sp}(G) := \{\lambda_1, \ldots, \lambda_n\}$.

Proposition 1.2.1
The following properties hold :

(i) $\lambda_1 = d$ *and we can choose* $v_1 = \dfrac{1}{\sqrt{n}}e$ *;*

(ii) G *is connected* $\Leftrightarrow \lambda_1 > \lambda_2$.

PROOF :

(i) It is clear that d is an eigenvalue of A because since G is d–regular we have :

$$\forall i \in [n],\ \sum_{j=1}^{n} a_{i,j} = d \tag{1.1}$$

Now let ν be any eigenvalue of A and let v be an associated eigenvector. Since $v \neq 0$, we can normalize v so that there exists $i \in [n]$ such that $v_i = 1$ and $\forall j \in [n]$, $|v_j| \leq 1$ (replace v by $\dfrac{v}{\max_j |v_j|}$). Now remark that :

$$\nu v_i = \sum_{j=1}^{n} a_{i,j} v_j$$

Thus :

$$\begin{aligned}|\nu| &= \left|\sum_{j=1}^{n} a_{i,j} v_j\right| \\ &\leq \sum_{j=1}^{n} |a_{i,j} v_j| \\ &\leq \sum_{j=1}^{n} |a_{i,j}| \\ &= d \text{ since } G \text{ is } d\text{–regular and } \forall j \in [n],\ a_{i,j} \geq 0\end{aligned}$$

Therefore, d is A's largest eigenvalue.

(ii) If G isn't connected then $A(G)$ is block diagonal with at least 2 distinct blocks, and so its characteristic polynomial χ is a product of at least two characteristic polynomials of matrices satisfying (1.1). Therefore $(X - d)^2|\chi$ and so $\lambda_2 = d = \lambda_1$. Conversely, suppose that G is connected and let v be any λ_1 eigenvector for A and rescale v such that its entry of largest absolute value v_i is one. Therefore, we have that $(Av)_i = dv_i = d$. Now since $(Av)_i = \sum_{j=1}^{n} a_{i,j} v_j$, with the $a_{i,j} \in \{0, 1\}$, then at least $d - 1$ other entries v_j are ones. Recall that G is connected and so A isn't block diagonal which implies that by repeating this process with these other $v_j = 1$, we find that all entries in v are ones. Ergo $v = e$ and so any λ_1 eigenvector is a scalar multiple of e and so $\lambda_1 \neq \lambda_2$. The proof is thus concluded.

We now define the spectral gap of a graph as (surprisingly enough) the distance between its two largest eigenvalues. We will show later on that this quantity can fully control the graph's expansion ratio.

Definition 1.2.3 (Spectral Gap)
We call spectral gap of the graph G the real number $g(G)$ defined by :

$$g(G) := \lambda_1 - \lambda_2 = d - \lambda_2$$

The following lemma gives us a mean to compare any graph to its uniform random counterpart, in some sense.

Lemma 1.2.1 (Expander Mixing Lemma)
Recall that G is d–regular.
Let $\lambda := \max(|\lambda_2|, |\lambda_n|)$ be the largest absolute value of an eigenvalue of G that isn't λ_1.
Then, for all $S, T \subset V$:

$$\left| |E(S,T)| - \frac{d|S||T|}{n} \right| \leq \lambda\sqrt{|S||T|}$$

Remark : $|E(S,T)|$ is the actual number of edges between S and T and $\frac{d|S||T|}{n}$ is the expected number of such edges in a random graph of edge density $\frac{d}{n}$. A small λ thus implies that the graph G is nearly random in some sense.

Proof : Let 1_S (resp. 1_T) be the characteristic vector of S (resp. T), i.e the vector whose v–th coordinate (for $v \in V$) is equal to one if $v \in S$ (resp. T), and to zero if $v \notin S$ (resp. T). We then express those two vectors in the system $(v_1, \ldots, v_n)$:

$$1_S = \sum_{i=1}^{n} a_i v_i \text{ and } 1_T = \sum_{i=1}^{n} b_i v_i$$

Then :

$$\begin{aligned}
|E(S,T)| &= {}^t 1_S A 1_T \\
&= \left(\sum_{i=1}^{n} a_i^t v_i\right) A \left(\sum_{j=1}^{n} b_j v_j\right) \\
&= \sum_{i=1}^{n} \lambda_i a_i b_i \\
&= d a_1 b_1 + \sum_{i=2}^{n} \lambda_i a_i b_i \text{ since } \lambda_1 = d
\end{aligned}$$

Recall that since the system $(v_1, \ldots, v_n)$ is orthonormal, we have (for any index i) $a_i = \langle 1_S, v_i \rangle$ and $b_i = \langle 1_T, v_i \rangle$. In particular, $a_1 = \frac{|S|}{\sqrt{n}}$ and $b_1 = \frac{|T|}{\sqrt{n}}$, therefore we have :

$$|E(S,T)| = d\frac{|S||T|}{n} + \sum_{i=2}^{n} \lambda_i a_i b_i$$

We also have :

$$\begin{aligned}\left|\sum_{i=2}^{n}\lambda_i a_i b_i\right| &\leq \sum_{i=2}^{n}|\lambda_i a_i b_i| \\ &\leq \lambda\sum_{i=2}^{n}|a_i b_i| \\ &\leq \lambda\sum_{i=1}^{n}|a_i b_i| \\ \\ &= \lambda\langle 1_S, 1_T\rangle \\ &\leq \lambda\|1_S\|\|1_T\| \text{ by Cauchy–Schwarz} \\ &= \lambda\sqrt{|S||T|}\end{aligned}$$

Hence :

$$\left||E(S,T)| - \frac{d|S||T|}{n}\right| = \left|\sum_{i=2}^{n}\lambda_i a_i b_i\right| \leq \lambda\sqrt{|S||T|}$$

1.2.2 Link Between Spectral Gap and Expansion

In this subsection, we will prove that under certain conditions, a large spectral gap is equivalent to a high expansion ratio for the graph G, namely we can relate the variations of its expansion ratio $h(G)$ to those of its spectral gap. But first, we need to define a couple operators on the mappings "related" to G.

Definition 1.2.4 (Laplacian)
We define the Laplacian operator on mappings $f : V \to \mathbb{R}$ as $L := dI_n - A(G)$, i.e for any such mapping f we have :

$$\forall x \in V,\ Lf(x) := df(x) - (A(G)f)(x)$$

Definition 1.2.5 (Divergence)
We define the divergence of a mapping $g : E \to \mathbb{R}$ as follows :

$$\begin{aligned}\forall x \in V,\ Kg(x) &:= \sum_{e\in E \ \ exits\ x} g(e) - \sum_{e\in E\ \ enters\ x} g(e) \\ &= \sum_{y\,|\,(x,y)\in E} g(x,y) - \sum_{y\,|\,(y,x)\in E} g(y,x)\end{aligned}$$

✍ Note that if $f : V \to \mathbb{R}$ is a real mapping on V we have :

$$\|{}^t fK\|^2 = \sum_{(u,v)\in E}(f(u) - f(v))^2 = {}^t fLf$$

We now aim to demonstrate the following proposition, which links the graph's expansion ratio and its spectral gap :

Proposition 1.2.2
Suppose G connected.
Then :

$$\frac{g(G)}{2} \leq h(G) \leq \sqrt{2dg(G)}$$

Proof : We begin by proving the left inequality : $\dfrac{d-\lambda_2}{2} \leq h(G)$. First, consider a subset $S \subset V$ such that $h(G) = \dfrac{|\partial S|}{|S|}$ and $|S| \leq \dfrac{n}{2}$, then define the function $f := |S^c|\mathbf{1}_S - |S|\mathbf{1}_{S^c}$. Note that we have :

$$\|f\|^2 = |S^c|^2|S| + |S|^2|S^c| = (|S| + |S^c|)|S||S^c| = n|S||S^c|$$

We also have :

$$\begin{aligned}
{}^t f A(G) f &= \sum_{x\in V} f(x) \sum_{y\in V} a_{x,y} f(y) \text{ if we denote by } a_{x,y} \text{ the coefficients of A(G)}\\
&= \sum_{x\in S} f(x) \sum_{y\in V} a_{x,y} f(y) + \sum_{x\in S^c} f(x) \sum_{y\in V} a_{x,y} f(y)\\
&= \sum_{x\in S} |S^c| \left(\sum_{y\in S} a_{x,y}|S^c| + \sum_{y\in S^c} a_{x,y}|S| \right) + \sum_{x\in S^c} |S| \left(\sum_{y\in S} a_{x,y}|S^c| + \sum_{y\in S^c} a_{x,y}|S| \right)\\
&= 2(|E(S)||S^c|^2 + |E(S^c)||S|^2 - |S||S^c||\partial S|)
\end{aligned}$$

Since G is d–regular, we have $|E(S)| = d|S| - |\partial S|$ and $|E(S^c)| = d|S^c| - |\partial S|$ therefore :

$$ {}^t f A(G) f = nd|S||S^c| - n^2|\partial S| $$

Thus :

$$\begin{aligned}
\lambda_2 &\geq \frac{{}^t f A(G) f}{\|f\|^2}\\
&= \frac{nd|S||S^c| - n^2|\partial S|}{n|S||S^c|}\\
&= d - \frac{n|\partial S|}{|S||S^c|}\\
&\geq d - 2h(G) \text{ since } |S^c| \geq \frac{n}{2}
\end{aligned}$$

Let us now prove the right inequality : $h(G) \leq \sqrt{2d(d-\lambda_2)}$. Since the associated eigenvector v_2 is orthogonal to $e = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$, it necessarily has both positive and negative entries, thus we define $f := v_2^+$ (i.e $f : v \mapsto \max(v_2(v), 0)$) and $V^+ := \mathrm{supp}(f)$. We can assume, by replacing v_2 with $-v_2$ if necessary, that $|V^+| \leq \dfrac{n}{2}$ and we aim to prove the two following inequalities :

(i) $\dfrac{{}^t f L f}{\|f\|^2} \leq d - \lambda$;

(ii) $\dfrac{h(G)^2}{2d} \leq \dfrac{{}^t f L f}{\|f\|^2}$.

To prove (i), take $x \in V^+$ and compute :

$$\begin{aligned}
Lf(x) &= df(x) - \sum_{y\in V} a_{x,y} f(y)\\
&= dv_2(x) - \sum_{y\in V^+} a_{x,y} v_2(y)\\
&\leq dv_2(x) - \sum_{y\in V} a_{x,y} v_2(y) \text{ since } \forall y \notin V^+,\ v_2(y) \leq 0\\
&= Lv_2(x)\\
&= dv_2(x) - A(G)v_2(x)\\
&= (d-\lambda)v_2(x)
\end{aligned}$$

As $\forall x \notin V^+,\ f(x) = 0$, we have :

$$\begin{aligned}
{}^t fLf &= \sum_{x \in V} f(x) Lf(x) \\
&\leq \sum_{x \in V} f(x)(d-\lambda) v_2(x) \\
&= (d-\lambda) \sum_{x \in V^+} v_2^2(x) \\
&= (d-\lambda) \sum_{x \in V} f^2(x) \\
&= (d-\lambda) \|f\|^2
\end{aligned}$$

Hence the result. In order to now prove (ii), introduce this other quantity :

$$Bf := \sum_{(x,y) \in E} |f^2(x) - f^2(y)|$$

We now aim to prove the following inequality, which implies (ii) since $\|{}^t fK\|^2 = {}^t fLf$:

$$h(G)\|f\|^2 \leq Bf \leq \sqrt{2d}\|{}^t fK\|\|f\|$$

For ease of notation, we consider that $V = [n]$ is ordered so that $f(1) \geq \ldots \geq f(n)$. To obtain the right inequality, one just has to pursue the following computation :

$$\begin{aligned}
Bf &= \sum_{(x,y) \in E} |f^2(x) - f^2(y)| \\
&= \sum_{(x,y) \in E} |f(x) + f(y)||f(x) - f(y)| \\
&\leq \sqrt{\sum_{(x,y) \in E} (f(x) + f(y))^2} \sqrt{\sum_{(x,y) \in E} (f(x) - f(y))^2} \text{ by Cauchy–Schwarz} \\
&= \sqrt{\sum_{(x,y) \in E} (f(x) + f(y))^2} \|{}^t fK\| \\
&\leq \sqrt{2 \sum_{(x,y) \in E} f(x)^2 + f(y)^2} \|{}^t fK\| \\
&= \sqrt{2d \sum_{x \in V} f^2(x)} \|{}^t fK\| \\
&= \sqrt{2d}\|{}^t fK\|\|f\|
\end{aligned}$$

The left inequality then stems from another calculation on Bf :

$$
\begin{aligned}
Bf &\geq \sum_{\substack{x,y\in E\\ x<y}} (f^2(x) - f^2(y)) \\
&= \sum_{\substack{x,y\in E\\ x<y}} \sum_{i=x}^{y-1} (f^2(i) - f^2(i+1)) \\
&= \sum_{i=1}^{n-1} (f^2(i) - f^2(i+1))|\partial[i]| \\
&= \sum_{i\in V^+} (f^2(i) - f^2(i+1))|\partial[i]| \\
&\geq h(G) \sum_{i\in V^+} (f^2(i) - f^2(i+1))i \\
&= h(G) \sum_{i\in V^+} f^2(i) \text{ by collapsing the telescopic sum and remarking that } f(|V^+|+1) = 0 \\
&= h(G)\|f\|^2
\end{aligned}
$$

We then have inequality (ii), which ends the proof.

1.2.3 Diameter of Expander Graphs

In this subsection we aim to prove that the diameter of an expander graph is $O(\log(n))$. We call diameter of a graph $G = (V, E)$ the following integer (defined exactly as is usually done for bounded metric spaces) :

$$\operatorname{diam}(G) := \max_{x,y\in V} d_G(x, y)$$

Lemma 1.2.2
Let $G = (V, E)$ be a (n, d, c)−expander graph.
Let $r > 0$
Suppose that $|\overline{\mathcal{B}}(x, r)| \leq \frac{n}{2}$.
Then :

$$\exists \varepsilon > 0,\ |\overline{B}(x, r + 1)| \geq (1 + \varepsilon)|\overline{B}(x, r)|$$

Proof : Let $S := \overline{B}(x, r)$ and remark that :

$$|\overline{B}(x, r + 1)| = |S| + |\partial S|$$

Then, by expander property :

$$
\begin{aligned}
|\overline{B}(x, r + 1)| = |S| + |\partial S| &\geq |S| + c\left(1 - \frac{|S|}{n}\right)|S| \\
&\geq |S|\left(1 + c\left(1 - \frac{1}{2}\right)\right) \text{ since } |S| \leq \frac{n}{2} \\
&= \left(1 + \frac{c}{2}\right)|S|
\end{aligned}
$$

The result then follows with $\varepsilon := \frac{c}{2}$.

Proposition 1.2.3
Let $G = (V, E)$ be a (n, d, c)−expander graph.
Then $\operatorname{diam}(G) = O(\log(n))$.

Proof : Let $x \in V$. Suppose that $\forall r > 0$, $|\overline{\mathcal{B}}(x, r)| \leq \frac{n}{2}$. Then, by lemma 1.2.2 we have :

$$\forall r > 0, \exists \varepsilon > 0,\ |\overline{B}(x, r + 1)| \geq (1 + \varepsilon)|\overline{B}(x, r)| > |\overline{\mathcal{B}}(x, r)|$$

So the sequence $(|\overline{\mathcal{B}}(x,r)|)_{r\in\mathbb{N}^*}$ is an increasing sequence of integers and so $|\overline{\mathcal{B}}(x,r)| \xrightarrow[r\to\infty]{} \infty$, which is impossible since V is finite. Thus :

$$\forall x \in V,\ \exists r(x) > 0,\ |\overline{\mathcal{B}}(x, r(x))| > \frac{n}{2}$$

Now let $r := \max_{x\in V} r(x)$. Since V is finite, r is well defined and so we have :

$$\exists r > 0\, \forall x \in V,\ |\overline{\mathcal{B}}(x, r)| > \frac{n}{2}$$

Furthermore, since the ball $\overline{\mathcal{B}}(x,r)$ contains less than d^r elements (as G is d–regular), we can take r so that $d^r \leq n$ (another way to achieve this is to set for every x $r(x) := \min\left\{\rho > 0 \,\middle|\, |\overline{\mathcal{B}}(x,\rho)| > \frac{n}{2}\right\}$) and so $r \leq \log_d(n)$. Hence we have proved that :

$$\exists r = O(\log(n)),\ \forall x \in V,\ |\overline{\mathcal{B}}(x, r)| > \frac{n}{2}$$

Now fix $x \in V$ and suppose that there exists $y \in V$ such that $d_G(x, y) > 2r$. Then we naturally have :

$$\overline{\mathcal{B}}(x, r) \cap \overline{\mathcal{B}}(y, r) = \emptyset$$

But this last equality is clearly false, since both $|\overline{\mathcal{B}}(x,r)|$ and $|\overline{\mathcal{B}}(y,r)|$ are over $\frac{n}{2}$. Thus there is no such vertex y, henceforth $V = \overline{\mathcal{B}}(x, 2r)$. This in turn implies that :

$$\operatorname{diam}(G) \leq 4r = O(\log(n))$$

1.3 Metric Embeddings of Expander Graphs

The metric embedding problem for graphs can be summed up as follows : given a finite graph G, how well can the associated metric d_G be approximated by an Euclidean metric ? In particular, we will interest ourselves in the embedding of expander graphs into ℓ_2 spaces. But first, we need to define what we mean by "approximated by an Euclidean metric".

1.3.1 Some Generic Results

Definition 1.3.1 (Metric Embedding)
Let (X, d) and (Y, e) be two metric spaces.
We say that a map $f : X \to Y$ is a metric embedding if $f : X \to f(X)$ is an homeomorphism.

Remark : In particular, any metric embedding is injective and continuous.

Definition 1.3.2 (Expansion, Contraction and Distortion)
Let (X, d) be a finite metric space.
Let $f : X \to \mathbb{R}^n$.
We then define the following quantities :

(i) the expansion of f :

$$e(f) := \max_{x,y\in X} \frac{\|f(x) - f(y)\|}{d(x, y)}$$

(ii) the contraction of f :

$$c(f) := \max_{x,y\in X} \frac{d(x, y)}{\|f(x) - f(y)\|}$$

(iii) the distortion of f :

$$\partial(f) := e(f) \times c(f)$$

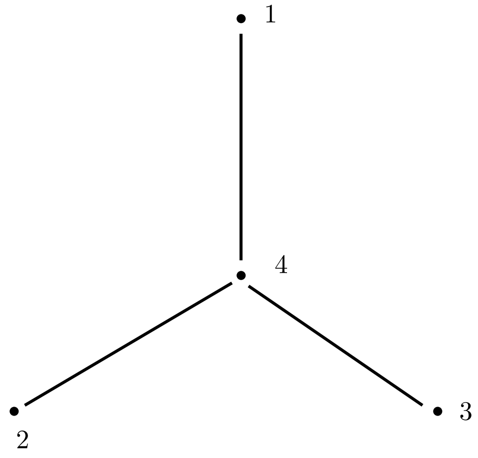

Figure 1.2: A very simple – although nontrivial – graph.

So our problem can be formulated as follows : given a finite graph $G = (V, E)$, what is the minimum distortion an embedding $f : (G, d_G) \to \ell_2^n$ can achieve ? The best scenario would be to have $\partial(f) = 1$ (in such a case, we say that f is without distortion), but this obviously can only happen in very specific[1.2] cases : indeed, even very simple graphs[1.3] like the one in Fig. 1.2 can not be embedded without distortion.

Let us see why such a graph (let's call it $G = (V, E)$), simple as it may be, does not "fit" in any Euclidean metric, not matter how high the dimension. Suppose that we have a distortion–free embedding $f : V \to \mathbb{R}^n$, such that $\partial(f) = 1$. Then, as $d_G(1, 4) = d_G(3, 4) = d_G(2, 4) = 1$ and $d_G(i, j) = 2$ for all other pairings of $i, j \in [4]$, then, if we denote the ℓ_2 norm by $\|.\|$, we must have $\|f(1) - f(4)\| = \|f(3) - f(4)\| = \|f(2)f(4)\| = 1$ and $\|f(i) - f(j)\| = 2$ otherwise, which implies that $f(1), f(2)$ and $f(4)$ must be aligned, as do $f(1), f(2)$ and $f(3)$. All in all, all the points of our embedded graph must be on the same line, which contradicts the distance conditions previously stated.

The first result we will prove here is a very general one, which we can apply to any finite metric space (and so to any finite graph) :

Proposition 1.3.1
Let (X, d) be a finite metric space of cardinality n.
Let $p > 2$.
Then there exists $Q = O(\log(n)^2)$ such that we can find in polynomial time (in n) an embedding $f : X \to \ell_p^Q$ so that $\partial(f) = O(\log(n))$.

Proof : Consider $x, y \in X$ such that $x \neq y$ and set $\rho_0 = 0$. Then, whenever such a thing is possible, define ρ_t ($t \in \mathbb{N}^*$) to be the minimal radius so that the following conditions are satisfied :

1. $|\overline{\mathcal{B}}(x, \rho_t)| \geq 2^t$;
2. $|\overline{\mathcal{B}}(y, \rho_t)| \geq 2^t$;
3. $\rho_t \leq \dfrac{1}{4} d(x, y)$.

Then let $\widehat{t}$ be the largest integer t such that we can define such a radius ρ_t and set $\rho_{\widehat{t}+1} := \dfrac{1}{4} d(x, y)$. Lastly, remark that :

$$\forall i, j \in [\widehat{t} + 1],\ \overline{\mathcal{B}}(y, \rho_j) \cap \overline{\mathcal{B}}(x, \rho_i) = \emptyset$$

Also observe that, for any $A \subset X$ and $t \in [\widehat{t}]$, we have :

$$A \cap \mathcal{B}(x, \rho_t) = \emptyset \Leftrightarrow d(x, A) \geq \rho_t$$

And :

$$A \cap \overline{\mathcal{B}}(y, \rho_t) \neq \emptyset \Leftrightarrow d(y, A) \leq \rho_t$$

[1.2] By "specific" we mostly mean "not so interesting" ...
[1.3] At this point, we will be very upset if we hear about the empty graph ...

Thus, if $A \cap \mathcal{B}(x, \rho_t) = A \cap \overline{\mathcal{B}}(y, \rho_{t-1}) = \emptyset$, then :

$$|d(y, A) - d(x, A)| \geq \rho_t - \rho_{t-1}$$

Now fix $t \in [\widehat{t}]$. By exchanging if necessary the roles played by x and y, we can also assume that $|\mathcal{B}(x, \rho_t)| < 2^t$, which implies that $|\overline{\mathcal{B}}(y, \rho_{t-1})| \geq 2^t$ and so any random set of size $\Theta\left(\frac{n}{2^t}\right)$ has the same probability of both intersecting $\overline{\mathcal{B}}(y, \rho_{t-1})$ and missing (i.e not intersecting) $\mathcal{B}(x, \rho_t)$.

Randomly select $q = O(\log(n))$ sets $A_1, \ldots, A_q \subset X$ of cardinality $2^{m(t)}$, where :

$$m(t) := \min \left\{ k \in \mathbb{N} \;\middle|\; 2^k \geq \frac{n}{2^{t+1}} \right\}$$

So, with high probability (remember that we are looking for an algorithm), at least $\frac{q}{10}$ of the chosen sets will intersect $\overline{\mathcal{B}}(y, \rho_{t-1})$ but not $\mathcal{B}(x, \rho_t)$. Also note that this also holds for $t = \widehat{t} + 1$ since we only want to miss a set of cardinality less than $2^{\widehat{t}+1}$ and intersect one of cardinality greater or equal to $2^{\widehat{t}}$.

Thus, for almost every choice of $A_1, \ldots, A_q$ and any $t \in [\widehat{t} + 1]$, we have :

$$\sum_{i=1}^{q} |d(x, A_i) - d(y, A_i)| \geq \log(n) \frac{\rho_t - \rho_{t-1}}{10}$$

Now repeat this for every $t \in [\widehat{t} + 1]$. We now have $Q = O(\log(n)^2)$ sets $A_1, \ldots, A_Q \subset X$ such that :

$$\begin{aligned}
\sum_{i=1}^{Q} |d(x, A_i) - d(y, A_i)| &\geq \frac{\log(n)}{10} \sum_{i=1}^{\widehat{t}+1} \rho_i - \rho_{i-1} \\
&= \frac{\log(n)}{10} (\rho_{\widehat{t}+1} - \underbrace{\rho_0}_{=0} \\
&\geq \log(n) \frac{d(x, y)}{40}
\end{aligned}$$

Remark that for any A_i, $|d(x, A_i) - d(y, A_i)| \leq d(x, y)$ and so, since $Q = O(\log(n)^2)$, there exists $C > 0$ such that :

$$\sum_{i=1}^{Q} |d(x, A_i) - d(y, A_i)| \leq C \log(n)^2 d(x, y)$$

Now show that the following mapping is a metric embedding with distortion $O(\log(n))$:

$$\begin{aligned}
f : X &\to \ell_p^Q \\
x &\mapsto \left(\frac{d(x, A_i)}{Q^{\frac{1}{p}}} \;\middle|\; i \in [Q] \right)
\end{aligned}$$

Indeed, if we fix $x, y \in X$ and set $\tau(x, y) = \|f(x) - f(y)\|$ then, since for any A_i, $|d(x, A_i) - d(y, A_i)| \leq d(x, y)$, $\tau(x, y) \leq d(x, y)$ and :

$$\begin{aligned}
d(x, y) &\leq \frac{40}{\log(n)} \sum_{i=1}^{Q} |d(x, A_i) - d(y, A_i)| \\
&= O\left(\frac{\log(n)}{n} \sum_{i=1}^{Q} |d(x, A_i) - d(y, A_i)| \right) \\
&= O(\log(n) \tau(x, y))
\end{aligned}$$

In conclusion, we did prove that it was possible to find such an embedding f in polynomial time, as claimed.

Definition 1.3.3
Let (X, d) be a finite metric space.
We denote the least distortion with which X may be embedded into ℓ_p (of any dimension) by $c_p(X)$.

Remark : One deduces from proposition 1.3.1 that for any $p > 2$ $c_p(X) = O(\log(|X|)$. We will show later on that this holds if $p = 2$ for expander graphs.

Let us now prove another computational result. But first, we recall the following lemma from linear algebra :

Lemma 1.3.1
A matrix $M \in \mathcal{M}_n(\mathbb{R})$ is positive semidefinite if and only if there exists another matrix $A \in \mathcal{M}_n(\mathbb{R})$ such that $M = {}^tAA$.

Also remark that for any embedding f of a finite metric space $(X = \{x_1, \ldots, x_N\}, d)$ into ℓ_p, we can scale f so that $c(f) = 1$ thus for every $\gamma > 0$ we have :

$$\partial(f) \leq \gamma \Leftrightarrow \forall i, j \in [N],\ d(x_i, x_j)^2 \leq \|f(x_i) - f(x_j)\|^2 \leq \gamma^2 d(x_i, x_j)^2 \tag{1.2}$$

Now we prove the computational result we promised :

Proposition 1.3.2
Let $(X = \{x_1, \ldots, x_n\}, d)$ be a finite metric space.
Then there exists a polynomial time algorithm which computes $c_2(X)$.

Proof : Let $f : X \to \ell_2^n$ be an embedding and, for all $i \in [n]$, set $u_i := f(x_i)$. Now let $U \in \mathcal{M}_n(\mathbb{R})$ be the matrix whose rows are the vectors u_i and let $Z := U^tU$. With these notations we have :

$$\|u_i - u_j\|^2 = z_{i,i} + z_{j,j} - 2z_{i,j}$$

Finding f satisfying (1.2) for any given $\gamma > 0$ is thus equivalent to finding a matrix $Z \in S_n^+(\mathbb{R})$ such that :

$$\forall i, j \in [n],\ d(x_i, x_j)^2 \leq z_{i,i} + z_{j,j} - 2z_{i,j} \leq \gamma^2 d(x_i, x_j)^2 \tag{1.3}$$

Therefore $c_2(X) \leq \gamma$ if and only if we can find a matrix $Z \in S_n^+(\mathbb{R})$ satisfying (1.3). The result now stems from the fact that such an optimisation problem can be solved in polynomial time using the ellipsoid algorithm (cf. [Aro05] for more details).

We now close on the main theorem of this section : an explicit formula for $c_2(X)$, coming from a paper by Linial, London and Rabinovich (cf. [LLR95]). But we first need to recall yet another linear algebra result.

Lemma 1.3.2
Let $Z \in \mathcal{M}_n(\mathbb{R})$.
Then :

$$Z \in S_n^+(\mathbb{R}) \ \Leftrightarrow\ \forall Q \in S_n^+(\mathbb{R}),\ \sum_{i=1}^{n}\sum_{j=1}^{n} q_{i,j} z_{i,j} \geq 0$$

In light of this lemma, the optimization problem alluded earlier can be reformulated as follows (note also that the following reformulation is "easier" to feed to the ellipsoid algorithm) :

Problem (P1)
Let $(X = \{x_1, \ldots, x_n\}, d)$ be a finite metric space.
Let $\gamma > 0$.
Find a matrix $Z \in \mathcal{M}_n(\mathbb{R})$ such that :

$$\forall Q \in S_n^+(\mathbb{R}),\ \sum_{i=1}^{n}\sum_{j=1}^{n} q_{i,j} z_{i,j} \geq 0 \tag{1.4}$$

$$\forall i, j \in [n],\ z_{i,i} + z_{j,j} - 2z_{i,j} \geq d(x_i, x_j)^2 \tag{1.5}$$

$$\forall i, j \in [n],\ z_{i,i} + z_{j,j} - 2z_{i,j} \leq \gamma^2 d(x_i, x_j)^2 \tag{1.6}$$

We will now use the fact that problem (P1) for any given $\gamma > 0$ is equivalent to $c_2(X) \leq \gamma$ to prove this section's main theorem, which is the following :

Theorem 1.3.3 (Linial – London – Rabinovich)
Let (X,d) be a finite metric space.
Then :

$$c_2(X) = \max_{\substack{Q \in S_n^+(\mathbb{R}) \\ Qe=0}} \sqrt{\frac{\sum_{\substack{i,j\in[n] \\ q_{i,j}>0}} q_{i,j} d(x_i,x_j)^2}{-\sum_{\substack{i,j\in[n] \\ q_{i,j}<0}} q_{i,j} d(x_i,x_j)^2}}$$

PROOF : Let $\gamma < c_2(X)$ be a positive real number. Since (P1) for γ is equivalent to the fact that $\gamma \geq c_2(X)$, any nonnegative linear combination of the constraints (1.4), (1.5) and (1.6) applied to γ *must* yield a contradiction. So we apply the following steps to the aforementioned constraints :

- if $q_{i,j} = 0$, multiply any constraint in (P1) involving $z_{i,j}$ by 0 ;
- if $q_{i,j} > 0$, multiply the constraints of type (1.5) involving $z_{i,j}$ by $\frac{q_{i,j}}{2}$;
- if $q_{i,j} < 0$, multiply the constraints of type (1.6) involving $z_{i,j}$ by $\frac{q_{i,j}}{2}$.

Now we choose Q so that $Qe = 0$, i.e :

$$\forall i \in [n], \sum_{j=1}^{n} q_{i,j} = 0$$

Then, by combining the constraints in (P1), we obtain :

$$\sum_{\substack{i,j\in[n] \\ q_{i,j}>0}} q_{i,j} d(x_i,x_j)^2 + \gamma^2 \sum_{\substack{i,j\in[n] \\ q_{i,j}<0}} q_{i,j} d(x_i,x_j)^2 \leq 0 \tag{1.7}$$

Since $\gamma < c_2(X)$, then (1.7) is false and thus we must have :

$$\gamma^2 < \frac{\sum_{\substack{i,j\in[n] \\ q_{i,j}>0}} q_{i,j} d(x_i,x_j)^2}{-\sum_{\substack{i,j\in[n] \\ q_{i,j}<0}} q_{i,j} d(x_i,x_j)^2} \tag{1.8}$$

And so :

$$\gamma < \sqrt{\frac{\sum_{\substack{i,j\in[n] \\ q_{i,j}>0}} q_{i,j} d(x_i,x_j)^2}{-\sum_{\substack{i,j\in[n] \\ q_{i,j}<0}} q_{i,j} d(x_i,x_j)^2}}$$

Which implies that :

$$c_2(X) < \max_{\substack{Q \in S_n^+(\mathbb{R}) \\ Qe=0}} \sqrt{\frac{\sum_{\substack{i,j\in[n] \\ q_{i,j}>0}} q_{i,j} d(x_i,x_j)^2}{-\sum_{\substack{i,j\in[n] \\ q_{i,j}<0}} q_{i,j} d(x_i,x_j)^2}}$$

Now take $\gamma \geq c_2(X)$. Then (1.7) must hold since it is a linear combination of the constraints in (P1) and so :

$$\gamma \geq \sqrt{\frac{\sum_{\substack{i,j\in[n] \\ q_{i,j}>0}} q_{i,j} d(x_i,x_j)^2}{-\sum_{\substack{i,j\in[n] \\ q_{i,j}<0}} q_{i,j} d(x_i,x_j)^2}}$$

Therefore we have :

$$c_2(X) \geq \max_{\substack{Q \in S_n^+(\mathbb{R}) \\ Qe=0}} \sqrt{\frac{\sum_{\substack{i,j\in[n] \\ q_{i,j}>0}} q_{i,j} d(x_i,x_j)^2}{-\sum_{\substack{i,j\in[n] \\ q_{i,j}<0}} q_{i,j} d(x_i,x_j)^2}}$$

Thus the proof is concluded.

1.3.2 Embedding Expander Graphs into ℓ_2 Spaces

We will now try to answer our opening question : how accurately can we approximate an expander graph's metric using ℓ_p metrics ? We will focus on the ℓ_2 case and show that the graph metric of an expander is as far from an ℓ_2 metric as possible.

First, consider a k–regular graph $G = (V = \{v_1, \ldots, v_n\}, E)$, with $|V| = n$ and $k \geq 3$ (thus $n \geq 4$). Assume that there exists a positive ε such that $\lambda_2(G) \leq k - \varepsilon$. Then we define the following embedding (where $(e_i)_{i \in [n]}$ denotes the canonical basis of $\mathbb{R}^n$) :

$$\begin{aligned} f : V &\to \ell_2^n \\ v_i &\mapsto \frac{e_i}{\sqrt{2}} \end{aligned}$$

This embedding maps the vertex set V onto the simplex. Moreover, for all $i, j \in [n]$, we have :

$$\|f(v_i) - f(v_j)\| = \frac{1}{\sqrt{2}}\|e_i - e_j\| = \frac{\sqrt{2}}{\sqrt{2}} = 1$$

And thus :

$$c(f) = \max_{i,j \in [n]} d_G(x_i, x_j) = \mathrm{diam}(G)$$

Moreover, since $\forall i, j \in [n]$, $d_G(x_i, x_j) \geq 1$ and there exist $i, j \in [n]$ such that $d_G(x_i, x_j)$, then :

$$e(f) = \max_{i,j \in [n]} \frac{1}{d_G(x_i, x_j)} = 1$$

Now, if G is an expander we know that $\mathrm{diam}(G) = O(\log(n))$ and so any expander graph can be embedded into ℓ_2 by mean of this mapping f with distortion $\partial f = O(\log(n))$. We will now aim to prove that this embedding is optimal , up to a multiplicative constant independent of n.

For the remainder of this subsection, we consider an (n, k, c)–expander graph $G = (V, E)$, with $n \equiv 0[2]$ and $k \geq 3$.

Lemma 1.3.3
Let $H := (V, E')$ be the spanning subgraph of G whose edge set E' is defined as follows :

$$E' := \{(e, f) \in V^2 \,|\, d_G(e, f) \geq \lfloor \log_k(n) \rfloor\}$$

Then H has a perfect matching.

Proof : Since G is k–regular, any vertex in G has less than k^r vertices within distance r for any $r \geq 0$, so if we take $r := \lfloor \log_k(n) \rfloor - 1$ then $k^r \leq \frac{n}{2}$ thus H has minimal degree of at least $\frac{n}{2}$. Therefore, by the Dirac theorem (theorem A.1.3), H has a Hamilton cycle and thus a perfect matching (since n is even).

The next result, another theorem by Linial, London and Rabinovich, proves that the estimate in $O(\log(n))$ is optimal for expander graphs. One may find the condition $\lambda_2(G) \leq k - \varepsilon$ artificial, but it is in fact redundant with the k–regular and connected nature of the expander graph studied (see proposition 1.2.1, (i) and (ii)).

Proposition 1.3.4 (Linial – London – Rabinovich)
Assume that there exists $\varepsilon > 0$ such that $\lambda_2(G) \leq k - \varepsilon$.
Then $c_2(G) = \Omega(\log(n))$ and the implicit constant depends only on k and ε.

Proof : Define a subgraph H of G as in lemma 1.3.3. We know that H has a perfect matching, whose adjacency matrix we denote by B. Define the following matrix :

$$P := kI_n - A(G) + \frac{\varepsilon}{2}(B - I_n)$$

Now remark that if, for any $i, j \in [n]$, $b_{i,j} = 1$, then as $d_G(i,j) \geq \lfloor \log_k(n) \rfloor > 1$ then $a_{i,j} = 0$. Therefore, if furthermore $i \neq j$, $p_{i,j} = \frac{\varepsilon}{2}$. If on the contrary $b_{i,j} = 0$ and $i \neq j$ then $p_{i,j} = -a_{i,j} \in \{0, 1\}$. From this we deduce two things. First :

$$\begin{aligned} - \sum_{\substack{i,j \in [n] \\ p_{i,j} < 0}} p_{i,j} d_G(i,j)^2 &= \sum_{\substack{i,j \in [n] \\ p_{i,j} < 0}} d_G(i,j)^2 \\ &= \sum_{i=1}^{n} \sum_{\substack{j \in [n] \\ p_{i,j} < 0}} d_G(i,j)^2 \end{aligned}$$

For any given $i \in [n]$, there are less than $k^{\lfloor \log_k(n) \rfloor} \leq n$ vertices within distance $\lfloor \log_k(n) \rfloor$. We've seen that to have $p_{i,j} < 0$ (we only consider the case $i \neq j$ since $d(i,i)^2 = 0$) we need to have $a_{i,j} = 1$ and so $d_G(i,j) = 1$. Therefore :

$$\begin{aligned} - \sum_{\substack{i,j \in [n] \\ p_{i,j} < 0}} p_{i,j} d_G(i,j)^2 &= \sum_{i=1}^{n} \sum_{\substack{j \in [n] \\ p_{i,j} < 0}} 1 \\ &= \sum_{i=1}^{n} k \text{ since } A \text{ is } k\text{–regular and therefore for any } i,\ a_{i,j} = 1 \text{ for exactly } k \text{ values of } j \\ &= nk \end{aligned}$$

On the other hand :

$$\begin{aligned} \sum_{\substack{i,j \in [n] \\ p_{i,j} > 0}} p_{i,j} d_G(i,j)^2 &= \sum_{\substack{i,j \in [n] \\ b_{i,j} = 1}} p_{i,j} d_G(i,j)^2 \\ &\geq \frac{\varepsilon}{2} \sum_{\substack{i,j \in [n] \\ b_{i,j} = 1}} \lfloor \log_k(n) \rfloor^2 \\ &\geq \frac{\varepsilon}{2} n \lfloor \log_k(n) \rfloor^2 \end{aligned}$$

In fine, we have :

$$c_2(X) \geq \frac{\varepsilon}{2k} \lfloor \log_k(n) \rfloor^2 = \Omega(\log(n))$$

And so the proof is complete.

To put this result into perspective, we recall the following theorem :

Theorem 1.3.5 (Bourgain)
Any finite metric space of cardinality $n \geq 1$ can be embedded into any ℓ_p space ($p > 0$) with distortion $O(\log(n))$

One consequence of this result is that, basically, there is nothing worse than expander graphs when it comes to metric embeddings. Indeed, the upper bound on the c_2 constant given by Bourgain is in this case optimal, as we just proved. This justifies our earlier saying that expander graphs where "as far as possible" from ℓ_2 metrics.

Chapter 2

The Margulis Construction

In this chapter, we give our first[2.1] example of expander family. Since this construction, named after its creator Grigory Margulis, makes heavy use of Kazhdan's property (T) we will begin by proving a few related results.

2.1 Kazhdan Groups

This first section recalls the basics of Kazhdan groups theory. The reader already familiar with these may turn to section 2.2 (or even 2.3 if he is also familiar with the Kazhdan constants of $SL_n(\mathbb{Z})$). On the other hand, those struggling with representation theory may find some comfort[2.2] in appendix A.2.

Definition 2.1.1 (Almost Invariant Vectors)
Let G be a topological group.
Let $(\pi, \mathcal{H})$ be a unitary representation of G.

(i) Consider $Q \subset G$ and $\varepsilon > 0$. We say that a vector $\xi \in \mathcal{H}$ is (Q,ε)–invariant if :

$$\sup_{x \in Q} \|\pi(x)\xi - \xi\| < \varepsilon \|\xi\|$$

(ii) We say that $(\pi, \mathcal{H})$ almost has invariant vectors if the representation $(\pi, \mathcal{H})$ has a (Q,ε) invariant vector for any compact subset $Q \subset\subset G$ and any positive real number ε.

Remark : $\xi \in \mathcal{H}$ is (Q,ε)–invariant if and only if it is $(\overline{Q \cup Q^{-1}}, \varepsilon)$–invariant. This follows from the fact that $\forall g \in G$, $\|\pi(g)\xi - \xi\| = \|\pi(g^{-1})\xi - \xi\|$.

Definition 2.1.2 (Kazhdan Group)
Let G be a topological group.

(i) We say that a subset $Q \subset G$ is Kazhdan if there exists $\varepsilon > 0$ such that every unitary representation of G which has a (Q,ε)–invariant vector also has a nontrivial invariant vector. Any such ε is called a Kazhdan Constant for Q and (Q,ε) is called a Kazhdan pair for G.

(ii) G is said to be a Kazhdan group, or to have property (T), if it has a compact Kazhdan subset.

We will now denote by ρ_0 the one–dimensional trivial representation on a topological group G.

Definition 2.1.3 (Kazhdan Constant)
Let G be a topological group.
Let $(\pi, \mathcal{H})$ be a unitary representation of G.
Let $Q \subset\subset G$.
We define the Kazhdan constant of G associated to Q and π as follows :

$$\kappa(G, Q, \pi) := \inf_{\xi \in \mathcal{H},\, \|\xi\|=1} \max_{x \in Q} \|\pi(x)\xi - \xi\|$$

[2.1] And only ...
[2.2] Or at least, we hope, some measure of relief.

We also define the Kazhdan constant of G and Q as the lower bound (on π) of such constants :

$$\kappa(G,Q) := \inf_{\pi \text{ unitary representation}} \kappa(G,Q,\pi)$$

Remark : Under these circumstances, it is clear that for any unitary representation π we have that :

$$\rho_0 \propto \pi \Leftrightarrow \forall Q \subset\subset G,\ \kappa(G,Q,\pi) = 0$$

Therefore :

$$G \text{ has property } (T) \Leftrightarrow \exists Q \subset\subset G,\ \kappa(G,Q) > 0 \tag{2.1}$$

If this is the case, then the Kazhdan constant $\kappa(G,Q)$ is the optimal ε such that (Q,ε) is a Kazhdan pair.

Let us now introduce our first example family of Kazhdan groups : the compact groups.

Proposition 2.1.1
Let G be a topological group.
Then $(G,\sqrt{2})$ is a Kazhdan pair. In particular, every compact group has property (T).

Proof : Let $(\pi,\mathcal{H})$ be a unitary representation of G which has a unit vector ξ such that :

$$\sup_{x\in G} \|\pi(x)\xi - \xi\| < \sqrt{2}$$

Also define $C := \overline{\text{conv}}(\pi(G)\xi) \subset \mathcal{H}$. Then $\exists! \eta_0 \in C$, $\|\eta_0\| = \min_{\eta\in C}\|\eta\|$. Since C is G–invariant and $\forall x \in G, \forall \eta \in \mathcal{H}$, $\|\pi(x)\eta\| = \|\eta\|$ the uniqueness of η_0 yields that it is a G–invariant vector.

All we now need to show is that $\eta_0 \neq 0$. We begin by setting :

$$\varepsilon := \sqrt{2} - \sup_{x\in G}\|\pi(x)\xi - \xi\| > 0$$

Then, as ξ is of unit norm, we have, for $x \in G$:

$$2 - 2\Re(\langle \pi(x)\xi, \xi\rangle) = \|\pi(x)\xi - \xi\|^2 \leq (\sqrt{2}-\varepsilon)^2$$

Hence :

$$\Re(\langle \pi(x)\xi,\xi\rangle) \geq \frac{2-(\sqrt{2}-\varepsilon)^2}{2} = \varepsilon\frac{2\sqrt{2}-\varepsilon}{2} > 0$$

Thus :

$$\forall \eta \in C,\ \Re(\eta,\xi\rangle) \geq \varepsilon\frac{2\sqrt{2}-\varepsilon}{2} > 0$$

And so $0 \notin C$. In particular, $\eta_0 \neq 0$ so π has a nontrivial invariant vector, as claimed.

Property (T) can also be expressed using weak containment, as shown by the following proposition :

Proposition 2.1.2
Let G be a topological group.
The following statements are equivalent :

(i) G has property (T) ;

(ii) whenever a unitary representation $(\pi,\mathcal{H})$ of G weakly contains ρ_0, it contains ρ_0.

Proof : It is obvious that (i) implies (ii). Conversely, assume that G doesn't have property (T), and set $I := \{(Q,\varepsilon)\,|\,Q \subset\subset G,\ \varepsilon > 0\}$. Then for every $(Q,\varepsilon) \in I$, there exists a unitary representation $(\pi_{Q,\varepsilon},\mathcal{H}_{Q,\varepsilon})$ without nontrivial invariant vector but with a unit (Q,ε)–invariant vector. Now define the following unitary representation of G :

$$\pi := \bigoplus_{(Q,\varepsilon)\in I} \pi_{Q,\varepsilon}$$

Plainly, $\rho_0 \propto \pi$, but if we consider an invariant vector ξ for π then $\forall (Q,\varepsilon) \in I$, the coordinate $\xi_{Q,\varepsilon}$ is a $\pi_{Q,\varepsilon}$–invariant vector, so is trivial. In fine, $\xi = 0$ and so $\rho_0 \not\subset \pi$.

Property (T) can also be reformulated using the Fell topology (cf. definition A.2.11) through the following proposition, of which the reader will find a proof in [BdlHV08].

Proposition 2.1.3
Let G be a topological group.
The following statements are equivalent :

(i) G *has property* (T) *;*

(ii) ρ_0 *is isolated in* $\mathcal{R} \cup \{\rho_0\}$ *for every set* $\mathcal{R}$ *of equivalence classes of unitary representations of* G *without invariant vector.*

The following lemma will see some use while proving our main theorem in section 2.3 :

Lemma 2.1.1
Let Γ be a finitely generated Kazhdan group.
Let S be a finite generating set of Γ.
Let K be a compact (i.e finite) subset of Γ. We assume that each $k \in K$ can be written as a word of length at most ℓ in the elements of S.
Let $(\rho, \mathcal{H})$ be a nontrivial representation of Γ.
Suppose that for some $v \in \mathcal{H}$ we have :

$$\forall s \in S,\ \|\rho(s)v - v\| < \varepsilon \|v\|$$

Then :

$$\forall k \in K,\ \|\rho(k)v - v\| < \ell\varepsilon \|v\|$$

Proof : Let $k = s_1 \dots s_n \in K$, with $s_i \in S$ $(n \geq \ell)$. Then :

$$\begin{aligned}
\|\rho(k)v - v\| &= \left\| \prod_{i=1}^{n} \rho(s_i)v - v \right\| \\
&= \left\| \prod_{i=1}^{n} \rho(s_i)v - \prod_{i=2}^{n} \rho(s_i)v + \prod_{i=2}^{n} \rho(s_i)v - v \right\| \\
&\leq \left\| \rho(s_1) \left(\prod_{i=2}^{n} \rho(s_i) \right) - \prod_{i=2}^{n} \rho(s_i)v \right\| + \left\| \prod_{i=2}^{n} \rho(s_i)v - v \right\| \\
&\leq \varepsilon\|v\| + \left\| \prod_{i=2}^{n} \rho(s_i)v - v \right\| \\
&\vdots \\
&\leq n\varepsilon\|v\| \text{ by induction} \\
&\leq \ell\varepsilon\|v\|
\end{aligned}$$

Remark : This lemma shows that if there exists $\varepsilon > 0$ such that $\forall v \in \mathcal{H}$, $\exists k \in K$ such that $\|\rho(k)v - v\| > \varepsilon$ then $\forall v \in \mathcal{H}$, $\exists s \in S$ such that $\|\rho(s)v - v\| > \varepsilon$.

We will also need to define a relative version of property (T). The reader may find further details on many applications of this new property in [Jau07].

Definition 2.1.4 (Relative Property (T))
Let G be a topological group.
Let H be a closed subgroup of G.
We say that the pair (G, H) has relative property (T) if there exist $Q \subset\subset G$ and $\varepsilon > 0$ such that every unitary representation of G which has (Q, ε)–invariant vectors has a nontrivial vector invariant under H. In that case, we call (Q, ε) a Kazhdan pair for (G, H).

✍ More concretely, this means that if $(\pi, \mathcal{H})$ is a unitary representation of G which has (Q, ε)–invariant vectors, then there exists $\xi \in \mathcal{H} \setminus \{0\}$ such that $\forall h \in H$, $\pi(h)\xi = \xi$.
☞ Of course, if G is Kazhdan then for any closed subgroup $H \leq G$, the pair (G, H) has relative property (T).

2.2 Property (T) for $SL_n(\mathbb{Z})$ $(n \geq 3)$

In this section we will follow Shalom's proof of property (T) for $SL_n(\mathbb{Z})$ $(n \geq 3)$ (cf. [Sha99]), using bounded elementary generation. We will also give a Kazhdan constant for these groups, which we will use to estimate the "robustness" of the family of expanders shown in section 2.3.

2.2.1 Bounded Elementary Generation of $SL_n(\mathbb{Z})$

Definition 2.2.1 (Elementary Matrices and Operations) *Let $\mathbb{A}$ be a commutative ring with unit.*

(i) We define the elementary matrix $E_{i,j}(t) \in \mathcal{M}_n(\mathbb{A})$, where $i, j \in [n]$ and $t \in \mathbb{A}$, as the matrix whose diagonal coefficients are ones, whose (i,j)–th coefficient is t and whose other coefficients are zero.

(ii) We call elementary operation on a matrix $M \in \mathcal{M}_n(\mathbb{A})$ any left (resp. right) multiplication of M by an elementary matrix $E_{i,j}(t)$. Such an operation adds t times the j–th row (resp. the i–th column) to the i–th one (resp. the j–th one).

Remark : Observe that if any number of elementary operations transforms a matrix A into a matrix B, then the same number of elementary operations will transform ${}^tA$ into ${}^tB$ and A^{-1} into B^{-1}.

Definition 2.2.2 (Bounded Elementary Generation)
We say that $SL_n(\mathbb{A})$ has bounded elementary generation if there exists $\nu \in \mathbb{N}^*$ such that every matrix in $SL_n(\mathbb{A})$ can be written as a product of at most ν elementary matrices.

Remark : When $SL_n(\mathbb{A})$ has bounded elementary generation, we denote the minimal such integer ν by $\nu_n(\mathbb{A})$.

Example : Let $\mathbb{K}$ be a field. Then, by applying Gauss's elimination, we show that $SL_n(\mathbb{K})$ has bounded elementary generation and that $\nu_n(\mathbb{K}) \leq n(n-1)$.

We now wish to prove that $SL_n(\mathbb{Z})$ has bounded elementary generation. To achieve this, we will need a few (quite) technical lemmas[2.3].

Lemma 2.2.1
Let $n \geq 3$.
Let $A \in SL_n(\mathbb{Z})$.
Then A can be transformed, using at most $\frac{1}{2}(3n^2 - n - 10)$ elementary operations, into a matrix of the following form $(a, b, c, d \in \mathbb{Z})$:

$$\begin{pmatrix} a & b & & & \\ c & d & & (0) & \\ & & 1 & & \\ & (0) & & \ddots & \\ & & & & 1 \end{pmatrix}$$

PROOF : Denote by $u_1, \ldots, u_n$ the coefficients of A's n–th row. Since $A \in SL_n(\mathbb{Z})$, $\gcd(u_1, \ldots,_n) = 1$ (indeed, $\det(A) = 1$ is a polynomial in the coefficients of A). We aim to prove that using at most one elementary operation we can transform A into a matrix $B \in SL_n(\mathbb{Z})$ whose n–th row's coefficients $v_1 \ldots v_n$ satisfy $\gcd(v_1, \ldots, v_{n-1}) = 1$.

First, if $u_1, \ldots, u_{n-1} = 0$ then $u_n \in \{-1, 1\}$ and simply adding the last column to the first yields the desired result. Now assume that there exists $i \in [n-1]$ such that $u_i \neq 0$: by the Chinese remainder theorem, there exists $t \in \mathbb{Z}$ so that $t \equiv 1$ modulo all primes dividing $\gcd(u_1, \ldots, u_{n-1})$ and $t \equiv 0$ modulo all primes dividing $\gcd(u_2, \ldots, u_{n-1})$ but not u_1. Let now p be a prime divisor of $\gcd(u_2, \ldots, u_{n-1})$.

[2.3] We beg the reader for forgiveness.

- If $p|u_1$ then $t \equiv 1[p]$ and $u_1 + tu_n \equiv u_n[p]$. Moreover, $\gcd(u_1, \ldots, u_n) = 1$ thus $p \nmid u_1 + tu_n$.

- If $p \nmid u_1$ the $t \equiv 0[p]$ therefore $u_1 + tu_n \equiv u_1[p]$. In fine, $p \nmid u_1 + tu_n$.

We deduce that $\gcd(u_1 + tu_n, u_2, \ldots, u_{n-1}) = 1$. All we now have to do is to add t times the n–th column of A to its first one, obtaining B (with $v_1 := u_1 + tu_n, v_2 := u_2, \ldots, v_n := u_n$).

As $gcd(v_1, \ldots, v_{n-1}) = 1$, there exist $t_1, \ldots, t_n \in \mathbb{Z}$ such that :

$$1 - v_n = \sum_{i=1}^{n-1} t_i v_i$$

This gives us a way, using $n-1$ elementary operations, to transform B into a matrix of the following form :

$$C := \begin{pmatrix} & & & & \\ & & (*) & & \\ & & & & \\ v_1 & \ldots & \ldots & v_{n-1} & 1 \end{pmatrix}$$

It is now quite simple, using less than $n-1$ elementary operations, to transform C into a matrix of the following form :

$$\begin{pmatrix} & & & & \\ & & (*) & & \\ & & & & \\ 0 & \ldots & \ldots & 0 & 1 \end{pmatrix}$$

By repeating this process as many times as required (i.e $n-2$), we are now able to transform A into a matrix of the desired form, using at most $1 + 3(n-k)$ elementary operations at any given step k. In fine, remark that :

$$\sum_{k=1}^{n-2} 1 + 3(n-k) = \frac{1}{2}(3n^2 - n - 10)$$

Hence the desired upper bound.

Lemma 2.2.2
Let $s \in \mathbb{N}$.
Let :

$$A := \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; B := \begin{pmatrix} a^s & b & 0 \\ x & y & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(\mathbb{Z})$$

Then one can transform A^s into B using at most 16 elementary operations.

Proof : Consider the matrix $L := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Then, by the Cayley – Hamilton theorem, there exist $f, g \in \mathbb{Z}$ such that $L^s = fI_2 + gL$. Moreover, $\det(L) = 1$ thus $\det(fI_2 + gL) = \det(L)^s = 1$. Furthermore, notice that :

$$\begin{aligned} 1 = \det(fI_2 + gL) &\equiv \det(gL)[f] \\ &\equiv g^2 \det(L)[f] \\ &\equiv g^2[f] \end{aligned}$$

Thus $f|g^2 - 1 = (g-1)(g+1)$ and so if we set $f^+ := \gcd(f, g+1)$, there exist $f^-, g_1, g_2 \in \mathbb{Z}$ such that $f = f^+f^-$, $g+1 = f^+g_1$ and $g-1 = f^-g_2$. Now define the following matrices :

$$G := E_{2,3}(f^-)E_{3,2}(g_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & g & f^- \\ 0 & g_2 & 1 \end{pmatrix}$$

$$H := E_{3,1}(-1)E_{1,3}(1-f^+)E_{2,1}(-f^-)E_{3,1}(g_1) = \begin{pmatrix} * & 0 & * \\ -f^- & 1 & 0 \\ g & 0 & f^+ \end{pmatrix}$$

$$J := GH = \begin{pmatrix} h & 0 & * \\ 0 & g & f \\ 1 & * & * \end{pmatrix}, \text{ for some } h \in \mathbb{Z}$$

We now submit the matrix J to the following sequence of elementary operations (r, t, v and w denoting four integers whose exact value is of no use to us) :

$$J \leftarrow E_{1,3}(1-h)J \qquad \begin{pmatrix} 1 & r & * \\ 0 & g & f \\ 1 & * & * \end{pmatrix}$$

$$J \leftarrow JE_{1,2}(-r) \qquad \begin{pmatrix} 1 & 0 & t \\ 0 & g & f \\ 1 & * & * \end{pmatrix}$$

$$J \leftarrow JE_{1,3}(-t-h) \qquad \begin{pmatrix} 1 & 0 & -h \\ 0 & g & f \\ 1 & * & * \end{pmatrix}$$

$$J \leftarrow JE_{2,3}(a) \qquad \begin{pmatrix} 1 & 0 & -h \\ 0 & g & f+ga \\ 1 & v & w \end{pmatrix}$$

Note that this shows that the matrix $S := \begin{pmatrix} 1 & 0 & -h \\ 0 & g & f+ga \\ 1 & v & w \end{pmatrix}$ is a product of 10 elementary matrices. Furthermore, since $L^s = fI_2 + gL$ there exist $x_0, y_0 \in \mathbb{Z}$ such that :

$$A^s = \begin{pmatrix} f+ga & bg & 0 \\ x_0 & y_0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

And, as $A \mod b$ is triangular :

$$A^s \equiv \begin{pmatrix} a^s & 0 & 0 \\ * & d^s & 0 \\ 0 & 0 & 1 \end{pmatrix} [b]$$

Therefore, there exists $u \in \mathbb{Z}$ such that $f + ag = a^s + bu$ and so ($x, y \in \mathbb{Z}$) :

$$B = \begin{pmatrix} f+ag-bu & b & 0 \\ x & y & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We now submit the matrix B to a treatment comparable with the one J received (also featuring four not so interesting integers u_1, v_1, x_1 and y_1) :

$$B \leftarrow BE_{2,1}(u)S \qquad \begin{pmatrix} f+ag & bg & 0 \\ x+uy & yg & 1 \\ 1 & v & w \end{pmatrix}$$

$$B \leftarrow E_{3,2}(1-w)B \qquad \begin{pmatrix} f+ag & bg & 0 \\ x+uy & yg & 1 \\ u_1 & v_1 & 1 \end{pmatrix}$$

$$B \leftarrow E_{2,3}(-1)B \qquad \begin{pmatrix} f+ag & bg & 0 \\ x+uy-u_1 & yg-v_1 & 0 \\ u_1 & v_1 & 1 \end{pmatrix}$$

$$B \leftarrow BE_{3,1}(-u_1)E_{3,2}(-v_1) \qquad \begin{pmatrix} f+ag & bg & 0 \\ x_1 & y_1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Since $1 = \det(A^s) = \det(B)$ we have $(f+ag)y_0 - bgx_0 = (f+ag)y_1 - bgx_1$, which yields :

$$0 = (f+ag)(y_0 - y_1) = bg(x_0 - x_1)$$

As $\gcd(f+ag, bg) = 1$, there exists $q \in \mathbb{Z}$ such that $y_0 = y_1 + qbg$ and $x_0 = x_1 + q(f+ag)$. Thus :

$$E_{2,1}(q) \begin{pmatrix} f+ag & bg & 0 \\ x_1 & y_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} f+ag & bg & 0 \\ x_0 & y_0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = A^s$$

We have proved that one can transform B into A^s using at most 16 elementary operations, and so the converse can be done with the exact same amount of operations, as claimed.

In order to prove the next lemma, we will need to use the following classical number theory result :

Theorem 2.2.1 (Dirichlet's Prime Number Theorem)
Let $a, b \in \mathbb{N}^*$ be two relatively prime integers.
Then there are infinitely many primes $p \in \mathbb{N}^*$ such that $p \equiv a[b]$.

Lemma 2.2.3
Let $A := \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(\mathbb{Z})$, with $b \equiv 3[4]$.
Then A can be written as a product of at most 40 elementary matrices.

PROOF : First note that if either c or d is zero then a or b must be ± 1 and our claim becomes obvious. Else, remark that $\gcd(4d, b) = 1$ therefore by Dirichlet's theorem (2.2.1) there exists a positive prime number p such that $p \equiv b[4d]$. Using one elementary operation, one can thus transform A into a matrix of the form ($u \in \mathbb{Z}$) :

$$A' := \begin{pmatrix} u & p & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Observe that $p \equiv 3[4]$ and that since $p \neq \pm 1$ then $u \neq 0$. The Chinese remainder theorem then gives us an integer $t \in \mathbb{Z}$ such that $t \equiv c[u]$ and $t \equiv -1[r]$ for every prime r such that $r | p-1$ and $r \nmid u$.

Let s be a prime number dividing both $p-1$ and u. Then :

$$\begin{aligned} 1 = \det \begin{pmatrix} u & p & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} &= ud - pc \\ &\equiv -c[s] \\ &\equiv -t[s] \end{aligned}$$

Thus we have $t \equiv -1[r]$ for any prime number p dividing $p-1$. In particular, $p-1$ and t are relatively prime and since $\frac{p-1}{2}$ is odd, so do $\frac{p-1}{2}$ and $t-1$. Therefore, by Dirichlet's prime number theorem, there exists a positive prime s such that $q \equiv t[p-1]$ and, as $\frac{p-1}{2}$ and $t-1$ are relatively prime, $\gcd(\frac{p-1}{2}, q-1)$ is also one. This implies that there are two integers $m, m' \in \mathbb{Z}$ such that $t = mu + c$ and $q = (p-1)t + m'$. Thus $q = ((p-1)m + m')u + c$ hence one can transform, using one elementary operation, the matrix A into a matrix of the form ($v \in \mathbb{Z}$) :

$$H := \begin{pmatrix} u & p & 0 \\ q & v & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Since $\frac{p-1}{2}$ and $q-1$ are relatively prime, there exist $k, \ell \in \mathbb{Z}$ such that $k\frac{p-1}{2} + \ell(q-1) = 1$ and so by Fermat's theorem $v^{q-1} \equiv 1[q]$ and there is an integer $\alpha \in \mathbb{Z}$ such that $v^{(q-1)\ell} = 1 + \alpha q$. Now consider :

$$B := E_{1,2}(-q)E_{2,1}(-\alpha) = \begin{pmatrix} v^{(q-1)\ell} & -q & 0 \\ -\alpha & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

By lemma 2.2.2, we can transform B into the following matrix using less than 16 elementary operations :

$$\begin{pmatrix} v & -q & 0 \\ -p & u & 0 \\ 0 & 0 & 1 \end{pmatrix} = {}^t(H^{(q-1)\ell})^{-1}$$

Thus ${}^t(H^{(q-1)\ell})^{-1}$ can be written as a product of at most 18 elementary matrices. Then, by Fermat's theorem, $u^{p-1} \equiv 1[p]$ and so $u^{k\frac{p-1}{2}} \equiv \pm 1[p]$.

- If $u^{k\frac{p-1}{2}} \equiv 1[p]$, then there exists $r \in \mathbb{Z}$ such that $u^{k\frac{p-1}{2}} = 1 + rp$. Let :

$$V := E_{1,2}(p)E_{2,3}(r) = \begin{pmatrix} u^{k\frac{p-1}{2}} & p & 0 \\ r & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  Then by lemma 2.2.2 one can transform V into $H^{k\frac{p-1}{2}}$ using less than 16 elementary operations, thus $H^{k\frac{p-1}{2}}$ can be written as a product of less than 18 elementary matrices. Note then that :

$$H = H^{k\frac{p-1}{2} - \ell(q-1)} = H^{k\frac{p-1}{2}} H^{-\ell(q-1)}$$

  Hence H can written as a product of less than $18 + 18 = 36$ elementary matrices, therefore A can be written as a product of less than 38 elementary matrices.

- If $u^{k\frac{p-1}{2}} \equiv -1[p]$, then there exists $r \in \mathbb{Z}$ such that $u^{k\frac{p-1}{2}} = -1 + rp$. Let :

$$W := E_{1,2}(2)E_{2,1}(-1)E_{2,1}(2-p)E_{2,1}(r) = \begin{pmatrix} u^{k\frac{p-1}{2}} & p & 0 \\ pr - r - 1 & p-1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  Then by lemma 2.2.2 one can transform W into $H^{k\frac{p-1}{2}}$ using less than 16 elementary operations, thus $H^{k\frac{p-1}{2}}$ can be written as a product of less than 20 elementary matrices. As before, we conclude that A can be written as a product of less than 40 elementary matrices, which concludes the proof.

We are now in position to show that $SL_n(\mathbb{Z})$ indeed has bounded generation by putting together the previous lemmas.

Proposition 2.2.2
Let $n \geq 3$.
Then $SL_n(\mathbb{Z})$ is has bounded elementary generation. Moreover :

$$\nu_n(\mathbb{Z}) \leq \frac{1}{2}(3n^2 - n) + 36$$

Proof : Let $A \in SL_n(\mathbb{Z})$. By lemma 2.2.1, A can be transformed using less than $\frac{1}{2}(3n^2 - n - 10)$ elementary operations into a matrix B of the form :

$$B := \begin{pmatrix} a & b & & & \\ c & d & & (0) & \\ & & 1 & & \\ & (0) & & \ddots & \\ & & & & 1 \end{pmatrix}$$

Using one further operations if necessary, we can assume that b is odd and so either $b \equiv 3[4]$ or $-b \equiv 3[4]$. Thus, by lemma 2.2.3, either B or B^{-1} (and so B) can be written as a product of less than 40 elementary matrices. Hence A can be written as a product of less than $\frac{1}{2}(3n^2 - n - 10) + 1 + 40 = \frac{1}{2}(3n^2 - n) + 36$ elementary matrices, as claimed.

2.2.2 Relative Property (T) for $(SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2, \mathbb{Z}^2)$

We continue our advance towards showing that $SL_n(\mathbb{Z})$ is Kazhdan for $n \geq 3$ by studying the pair $(SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2, \mathbb{Z})$. But first, let us recall a few basic things about semidirect products.

Definition 2.2.3 (Semidirect Product)
Let A and B be two groups.
Let $\phi : A \to \mathrm{Aut}(B)$ be a group homomorphism.
We call semidirect product (in regard to ϕ) of A and B the group $A \,_\phi\!\ltimes B$ which is defined as being $A \times B$ endowed with the following operation :

$$\forall (a_1, b_1), (a_2, b_2) \in A \times B,\ (a_1, b_1).(a_2, b_2) := (a_1 a_2, \phi(a_2)(b_1) b_2)$$

Now remark that the following mapping is indeed a group homomorphism :

$$\begin{aligned} \phi : SL_2(\mathbb{Z}) &\to \mathrm{Aut}(\mathbb{Z}^2) \\ M &\mapsto (x \mapsto Mx) \end{aligned}$$

Hence we can consider the semidirect product $SL_2(\mathbb{Z}) \,_\phi\!\ltimes \mathbb{Z}^2$, which we will simply denote by $SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$. We will also identify $SL_2(\mathbb{Z})$ and $\mathbb{Z}^2$ to the corresponding subgroups of the aforementioned semidirect product. We now define four sample matrices of $SL_2(\mathbb{Z})$ as follows :

$$U^- := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},\ U^+ := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ L^- := \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},\ L^+ := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Let us now prove the following lemma :

Lemma 2.2.4 (Burger)
Let ν be a probability measure on the Borel sets of $\Omega := \mathbb{R}^2 \setminus \{0\}$.
Then there exist $M \in \mathcal{B}(\Omega)$ and $\gamma \in \{U^-, U^+, L^+, L^-\}$ such that :

$$|\nu(\gamma M) - \nu(M)| \geq \frac{1}{4}$$

Where $\gamma M := \{\gamma x \,|\, x \in M\}$ as per the usual action of $SL_2(\mathbb{Z})$ on $\mathbb{R}^2$.

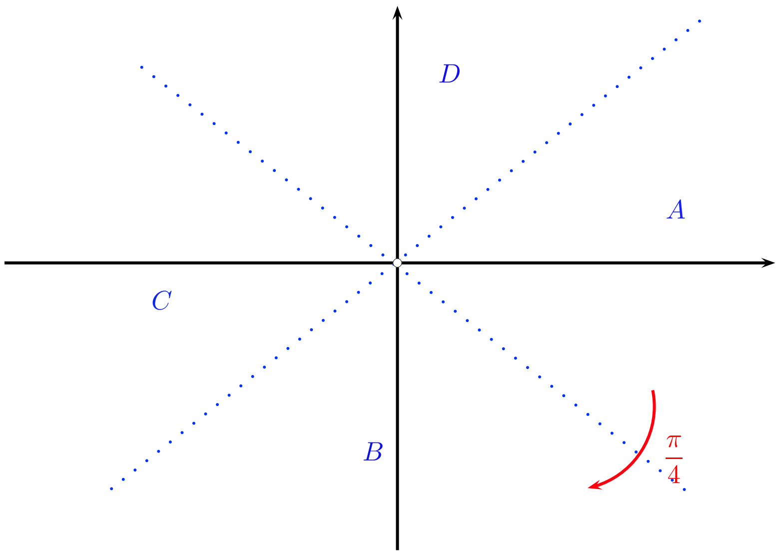

Figure 2.1: A partition of Ω.

PROOF : Set :

$$A := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \Omega \,|\, 0 \leq y < x \text{ or } x < y \leq 0 \right\}$$

By considering A and its images B, C and D by the counterclockwise rotations of angle $\frac{\pi}{4}, \frac{\pi}{2}$ and $\frac{3\pi}{4}$ we obtain a partition of Ω delimited by the lines "$x = y$" and "$x = -y$", as seen on figure 2.1. Plainly, the following equalities then hold :

$$U^+(A \cup B) = A,\ U^-(C \cup D) = D,\ L^+(A \cup B) = B,\ L^-(C \cup D) = C$$

Now suppose that $\forall M \in \mathcal{B}(\Omega)$, $\forall \gamma \in \{U^-, U^+, L^+, L^-\}$, $|\nu(\gamma M) - \nu(M)| < \frac{1}{4}$. Then if we take $M = A \cup B$, we obtain :

$$\begin{aligned} \nu(a) &= \nu(A \cup B) - \nu(B) \\ &= \nu(A \cup B) - \nu(L^+(A \cup B)) \\ &< \frac{1}{4} \end{aligned}$$

Using similar calculations, we show that $\nu(B), \nu(C)$ and $\nu(D)$ are also less that $\frac{1}{4}$. Hence :

$$1 = \nu(\Omega) = \nu(A) + \nu(B) + \nu(C) + \nu(D) < 1$$

The above inequality being blatantly incorrect, our lemma isn't[2.4].

Identify the character group $\widehat{\mathbb{Z}^2}$ to the torus $\mathbb{T}^2$ via the following bijective mapping :

$$\begin{aligned} \mathbb{T}^2 &\mapsto \widehat{\mathbb{Z}^2} \\ (z, w) &\mapsto ((m, n) \mapsto z^m w^n) \end{aligned}$$

We define the dual action of $SL_2(\mathbb{Z})$ on $\widehat{\mathbb{Z}^2}$ as the inverse transpose of the usual action of $SL_2(\mathbb{Z})$ on $\mathbb{Z}^2$, i.e $(M, x) \mapsto {}^tM^{-1}x$. Let us also set :

$$e^+ := \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ e^- := \begin{pmatrix} -1 \\ 0 \end{pmatrix},\ f^+ := \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ f^- := \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

Note that $Q := \{U^+, U^-, L^+, L^-, e^+, e^-, f^+, f^-\}$ is a generating set of $SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$. We are now finally able to prove the main result of this subsection, namely that the pair $(SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2, \mathbb{Z}^2)$ has relative property (T).

[2.4] And so is, in fact, correct !

Proposition 2.2.3
The pair $(SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2, \mathbb{Z}^2)$ has relative property (T). Indeed, $\left(Q, \frac{1}{10}\right)$ is a Kazhdan pair for $(SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2, \mathbb{Z}^2)$.

Proof : Let $(\pi, \mathcal{H})$ be a unitary representation of $SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ with a $\left(Q, \frac{1}{10}\right)$–invariant vector but without any $\mathbb{Z}^2$–invariant nontrivial vector. Let $E : \mathcal{B}(\mathbb{T}^2) \to L(\mathcal{H})$ be the projection valued measure on $\widehat{\mathbb{Z}^2}$ associated to the restriction $\pi_{|_{\mathbb{Z}^2}}$ by mean of the SNAG theorem (cf. theorem A.2.4), so that :

$$\forall z \in \mathbb{Z}^2,\ \forall \xi, \eta \in \mathcal{H},\ \langle \pi(z)\xi, \eta\rangle = \int_{\mathbb{T}^2} \chi(z) d\langle E(\chi)\xi, \eta\rangle$$

Also note that :

$$\forall \gamma \in SL_2(\mathbb{Z}),\ \forall B \in \mathcal{B}(\mathbb{T}^2),\ E(\gamma B) = \pi(\gamma^{-1})E(B)\pi(\gamma) \tag{2.2}$$

Set $\varepsilon := \frac{1}{10}$ and let $\xi \in \mathcal{H}$ be a (Q, ε)–invariant unit vector. Consider the following probability measure on $\mathbb{T}^2$:

$$\begin{aligned} \mu_\xi : \mathcal{B}(\mathbb{T}^2) &\to [0,1] \\ B &\mapsto \langle E(B)\xi, \xi\rangle \end{aligned}$$

We now identify $\widehat{\mathbb{Z}^2}$ with $\left(-\frac{1}{2}, \frac{1}{2}\right]^2$ using $(x, y) \mapsto \chi_{x,y} : (m, n) \mapsto e^{2i\pi(xm+yn)}$ and note that as $\pi_{|_{\mathbb{Z}^2}}$ as no nontrivial invariant vector then $E(\{0\}) = 0$ and thus $\mu_\xi(\{0\}) = 0$.

Let $X := \left(-\frac{1}{4}, \frac{1}{4}\right]^2$: since ξ is (Q, ε)–invariant and $e^+, e^-, f^+, f^- \in Q$ then we have :

$$\|\pi(e^\pm)\xi - \xi\|^2 = \int_{(-\frac{1}{2},\frac{1}{2}]^2} \left|e^{\pm 2i\pi x} - 1\right| d\mu_\xi(x, y) \leq \varepsilon^2$$
$$\|\pi(f^\pm)\xi - \xi\|^2 = \int_{(-\frac{1}{2},\frac{1}{2}]^2} \left|e^{\pm 2i\pi y} - 1\right| d\mu_\xi(x, y) \leq \varepsilon^2$$

Now remark that if $|t| \in \left[\frac{1}{4}, \frac{1}{2}\right]$ then :

$$|e^{\pm 2i\pi t} - 1|^2 = 2 - 2\cos(2\pi t) = 4\sin^2(\pi t) \geq 2$$

Hence :

$$\begin{aligned} \varepsilon^2 &\geq \int_{\substack{(x,y)\in(-\frac{1}{2},\frac{1}{2}]^2 \\ |x|\geq\frac{1}{4}}} 4\sin^2(\pi x) \\ &\geq 2\mu_\xi\left(\left\{(x, y) \in \left(-\frac{1}{2}, \frac{1}{2}\right]^2 \mid |x| \geq \frac{1}{4}\right\}\right) \end{aligned}$$

Thus :

$$\mu_\xi\left(\left\{(x, y) \in \left(-\frac{1}{2}, \frac{1}{2}\right]^2 \mid |x| \geq \frac{1}{4}\right\}\right) \leq \frac{\varepsilon^2}{2}$$

Using similar calculations, we show that :

$$\mu_\xi\left(\left\{(x, y) \in \left(-\frac{1}{2}, \frac{1}{2}\right]^2 \mid |y| \geq \frac{1}{4}\right\}\right) \leq \frac{\varepsilon^2}{2}$$

Hence :

$$\mu_\xi(X) \geq 1 - \varepsilon^2$$

Consider the following probability measure :

$$\begin{aligned} \nu : \mathcal{B}(\mathbb{T}^2) &\to [0,1] \\ B &\mapsto \frac{\mu_\xi(B \cap X)}{\mu_\xi(X)} \end{aligned}$$

Using equation (2.2), we have that (for $\gamma \in SL_2(\mathbb{Z})$ and $B \in \mathcal{B}(\mathbb{T}^2)$) :

$$\begin{aligned}
|\mu_\xi(\gamma B) - \mu_\xi(B)| &= |\langle \pi(\gamma^{-1}E(B)\pi(\gamma)\xi, \xi\rangle) - \langle E(B)\xi, \xi\rangle| \\
&\leq |\langle \pi(\gamma^{-1}E(B))\pi(\gamma)\xi, \xi\rangle - \langle \pi(\gamma^{-1}E(B)\xi, \xi\rangle| + |\langle \pi(\gamma^{-1}E(B))\xi, \xi\rangle - \langle E(B)\xi, \xi\rangle| \\
&= |\langle \pi(\gamma^{-1}E(B))(\pi(\gamma)\xi - \xi), \xi\rangle| + |\langle E(B)\xi, (\pi(\gamma)\xi - \xi)\rangle| \\
&\leq \|\pi(\gamma^{-1}E(B))(\pi(\gamma)\xi - \xi)\|\|\xi\| + \|E(B)\xi\|\|\pi(\gamma)\xi - \xi\| \text{ by Cauchy–Schwarz} \\
&\leq \|\pi(\gamma^{-1}E(B))\|\pi(\gamma)\xi - \xi\| + \|E(B)\|\|\pi(\gamma)\xi - \xi\| \\
&\leq 2\varepsilon
\end{aligned}$$

We also know that $0 \leq \mu_\xi(B) - \mu_\xi(B \cap X) \leq \varepsilon^2$ hence :

$$\begin{aligned}
\mu_\xi(\gamma B \cap X) - \mu_\xi(B \cap X) &= \mu_\xi(\gamma B \cap X) - \mu_\xi(\gamma B) + \mu_\xi(\gamma B) - \mu_\xi(B) + \mu_\xi(B) - \mu_\xi(B \cap X) \\
&\leq 0 + 2\varepsilon + \varepsilon^2
\end{aligned}$$

This inequality also holds for $\gamma^{-1}B$, thus :

$$|\mu_\xi(\gamma B \cap X) - \mu_\xi(B \cap X)| \leq 2\varepsilon + \varepsilon^2$$

So :

$$|\nu(\gamma B) - \nu(B)| \leq \frac{2\varepsilon + \varepsilon^2}{1 - \varepsilon^2} = \frac{21}{99} < \frac{1}{4}$$

Moreover, since $\mu_\xi(\{0\}) = 0$, we can see ν as a measure on Ω. Also remark that $\forall \gamma \in \{U^+, U^-, L^+, L^-\}$, $\gamma X \subset \left(-\frac{1}{2}, \frac{1}{2}\right)^2$ and since $\nu(X^c) = 0$ then $\forall B \in \mathcal{B}(\Omega)$, $|\nu(\gamma B) - \nu(B)| < \frac{1}{4}$, which contradicts lemma 2.2.4 and so concludes the proof.

Corollary 2.2.3.1
Let $\varepsilon > 0$.
Let $(\pi, \mathcal{H})$ be a unitary representation of $SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$.
Assume that π has a $\left(Q, \frac{\varepsilon}{20}\right)$–invariant unit vector ξ.
Then ξ is $(\mathbb{Z}^2, \varepsilon)$–invariant.

Proof : Let $\mathcal{H}_0 := \{x \in \mathcal{H} \,|\, \forall z \in \mathbb{Z}^2, \pi(z)x = x\}$ and $H_1 := \mathcal{H}_0^\perp$. Since $\mathbb{Z}^2 \lhd SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ then $\mathcal{H}_0$ and $\mathcal{H}_1$ are invariant under $SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$. Furthermore, since $\mathcal{H}_0$ is closed, $\mathcal{H} := \mathcal{H}_0 \oplus \mathcal{H}_1$ thus $\exists!(\xi_0, \xi_1) \in \mathcal{H}_0 \times \mathcal{H}_1$, $\xi = \xi_0 + \xi_1$. Now consider $\gamma \in SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ and observe that, by Pythagore's theorem :

$$\|\pi(\gamma)\xi - \xi\|^2 = \underbrace{\|\pi(\gamma)\xi_0 - \xi_0\|^2}_{=0} + \|\pi(\gamma)\xi_1 - \xi_1\|^2$$

Thus :

$$\|\pi(\gamma)\xi_1 - \xi_1\|^2 = \|\pi(\gamma)\xi - \xi\|^2 < \left(\frac{\varepsilon}{20}\right)^2$$

As there is no nontrivial $\mathbb{Z}^2$–invariant vectors in $\mathcal{H}$, then by proposition 2.2.3 :

$$\exists \lambda \in Q, \ \|\pi(\gamma)\xi_1 - \xi_1\|^2 \geq \left(\frac{\|\xi_1\|}{10}\right)^2$$

In fine :

$$\left(\frac{\|\xi_1\|}{10}\right)^2 < \left(\frac{\varepsilon}{20}\right)^2 \text{ i.e } \|\xi_1\| < \frac{\varepsilon}{2}$$

And so :

$$\forall t \in \mathbb{Z}^2, \ \|\pi(t)\xi - \xi\| = \|\pi(t)\xi_1 - \xi_1\| \leq 2\|\xi_1\| < \varepsilon$$

Therefore ξ is $(\mathbb{Z}^2, \varepsilon)$–invariant.

2.2.3 Finding an Explicit Kazhdan Constant for $SL_n(\mathbb{Z})$

Finally, we take the last steps towards our main result, namely that $SL_n(\mathbb{Z})$ has property (T) for $n \geq 3$. For the remainder of this subsection, we set an integer $n \geq 3$.

Lemma 2.2.5
Let $i, j \in [n]$ such that $i \neq j$.
Then there exists an injective homomorphism $\alpha : SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2 \to SL_n(\mathbb{Z})$ such that :

(i) $\forall t \in \mathbb{Z}$, $E_{i,j}(t) \in \alpha(\mathbb{Z}^2)$;

(ii) there exists $0 \leq k \leq n-2$ *such that :*

$$\forall M \in SL_2(\mathbb{Z}),\ \exists N \in SL_2(\mathbb{Z})\ \alpha(M) = \begin{pmatrix} I_k & & (0) \\ & N & \\ (0) & & I_{n-2-k} \end{pmatrix}$$

Proof : This lemma is proven by induction on $n \geq 3$ (an overview of the steps involved can be found in [BdlHV08]).

We now show that $SL_n(\mathbb{Z})$ has property (T) for $n \geq 3$ and compute an explicit Kazhdan constant for this group, using its bounded elementary generation.

Proposition 2.2.4
$SL_n(\mathbb{Z})$ has property (T) (recall that $n \geq 3$).
Indeed, if we set $Q_n := \{E_{i,j}(1) \,|\, i, j \in [n],\, i \neq j\}$ and $\nu_n := \nu_n(\mathbb{Z})$ then $\left(Q_n, \dfrac{1}{20\nu_n}\right)$ is a Kazhdan pair for $SL_n(\mathbb{Z})$.

Proof : Let $T_n := Q_n \cup Q_n^{-1}$ and recall that it suffices to show that $\left(T_n, \dfrac{1}{20\nu_n}\right)$ is a Kazhdan pair for $SL_n(\mathbb{Z})$. Let $(\pi, \mathcal{H})$ be a unitary representation of $SL_n(\mathbb{Z})$ with a $\left(T_n, \dfrac{1}{20\nu_n}\right)$–invariant unit vector ξ and let γ be any elementary matrix in $SL_n(\mathbb{Z})$. Then, by lemma 2.2.5, there exists $\alpha : SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2 \hookrightarrow SL_n(\mathbb{Z})$ such that $\gamma \in \alpha(\mathbb{Z}^2)$ and $\alpha(Q) = T_n \cap \alpha(SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2)$. By corollary 2.2.3.1, ξ is $\left(\alpha(\mathbb{Z}^2), \dfrac{1}{\nu_n}\right)$–invariant and so in particular :

$$\|\pi(\gamma)\xi - \xi\| < \frac{1}{\nu_n}$$

Assume now that γ is any matrix in $SL_n(\mathbb{Z})$. Then, as $SL_n(\mathbb{Z})$ has bounded elementary generation, there exists an integer $N \leq \nu_n$ and finitely many elementary matrices $\gamma_1, \ldots, \gamma_N \in SL_n(\mathbb{Z})$ so that :

$$\gamma = \prod_{i=1}^{N} \gamma_i$$

Therefore :

$$\begin{aligned} \|\pi(\gamma)\xi - \xi\| &\leq \sum_{i=0}^{N-1} \left\| \pi\left(\prod_{j=1}^{N-i} \gamma_j\right)\xi - \pi\left(\prod_{j=1}^{N-i-1} \gamma_j\right)\xi \right\| \\ &= \sum_{j=1}^{N} \|\pi(\gamma_j)\xi - \xi\| \\ &\leq \frac{N}{\nu_n} \\ &\leq 1 \\ &< \sqrt{2} \end{aligned}$$

Hence ξ is $(SL_n(\mathbb{Z}), \sqrt{2})$–invariant and so by proposition 2.1.1, π has nontrivial invariant vectors, and so the proposition is proven.

2.3 Main Theorem and Construction

In this last section, we finally construct an actual family of expanders, using property (T) on $SL_n(\mathbb{Z})$ $(n \geq 3)$. We first prove a (relatively) generic theorem linking some quotients of Kazhdan groups and expander families before applying it to the aforementioned special linear groups and thus obtaining an explicit family of expanders.

Theorem 2.3.1
Let Γ be a finitely generated Kazhdan group.
Let $\mathcal{L}$ be a family of finite index normal subgroups of Γ.
Let S be a finite symmetric generating set of Γ.
Then $(\mathcal{C}(\Gamma/N, S))_{N\in\mathcal{L}}$ is a family of $(|\Gamma/N|, |S|, c)$–expanders, for some $c > 0$.

PROOF : Let $N \in \mathcal{L}$. We consider the finite group $V := \Gamma/N$ and the separable Hilbert space $H := L^2(\Gamma/N)$ of the functions $f : \Gamma/N \to \mathbb{C}$ endowed with the following norm :

$$\|.\| : f \mapsto \sqrt{\sum_{x\in V} |f(x)|^2}$$

Let $H_0 := \{f \in H \mid \sum_{x\in V} f(x) = 0\}$. Then Γ acts on H as follows :

$$\forall\gamma \in \Gamma,\ \gamma.f = (x \mapsto f(x\gamma))$$

This action can be seen as a representation $\rho : \Gamma \to \mathcal{U}(H)$, where $\forall\gamma \in \Gamma, \forall f \in H$ we define $\rho(\gamma)f := \gamma.f$. Furthermore, as a Γ–module, $H = H_0 \oplus H_0^{\perp}$. Here, $H_0^{\perp} = \mathbb{C}\chi_V$, where $\chi_V : x \mapsto 1 \in H$ is the characteristic function of V.

The action of Γ on V is transitive, hence the only Γ–invariant functions of H are the constants (i.e the elements of $\mathbb{C}\chi_V$) (in particular, since ρ_0 is indeed Γ–invariant, $\rho_0 \notin H_0$). This transitivity also means that we can consider the representation (H_0, ρ). Since only the constants in H are Γ–invariant, H_0 doesn't contain any such function, i.e the representation (H_0, ρ) doesn't have any nontrivial invariant vector. Thus, since Γ is Kazhdan, this representation doesn't have any almost invariant vector, i.e there exists $\varepsilon > 0$ not dependent on N such that (cf. lemma 2.1.1) :

$$\forall f \in H_0,\ \exists\gamma \in S,\ \|\gamma.f - f\| > \varepsilon\|f\| \tag{2.3}$$

Let $A \subset V$ and let $B = A^c$. We denote $a := |A|$ and $b := |B| = n - a$. We then define the following mapping on V :

$$f : x \mapsto \begin{cases} b & \text{if } x \in A \\ -a & \text{if } x \in B \end{cases}$$

Plainly $f \in H_0$ and $\|f\|^2 = ab^2 + ba^2 = nab$, while (for any $\gamma \in \Gamma$) :

$$\begin{aligned} \|\gamma.f - f\|^2 &= \sum_{x\in V} |f(x\gamma) - f(x)|^2 \\ &= \sum_{x\in A} |f(x\gamma) - b|^2 + \sum_{x\in B} |f(x\gamma) + a|^2 \end{aligned}$$

Therefore, if we consider $E_\gamma(A, B) := \{x \in V \mid x \in A,\ x\gamma \in B \text{ or } x \in B,\ x\gamma \in A\}$ then :

$$\|\gamma.f - f\|^2 = (a + b)^2|E_\gamma(A, B)| = n^2|E_\gamma(A, B)|$$

Since $|E(A, B)| \geq \frac{1}{2}|E_\gamma(A, B)|$, then :

$$|\partial A| \geq \frac{1}{2}|E_\gamma(A, B)| = \frac{\|\gamma.f - f\|^2}{2n^2}$$

Thus (using equation 2.3):

$$\begin{aligned} \exists\gamma \in S,\ |\partial A| &\geq \frac{\varepsilon\|f\|}{2n^2} \\ &= \varepsilon\frac{ab}{2n} \\ &= \frac{\varepsilon}{2}\left(1 - \frac{|A|}{n}\right)|A| \end{aligned}$$

Hence the result with $c \geq \dfrac{\varepsilon}{2}$.

The Margulis Construction : Let $\Gamma_n := SL_n(\mathbb{Z})$, with $n \geq 3$ so that it has property (T). We know that this group is generated by $R := \{A_n, B_n\}$, where :

$$A_n := \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & & \vdots \\ 0 & \ddots & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B_n := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & \vdots & & \ddots & 1 \\ (-1)^{n-1} & 0 & \dots & \dots & 0 \end{pmatrix}$$

To apply theorem 2.3.1 we need a symmetric generating set S, therefore we set $S := \{A_n, B_n, C_n, D_n\}$, where :

$$C_n := A_n^{-1} = \begin{pmatrix} 1 & -1 & 0 & \dots & 0 \\ 0 & 1 & 0 & & \vdots \\ 0 & \ddots & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad D_n := B_n^{-1} = \begin{pmatrix} 0 & \dots & \dots & 0 & (-1)^{n-1} \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

Let p be a prime number. We denote $SL_n(p) := SL_n(\mathbb{F}_p)$ and $\Gamma_n(p) := \ker(SL_n(\mathbb{Z}) \to SL_n(p)) \lhd \Gamma_n$. These subgroups have finite index since $\Gamma_n/\Gamma_n(p) \cong SL_n(p)$, thus, by theorem 2.3.1, we have that $(\mathcal{C}(SL_n(p), S_n))_{p \text{ prime}}$ is a family of expander graphs, which we will call Margulis graphs.

How "effective" is this family of expanders ? Well, we know by theorem 2.3.1 that these graphs are 4–regulars and that their expansion constant is greater or equal to $\frac{\varepsilon}{2}$, where ε can be any Kazhdan constant for the group $SL_n(\mathbb{Z})$. But we also know by proposition 2.2.4 that $\frac{1}{20\nu_n(\mathbb{Z})}$ is a Kazhdan constant for this group, hence the Margulis graphs are expanders for a constant c such that :

$$c \geq \frac{1}{40\nu_n(\mathbb{Z})}$$

Since by proposition 2.2.2 we know that $\nu_n(\mathbb{Z}) \leq \frac{1}{2}(3n^2 - n) + 36$, we have that :

$$c \geq \frac{1}{20(3n^2 - n) + 1440}$$

In particular :

$$c = \Omega\left(\frac{1}{n^2}\right)$$

To give the reader some sort of a graphic illustration of these graphs, we computed the Cayley graph of $SL_3(2)$ (corresponding to the first Margulis graph for $n = 3$), using a `python` whose source code can be found in appendix B.

Each vertex on Fig. 2.2 represents one the 168 matrices in $SL_3(2)$, in the order they are computed by our `python\verb` script. Also remark that for this particular graph we have the following lower bound[2.5] on c :

$$c \geq \frac{1}{1920}$$

Therefore, for any set S of vertices in our graph, we have :

$$\frac{|\partial S|}{|S|} \geq \frac{1}{1920}\left(1 - \frac{|S|}{3}\right)|S|$$

Finally, remark that these bounds hold for any of the "$n = 3$" Margulis graphs.

[2.5] Which actually isn't *that* great ...

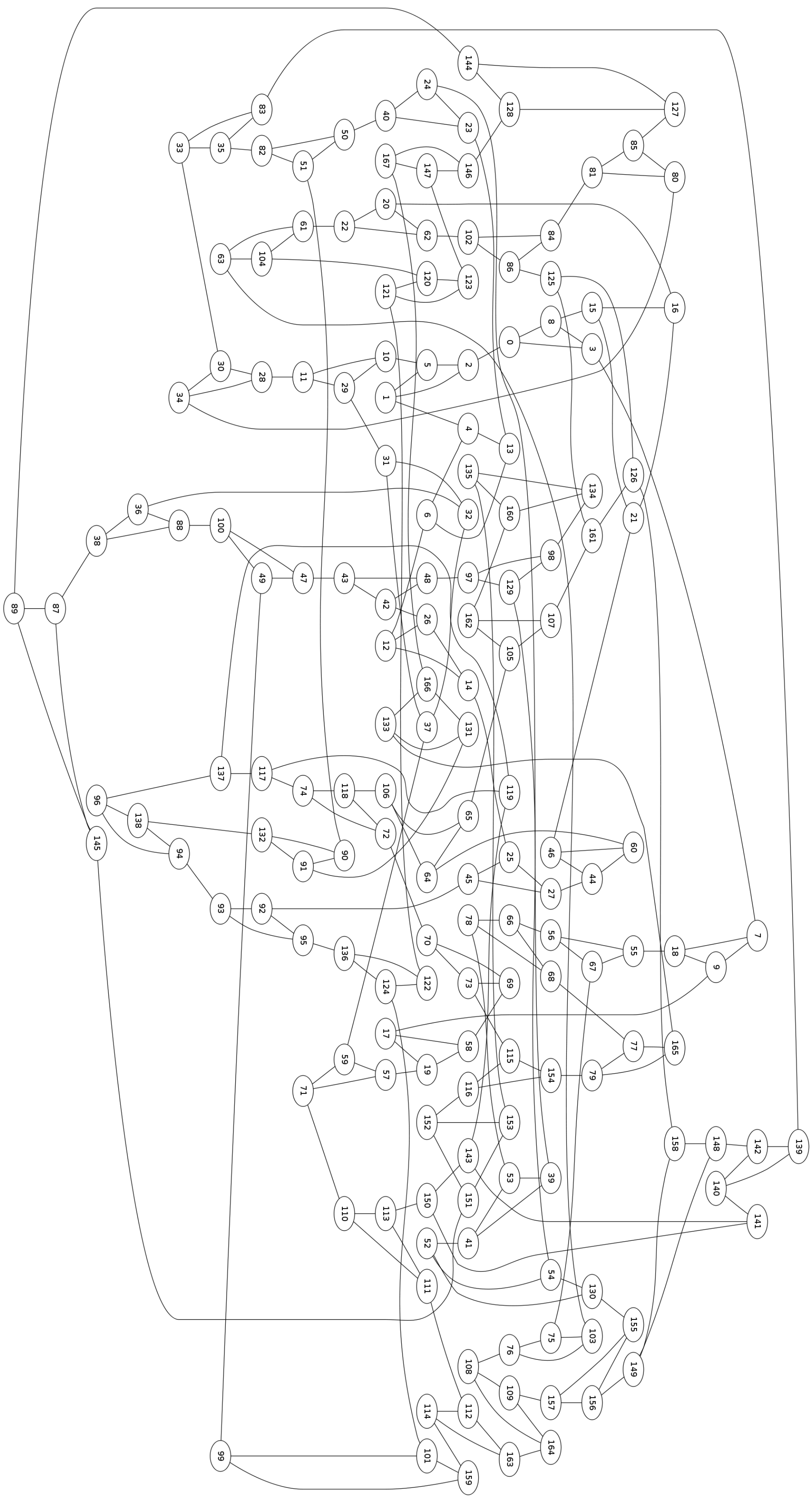

Figure 2.2: First Margulis Graph for $n = 3$

Acknowledgement

I would like to thank Dr. Cornelia Drutu for having me as an intern for two months, even though she was herself quite busy and for helping me getting on the right tracks, especially at the very beginning of my work in Oxford. I would also like to thank the kind residents of office SG09 at the Mathematical Institute, namely Jessica Banks, David Hume, Andrew Sale and Richard Wade for their help, their patience[2.6] and the much needed daily tea break. Actually, I am grateful to all the folks I encountered in the Mathematical Institute for the warm welcome I was given there. Last but certainly not least, I thank Ophélie Rouby for her support and proof–reading skills.

[2.6] And lack of face palming while answering my questions ...

Appendix A

Prerequisites

This appendix sums up a few generic results on graphs (A.1), group representations (A.2) and ℓ_p spaces (A.3). We tried to keep these as compact as we could, hence the utter lack of anything resembling a proof beyond this point[1.1].

A.1 Graphs

In this section we recall some generic notions about graphs. Since such elements have absolutely no use for expanders, we forbid graphs to have multiple edges and/or self–loops. Simple as that. All graphs considered are also assumed to be nonempty.

Recommended references : [Die05], [Coh89].

A.1.1 Basic Notions on Graphs

Definition A.1.1 (Graph)
We call (undirected) graph an ordered pair of sets $G := (V(G), E(G))$, where $E(G) \subset V(G) \times V(G)$ such that :

$$\forall (v, w) \in E(G),\ (w, v) \in E(G)$$

The elements of $E(G)$ are called the edges of the graph G and those of $V(G)$ its vertices.

If no ambiguity is to be feared, we will denote $E(G)$ (respectively $V(G)$) simply by E (resp. V). We also define two mappings $\sigma : E \to V$ and $\overline{\cdot} : E \to E$ such that $\forall e \in E$, $e \neq \overline{e}$ and $\overline{\overline{e}} = e$.

We then define another mapping $\tau : E \to V$ by $e\tau := \overline{e}\sigma$. Given one edge e, we call $e\sigma$ the beginning of e, $e\tau$ its ending and $\overline{e}$ its inverse.

Definition A.1.2 (d–Regular Graph)
A graph is called d–regular if each of its vertices has exactly d incident edges.

For the remainder of this section, let $G = (V, E)$ be a nonempty graph.

Definition A.1.3 (Path, Loop)
We call path in G any finite sequence $(e_1, \ldots, e_n)$ (with $n \geq 1$) of edges such that $\forall i \in [n-1]$, $e_i\tau = e_{i+1}\sigma$.
We call vertices of such a path the elements of the set $\{\sigma e_1\} \cup \ldots \cup \{\sigma e_n\} \cup \{e_n\tau\}$, and define its beginning (resp. end) to be $e_1\sigma$ (resp. $e_n\tau$).
A path is called a loop if $e_1\sigma = e_n\tau$.

Remark : The integer $\ell(e) := n$ is called length of the path e. It can sometimes be convenient to allow paths of length zero, which we define as a single vertex.

Definition A.1.4 (Simple Path, Circuit)
Let $(e_1, \ldots, e_n)$ be a path in G.

[1.1] You have been warned ...

(i) $(e_1, \dots, e_n)$ *is called a simple path if* $\forall i \neq j$, $\sigma e_i \neq \sigma e_j$ *and* $\sigma e_i \neq e_n\tau$.

(ii) $(e_1, \dots, e_n)$ *is called a circuit if it is a loop, if* $\forall i \neq j$, $\sigma e_i \neq \sigma e_j$ *and if it is not of the form* $(e, \overline{e})$.

Definition A.1.5 (Reducible Path)
A path $(e_1, \dots, e_n)$ *on* G *is called reducible if there exists* $1 \leq i \leq n$ *such that* $e_{i+1} = \overline{e_i}$. *Else, it is called irreducible.*

☞ Plainly, if two vertices can be joined by a path, they can be joined by an irreducible path.

Definition A.1.6 (Subgraph)
We call subgraph of G *any ordered pair of sets* (V_1, E_1) *such that :*

(i) $E_1 \subset E$;

(ii) $V_1 \subset V$;

(iii) $\forall e \in E, \overline{e} \in E_1$ *and* $e\sigma \in V_1$.

Note that the two conditions in *(iii)* imply that $\forall e \in E_1$, $e\tau \in V_1$.

Proposition A.1.1
The intersection (resp. reunion) of any family of subgraphs of G *is itself a subgraph of* G.

Definition A.1.7 (Full Subgraph)
Let $V_1 \subset V$.
Then we define the full subgraph on V_1 *as the subgraph*[1.2] (V_1, E_1) *of* G, *where we define* E_1 *as the following set :*

$$E_1 := \{e \in E \,|\, e\sigma,\, e\tau \in V_1\}$$

Definition A.1.8 (Spanning Subgraph)
A subgraph of G *is called spanning if its vertex set is equal to* V.

We then define the following equivalence relation on V : two vertices v and w are called connected (denoted $v \sim w$) if there exists a path $(e_1, \dots, e_n)$ on G such that $e_1\sigma = v$ and $e_n\tau = w$. Note that for $\sim$ to be an equivalence relation we need to allow paths of length zero so that each vertex is connected to itself.

Definition A.1.9 (Connected Graph)
A graph is said to be connected if any two of its vertices are connected.

✍ We also call connected components of a graph its full subgraphs whose vertex sets are the equivalent classes for $\sim$.

We now use these notions to endow the connected components of our graph with a metric.

Proposition A.1.2 (Graph Metric)
Let $H = (V', E')$ *a connected component of* G.
Then we define a distance d_H *on* E' *via the following :*

$$d_H : (x, y) \mapsto \begin{cases} 0 \text{ if } x = y \\ \min\{\ell(e) \,|\, e \text{ simple path linking } x \text{ and } y\} \text{ else} \end{cases}$$

Definition A.1.10 (Degree)
Let $v \in V$.

(i) *We call degree (or valency) of* v *the natural number* $\deg(v) := |E(\{v\})|$.

(ii) *We call minimal degree of* G *the following quantity :*

$$\delta(G) := \min_{v \in V} \deg(v)$$

[1.2] Plainly, such a pair is indeed a subgraph of G.

A.1.2 Matchings

Definition A.1.11 (Matching)
Let $G = (V, E)$ be a graph.
We call matching in E any subgraph M of G whose edges are independent, i.e none of its edges have a common end. Any vertex incident to an edge of M is called matched (by M), others are called unmatched (by M).

Example : On fig. A.1, the red edges define a matching on the example graph. Note that one vertex (5) is left out of the matching.

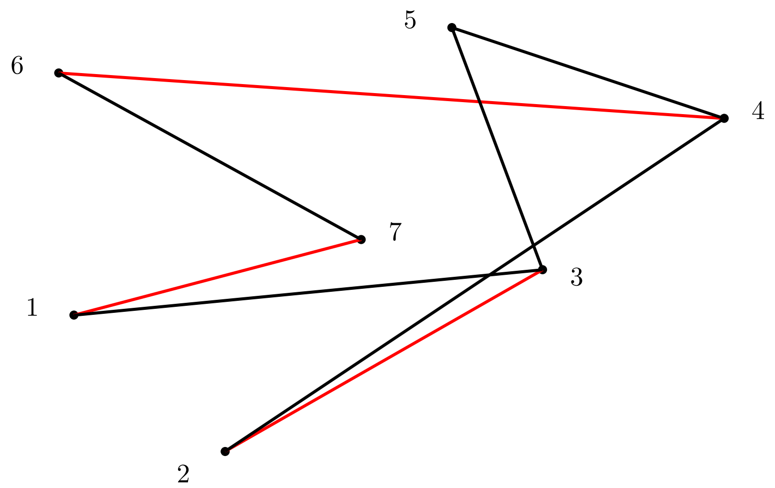

Figure A.1: Example graph

Definition A.1.12 (Matching of a Vertex Set)
Let $G = (V, E)$ be a graph.
Let $U \subset V$.
Let M be a matching on G.
We say that M is matching of U if every vertex in U is incident to at least an edge of M (and so exactly to one of them, since the edges in M are independent).

Example : On the example graph of fig. A.1, the red edges form a matching of $\{1, 2, 3, 4, 6, 7\}$ (and so of any of its subset). We can turn into a matching of the whole graph by removing the $(2, 3)$ edge and adding $(2, 4)$ and $(3, 5)$.

Definition A.1.13 (Perfect Matching)
Any 1–regular spanning matching is called a perfect matching.

☞ Note that this means that a perfect matching is exactly a matching of the whole vertex set.

Definition A.1.14 (Hamilton Cycle)
Let $G = (V, E)$ be a graph with more than 3 vertices.
We call Hamilton cycle on G any finite sequence $(v_0, e_0, \ldots, e_{k-1}, v_k)$ such that :

(i) $\forall 0 \leq i \leq k$, $v_i \in V$;

(ii) $\forall 0 \leq i \leq k-1$, $e_i \in E$ *and* $e_i = (v_i, v_{i+1})$;

(iii) $v_0 = v_k$;

(iv) the sequence $(v_0, \ldots, v_k)$ *contains every vertex in* V *exactly once.*

✍ It is easy to see that a graph which has a Hamilton cycle and an even number of vertices has a perfect matching : indeed, one can explicitly construct said matching by taking every even–numbered edge in the cycle.

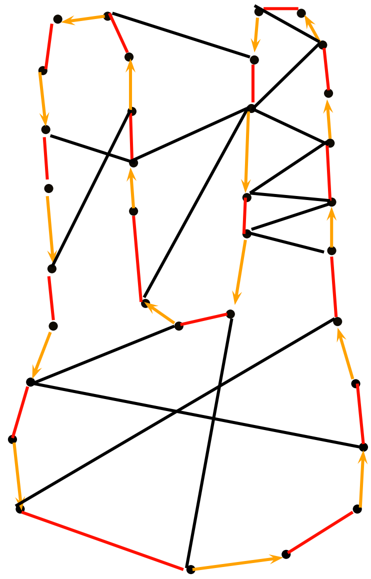

Figure A.2: Example graph

Example : On the example graph of fig. A.2 the orange and red edges define a Hamilton cycle. If you keep only the orange[1.3] edges, you obtain a perfect matching.

The following theorem can thus be used to show that a graph has a perfect matching.

Theorem A.1.3 (Dirac)
Every graph with more than $n = 3$ vertices and minimal degree above $\frac{n}{2}$ has a Hamilton cycle.

A.1.3 Cayley Graphs

Definition A.1.15 (Cayley Graph)
Let H be a group.
Let $S \subset H$ (note that S need not be a subgroup of H).
We call Cayley graph of S on H the graph $\mathcal{C}(H, S) = (V, E)$, where :

(i) the vertex set V is equal to H ;

(ii) $(g, h) \in E \Leftrightarrow \exists s \in S,\ g.s = h$.

Remark : Plainly, if S is symmetric then the Cayley graph $\mathcal{C}(H, S)$ is $|S|$–regular.

Proposition A.1.4
Let H be a group.
Let $S \subset H$.
Then :

$$S \text{ generates } H \\ \Leftrightarrow \\ \mathcal{C}(H, S) \text{ is connected}$$

A.2 Notions on Representation Theory

We now proceed to state a few results on group representations, which will mostly see use in chapter 2.

Recommended reference : [BdlHV08].

[1.3] Which are also sporting tiny arrowheads, in case you have printed this document in black and white.

A.2.1 Unitary Representations

For the remainder of this subsection, we consider a topological group G.

Definition A.2.1 (Unitary Representation)
A unitary representation of the group G is a pair $(\pi, \mathcal{H})$, where :

(i) $\mathcal{H}$ is a Hilbert space ;

(ii) $\pi : G \to \mathcal{U}(\mathcal{H})$ is a group homomorphism such that for every $\xi \in \mathcal{H}$, the following mapping is continuous :

$$\begin{aligned} G &\to \mathcal{H} \\ g &\mapsto \pi(g)\xi \end{aligned}$$

We call dimension of the representation $(\pi, \mathcal{H})$ the dimension of the linear space $\mathcal{H}$.

Note that since the choice of $\mathcal{H}$ is in a way "contained" in the mapping π, we will sometimes denote a representation $(\pi, \mathcal{H})$ simply by π.

Example : Suppose that G is finitely generated and let V be the vector space of all mappings $f : G \to \mathbb{C}$ (which is Hilbert since it is of finite dimension). Now consider the following mapping :

$$\forall f \in V,\, \forall x, h \in G,\, (r_G(h)f)(x) := f(xh)$$

Then (r_G, V) is a representation of G, known as the regular representation of the aforementioned group.

Proposition A.2.1 (Direct Sum of Unitary Representations)
Let $((\pi_i, \mathcal{H}_i))_{i\in I}$ be a family of unitary representations of G.
Then the pair $(\bigoplus_{i\in I} \pi_i, \bigoplus_{i\in I} \mathcal{H}_i)$ is a unitary representation of G, called direct sum of $((\pi_i, \mathcal{H}_i))_{i\in I}$, where :

$$\forall g \in G,\, \forall \xi = (\xi_i)_{i\in I} \in \bigoplus_{i\in I} \mathcal{H}_i,\, \left(\bigoplus_{i\in I} \pi_i\right)(g)\xi := (\pi_i(g)\xi_i)_{i\in I}$$

Definition A.2.2 (Matrix Coefficients)
Let $(\pi, \mathcal{H})$ be a unitary representation of G. We call matrix coefficients of π the following mappings (where $\xi, \eta \in \mathcal{H}$) :

$$\begin{aligned} G &\to \mathbb{C} \\ g &\mapsto \langle \pi(g)\xi, \eta\rangle \end{aligned}$$

Example : The matrix coefficients of the regular representation (r_G, V) of a finitely generated group G are the mappings $(f, g \in V)$:

$$\begin{aligned} G &\to \mathbb{C} \\ h &\mapsto \int_G f(xh)\overline{g(x)}dx \end{aligned}$$

Definition A.2.3 (Representation Invariants)
Let $(\pi, \mathcal{H})$ be a representation of G.

(i) A vector $x \in \mathcal{H} \setminus \{0\}$ is called an invariant vector of $(\pi, \mathcal{H})$ if :

$$\forall g \in G,\, \pi(g)x = x$$

(ii) A subset (resp. linear subspace) V of $\mathcal{H}$ is called an invariant subset (resp. subspace) of $(\pi, \mathcal{H})$ if :

$$\forall g \in G,\, \forall v \in V,\, \pi(g)v \in V \;\; (i.e\ \rho(g)V = V)$$

Remark :

- When no misunderstanding is deemed possible, we will call such invariants G–invariants, without specifying the representation π involved.
- Note that an invariant subset doesn't necessarily contain any invariant vector. For example, the orthogonal subspace of the set of constant functions on G is an invariant subspace for the regular representation, whose only invariant vectors are the constant mappings on G.

Proposition A.2.2
Let $(\pi, \mathcal{H})$ be a unitary representation of G.
Let $K \subset \mathcal{H}$ be a G–invariant subset of $\mathcal{H}$.
Then $K^{\perp}$ is G–invariant.

Definition A.2.4 (Irreducible Representation)
A representation is called irreducible if it has no nontrivial invariant subspace.

Definition A.2.5 (Equivalent Representations)
Let (ρ, V) and $(\pi, \mathcal{H})$ be two unitary representations of G.
We call these representations isomorphic (or equivalents) if there is a continuous isomorphism of vector spaces $T : V \to \mathcal{H}$ such that :

$$\forall g \in G,\, T\rho(g) = \pi(g)T$$

Definition A.2.6 (Dual of a Topological Group)
We call dual of the group G the set $\widehat{G}$ of all equivalent classes of unitary representations of G.

Proposition A.2.3
Let $(\pi, \mathcal{H})$ be a unitary representation of G.
Then there is an orthogonal decomposition of $\mathcal{H}$ into a direct sum of invariant subspaces $\mathcal{H}_i$ such that for every index i the representation $(\pi, \mathcal{H}_i)$ is irreducible. Moreover, this decomposition is unique up to isomorphism.

Definition A.2.7 (Subrepresentation)
Let $(\pi, \mathcal{H})$ be a unitary representation of G.
Let K be a closed G–invariant subset of $\mathcal{H}$.
We call subrepresentation of π associated with K the representation (π^K, K), where $\pi^K := \pi_{|_K}$.

Definition A.2.8 (Containment)
Let $(\pi, \mathcal{H})$ and (ρ, V) be two unitary representations of G.
We say that ρ is (strongly) contained in π, which we denote by $\rho \subset \pi$, if ρ is equivalent to any subrepresentation of π.

Remark : Plainly, a subrepresentation of a representation π is contained in π.

We will also need the notion of weak containment in order to study Kazhdan's property (T) :

Definition A.2.9 (Weak Containment)
Let $(\pi, \mathcal{H})$ and (ρ, V) be two unitary representations of G.
Then we say that ρ is weakly contained in π, denoted $\rho \propto \pi$, if every matrix coefficient of ρ is a limit, uniformly on compact sets of G, of matrix coefficients of π.

Remark : Note that strong containment doesn't imply weak containment. The existence (to a certain extent) of such properties is indeed one way to characterise Kazhdan's property (T).

A.2.2 Projection Valued Measures

The aim of this subsection is to introduce the SNAG theorem, which will be needed to show that $SL_n(\mathbb{Z})$ has property (T) for $n \geq 3$.

Definition A.2.10 (Projection Valued Measure)
Let X be a topological space.
Let $\mathcal{H}$ be a Hilbert space.
We call projection valued measure on X any mapping $E : \mathcal{B}(X) \to \mathcal{P}(\mathcal{H})$ such that :

(i) $E(\emptyset) = 0$;

(ii) $E(\mathcal{H}) = \mathrm{id}_{\mathcal{H}}$;

(iii) $\forall A, B \in \mathcal{B}(X)$, $E(A \cap B) = E(A)E(B)$;

(iv) if $(B_n)_n \in \mathcal{B}(X)^{\mathbb{N}}$ *is a sequence of pairwise disjoints Borel sets, we have that :*

$$E\left(\bigcup_{n\in\mathbb{N}} B_n\right) = \sum_{n=0}^{\infty} E(B_n)$$

Let us consider a topological group G. We wish to endow its dual $\widehat{G}$ with a nice topology in order to consider projection valued measures on it.

Definition A.2.11 (Fell Topology)
Let $(\pi, \mathcal{H}) \in \widehat{G}$.
We define open neighbourhoods of $(\pi, \mathcal{H})$ as follows : $\forall K \subset\subset G$, $\forall \varepsilon > 0$, $\forall v \in \mathcal{H}$ of unit norm, let :

$$W(K, \varepsilon, v) := \{(L, \sigma) \in \widehat{G} \,|\, \exists w \in L \textit{ of unit norm such that } \forall g \in K,\, |\langle v, \pi(g)v\rangle - \langle w, \sigma(g)w\rangle| < \varepsilon\}$$

This determines a topology on $\widehat{G}$, called the Fell topology.

Definition A.2.12
Let X be a topological space.
Let $\mathcal{H}$ be a Hilbert space.
Let $E : \mathcal{B}(X) \to \mathcal{P}(\mathcal{H})$ be a projection valued measure on X.
We say that E is regular if :

$$\begin{aligned}\forall \xi \in \mathcal{H},\, \forall B \in \mathcal{B}(X),\, \langle E(B)\xi, \xi\rangle &= \sup\{\langle E(C)\xi, \xi\rangle \,|\, C \subset B,\, C \textit{ closed }\} \\ &= \inf\{\langle E(O)\xi, \xi\rangle \,|\, B \subset O,\, O \textit{ open }\}\end{aligned}$$

We now state the following theorem[1.4], which we use to show that $SL_n(\mathbb{Z})$ has property (T) for $n \geq 3$:

Theorem A.2.4 (Stone – Naimark – Ambrose – Godement)
Let $(\pi, \mathcal{H})$ be a unitary representation of a locally compact Abelian group G.
Then there exists a unique regular projection valued measure $E_\pi : \mathcal{B}(\widehat{G}) \to \mathcal{P}(\mathcal{H})$ such that :

$$\forall x \in G,\, \pi(x) = \int_{\widehat{G}} \overline{\widehat{x}(x)} dE_\pi(\widehat{x})$$

A.3 ℓ_p Metrics

In this appendix we recall a few facts about ℓ_p spaces and the associated metrics.

RECOMMENDED REFERENCE : [Pis89].

Definition A.3.1 (ℓ_p^n Space)
Let $p > 0$.
Let $n \geq 1$.
We call ℓ_p^n space the normed vector space $(\mathbb{R}^n, \|.\|_p)$, where :

$$\forall x \in \mathbb{R}^n,\, \|x\|_p := \sqrt[p]{\sum_{i=1}^{n} |x_i|^p}$$

[1.4] Sometimes dubbed the "SNAG theorem", mostly in order to spare trees.

Remark :

- We will sometimes speak of "ℓ_p spaces". In that case, the dimension is omitted for an increase in generality[1.5]. Note however that this doesn't allow the aforementioned space to be infinitely dimensioned.
- When no ambiguity is deemed possible[1.6], we will denote $\|.\|_p$ simply by $\|.\|$.

Definition A.3.2 (ℓ_p Metric)
Let $(X = \{x_1, \dots, x_N\}, d)$ be a finite metric space.
We say that d is an ℓ_p metric if there exists a subset $S = \{s_1, \dots, s_N\}$ of an ℓ_p space such that :

$$\forall i, j \in [N],\ d(x_i, x_j) = \|s_i - s_j\|$$

Pretty much the only result we will need on ℓ_p metrics is the following :

Proposition A.3.1
Every ℓ_2 metric is an ℓ_1 metric.

[1.5] Hopefully without any increase in the reader's confusion ...
[1.6] That is, almost everywhere in this report.

Appendix B

Source Codes

The following scripts make no attempt either at robustness nor at optimization (see the matrix product for a prime example of our leniency), so we kindly ask the reader to keep this in mind while browsing this appendix. We only used these as an easy way to get a graphic representation of low–dimensional Margulis graphs

B.1 group.py

This first `python` script merely computes "any" group of (very) small cardinality through a very simple algorithm :

- start with a list of generators ;
- add to the list any product of these two which isn't already in ;
- repeat the previous step with the updated list as long as you find something to add.

Furthermore, this script will also write down all matrices in $SL_3(2)$ in a text file, for the sake of convenience.

```
# -*- coding: utf-8 -*-
from copy import *

def group(L,f) :
        #Bruteforce algorithm to compute
        #a (small !) group using a generating subset
        end = 0
        while (end == 0) :
                end = 1
                for x in L :
                        for y in L :
                                if not (f(x,y) in L) :
                                        L = L + [f(x,y)]
                                        end = 0
        return L

#A matrix is the list of its rows


def prod_mat(A,B) : #Matrix product (mod 2)
        R=deepcopy(A)
        for i in range(len(A)) :
        #We assume A and B to be
        #square matrices of same dimension
                for j in range(len(A)) :
                        S = 0
                        for k in range(len(A)):
```

```
                                S = S + A[i][k]*B[k][j]
                        R[i][j] = S % 2
        return R


def print_matrix(M) :
        #Print a matrix
        for i  in range(len(M)) :
                print M[i]
        print ' '

def exist(f):
        #Check if file f exists in the working directory
        try:
                fop = file(f, "r")
                fop.close()
                return True
        except:
                return False

def id_in_list(A,L) :
        #Check if A is in L and return its index
        r = -1
        for i in range(len(L)) :
                if L[i] == A :
                        r = i
        return r;


def write_3() :
        #Compute and write the list of the matrices
        #in SL_3(2) in group3.txt
        A = [[1,1,0],[0,1,0],[0,0,1]]
        B = [[0,1,0],[0,0,1],[1,0,0]]
        L = [A,B]
        outFileName='group3.txt'
        if exist(outFileName):
                print 'ERROR'
        else:
                R = group(L, prod_mat)
                outFile=file(outFileName,'w')
                for A in R :
                        for i  in range(len(A)) :
                                for j in range(len(A)):
                                        outFile.write(str(A[i][j]))
                                        outFile.write(' ')
                                outFile.write('\n')
                        outFile.write('\n')
                outFile.close

if __name__=='__main__':
        write_3()
```

B.2 graph.py

This script draws the first Margulis graph for $n = 3$ using the `pygraph` utility. Note that an attempt was made to compute this graph for $n = 4$, with very little success due to the crude nature of our group computing utility.

```
# -*- coding: utf-8 -*-

import sys
sys.path.append('.')
sys.path.append('/usr/lib/pyshared/python2.6')
from group import *
import gv
from pygraph import *
from pygraph.readwrite.dot import write

def draw_3() :
	#Draw the first Margulis graph for n = 3
	G = graph()
	A = [[1,1,0],[0,1,0],[0,0,1]] #A^2 mod 2 = Id
	B = [[0,1,0],[0,0,1],[1,0,0]]
	D = [[0,0,1],[1,0,0],[0,1,0]]
	L = [A,B]
	R = group(L,prod_mat)
	N = range(len(R))
	G.add_nodes(N)
	for i in N :
		for x in [A,B,D] :
			G.add_edge(i, id_in_list(prod_mat(R[i],x), R))
	dot = write(G)
	gvv = gv.readstring(dot)
	gv.layout(gvv,'dot')
	gv.render(gvv,'png','graph3.png')

def draw_4() :
	#Draw the first Margulis graph for n = 4 (not usable since "group"
	#isn't optimized enough). Besides, the picture would be a mess.
	G = graph()
	A = [[1,1,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1]] #A^2 mod 2 = Id
	B = [[0,1,0,0],[0,0,1,0],[0,0,0,1],[1,0,0,0]]
	D = [[0,0,0,1],[1,0,0,0],[0,1,0,0],[0,0,1,0]]
	L = [A,B]
	R = group(L,prod_mat)
	N = range(len(R))
	G.add_nodes(N)
	for i in N :
		for x in [A,B,D] :
			G.add_edge(i, id_in_list(prod_mat(R[i],x), R))
	dot = write(G)
	gvv = gv.readstring(dot)
	gv.layout(gvv,'dot')
	gv.render(gvv,'png','graph4.png')

if __name__=='__main__':
	draw_3()
	#draw_4() #Cardinality of ~20000 is too much for "group" to handle
```

Bibliography

[Aro05] Sanjeev Arora. The ellipsoid algorithm for linear programming. www.cs.princeton.edu/courses/archive/fall05/cos521/ellipsoid.pdf, 2005.

[BdlHV08] Bachir Bekka, Pierre de la Harpe, and Alain Valette. *Kazhdan's Property (T)*. Cambridge University Press, 2008.

[Coh89] Daniel E. Cohen. *Combinatorial Group Theory : a Topological Approach*. Cambridge University Press, 1989.

[Die05] Reinhard Diestel. *Graph Theory (third edition)*. Springer, 2005.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Widgerson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43, 2006.

[Jau07] Ghislain Jaudon. Notes on relative kazhdan's property (t). www.unige.ch/math/folks/jaudon/notes.pdf, 2007.

[LLR95] Nathan Linial, Eran London, and Yuri Rabinovich. The geometry of graphs and some of its algorithmic applications. *Combinatorica*, 15, 1995.

[Lub94] Alexander Lubotzky. *Discrete Groups, Expanding Graphs and Invariant Measures*. Birkhäuser, 1994.

[Pis89] Gilles Pisier. *The Volume of Convex Bodies and Banach Space Geometry*. Cambridge University Press, 1989.

[Sha99] Yehuda Shalom. Bounded generation and kazhdan's property (t). *Publications mathématiques de l'I.H.É.S*, 90, 1999.

Index