Expander graphs

Summer school
"Applications of expander graphs
to number theory and computer science"

UNC Greensboro, May 24 to 28, 2021

E. Kowalski

ETH Zürich
kowalski@math.ethz.ch

Contents

Lecture 1: combinatorial definition

In this first lecture, we define graphs, and explain the key concepts that are most relevant in the theory of expander graphs (especially the metric on graphs). Then we provide some examples before defining expander graphs.

1.1. Graphs.

We consider graphs of a certain specific type: unoriented graphs, where loops based at a vertex and multiple edges are permitted. There is more than one way to do it, so one should see the following definition as specifying a specific "encoding" of the intuitive notion that we want to use, and not as the only way to define graphs.

Definition 1.1 (Graph)**.** A *graph* Γ is given by a triple (V, E, ep) where V and E are arbitrary sets, called respectively the set of vertices of Γ and the set of edges of Γ, and

$$\mathrm{ep} : E \longrightarrow V^{(2)}$$

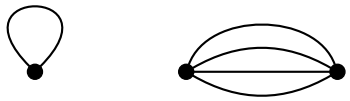
is an arbitrary map, called the *endpoint map*, where $V^{(2)}$ denotes the set of subsets $e \subset V$ of cardinality either 1 or 2.

If $\alpha \in E$ is an edge of Γ, the elements of $\mathrm{ep}(\alpha)$ are called *extremities* of α. If $\alpha \neq \beta$ are distinct edges of Γ, they are called *adjacent* at a vertex $x \in V$ if $x \in \mathrm{ep}(\alpha) \cap \mathrm{ep}(\beta)$ is a common extremity.

Given a vertex $x \in V$, the number of edges α such that x is an extremity, i.e., such that $x \in \mathrm{ep}(\alpha)$, is called the *degree* or *valency* of x, denoted $\mathrm{val}(x)$. If the valency is the same, say equal to $d \geqslant 0$, at all vertices, the graph is called *regular*, or d-regular.

A graph is *finite* when both V and E are finite; it is *countable* if both V and E are countable.

Remark 1.2. (1) The intuition should be clear, as the terminology indicates: to express a graph (say, one drawn on paper) in this form, one takes as set of edges the "physical" ones, and one defines $\mathrm{ep}(\alpha)$ to be the set of extremities of such an edge. This allows *loops*, which are edges where $\mathrm{ep}(\alpha) = \{x\}$ is a singleton (the loop is then based at x, of course), as well as multiple edges with the same endpoints, say $\alpha_1 \neq \alpha_2$ with $\mathrm{ep}(\alpha_1) = \mathrm{ep}(\alpha_2) = \{x, y\}$.

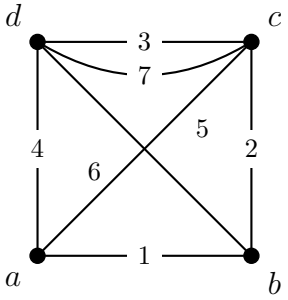


Conversely, to "draw" a graph Γ coded as a triple (V, E, ep), we can draw the points of V, then for each $\alpha \in E$, we look at $\mathrm{ep}(\alpha)$ and draw either (1) a loop from x to x if $\mathrm{ep}(\alpha) = \{x\}$ is a single element, or (2) an arc (without orientation) from x to y if $\mathrm{ep}(\alpha) = \{x, y\}$ with $x \neq y$.

For instance, consider the graph with $V = \{a, b, c, d\}$, $E = \{1, 2, 3, 4, 5, 6, 7\}$, and

$$\mathrm{ep}(1) = \{a, b\}, \quad \mathrm{ep}(2) = \{b, c\}, \quad \mathrm{ep}(3) = \{c, d\}, \quad \mathrm{ep}(4) = \{a, d\},$$
$$\mathrm{ep}(5) = \{a, c\}, \quad \mathrm{ep}(6) = \{b, d\}, \quad \mathrm{ep}(7) = \{c, d\},$$

and check that it can be represented as



As in this figure, it is not always possible to draw the edges without some overlap (graphs for which it is possible are called *planar*; see for instance [8, Ch. 10] for a discussion of properties and characterizations of planar graphs). However, for any finite graph, it is possible to "draw" it in $\mathbf{R}^3$ without overlap. This should be fairly clear intuitively, and the reader should attempt to see what is involved in a rigorous proof. (Basically, $\mathbf{R}^3$ minus a finite number of smooth compact curves, seen as images of maps $\gamma : [0,1] \longrightarrow \mathbf{R}^3$, is path-connected.)

(2) If Γ has no loops (which means that every set of endpoints $\mathrm{ep}(\alpha)$ contains two elements) and no multiple edges (so that ep is an injection of E into the set of subsets of order 2 in V), the graph is called *simple*. In that case, the set of edges can also be identified with a subset $R \subset V \times V$ such that $(x,y) \in R$ if and only if $(y,x) \in R$ (expressing the fact that edges are not oriented) and such that $(x,x) \notin R$ for all $x \in V$ (expressing the absence of loops). This is a more common way of "coding" simple graphs. We will sometimes omit mention of ep when considering a simple graph, viewing the edges as a set of subsets of V with two elements.

(3) We will also $x \sim y$ to say that vertices x and y are joined by at least one edge.

(4) By convention, for a graph Γ, we write $|\Gamma| = |V|$: the "size" of Γ is identified with the number of vertices. We also sometimes write $x \in \Gamma$ to mean $x \in V$.

In order to encode a finite graph, one can also use its *adjacency matrix*:

Definition 1.3 (Adjacency matrix)**.** Let Γ be a finite graph. The *adjacency matrix* $A_\Gamma = (a(x,y))$ is the matrix with rows and columns indexed by V_Γ and with $a(x,y)$ equal to the number of edges with extremities (x,y), formally

$$a(x,y) = |\{\alpha \in E_\Gamma \mid \mathrm{ep}(\alpha) = \{x,y\}\}|.$$

Note that the adjacency matrix is always symmetric (in the sense that $a(x,y) = a(y,x)$), which reflects our use of *unoriented* edges. Conversely, given a symmetric matrix with non-negative integral entriers, one easily constructs a graph for which it is the adjacency matrix.

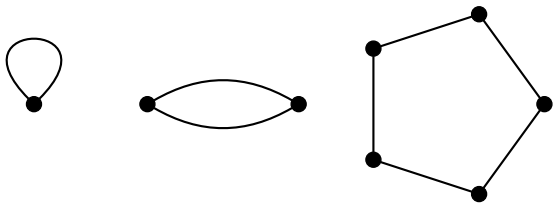
Example 1.4. Here are some elementary examples of "coding" for various families of graphs using Definition 1.1. The examples will be used frequently to illustrate some basic concepts.

(1) [Cycle] Let $m \geqslant 1$ be an integer. The m-cycle C_m is the graph with vertices $V_m = \mathbf{Z}/m\mathbf{Z}$, edges $E_m = \mathbf{Z}/m\mathbf{Z}$, and endpoint map given by

$$\mathrm{ep}(i) = \{i, i+1\}$$

for $i \in \mathbf{Z}/m\mathbf{Z}$. In other words, except when $m = 1$ (in which case the cycle is a single loop based at 0), there are two edges adjacent to any given $i \in V_m$: the edges coded by $i-1$, and the one coded by i itself.

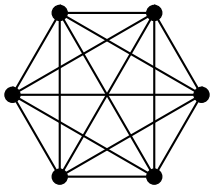
Here are the graphs for $m = 1$, $m = 2$ and $m = 5$:



(2) [Path] Let $m \geqslant 0$ be an integer. The *path of length* m, denoted P_m, is the graph with vertex set $V_m = \{0, \dots, m\}$ and edge set $E_m = \{1, \dots, m\}$, where $\mathrm{ep}(i) = \{i-1, i\}$ for $1 \leqslant i \leqslant m$. A path of length 0 is a graph with a single vertex and no edges. Here is the path of length 4:

We often say, somewhat abusively, that the vertices 0 and m are the *extremities* of the path.

(3) [Complete graph] Let again $m \geqslant 1$ be an integer. The *complete graph* K_m with m vertices has also $V_m = \{1, \dots, m\}$ but now $E_m = \{(x, y) \in V_m \mid x < y\}$, with $\mathrm{ep}((x, y)) = \{x, y\}$. In other words, each pair of distinct vertices is joined by (exactly) one edge. Here is the complete graph K_6:

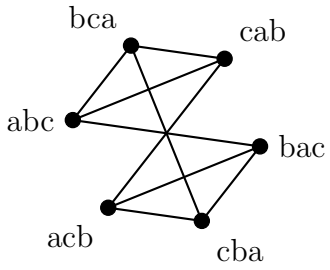


All graphs in these first examples are simple graphs, *except* for the cycles C_1 and C_2. Most of them are regular: C_1 is 1-regular, C_m is 2-regular for $m \geqslant 2$; P_0 is 0-regular, P_1 is 1-regular (but P_k is not regular for $k \geqslant 2$); K_m is $(m-1)$-regular for all $m \geqslant 1$.

(4) [A Cayley graph] Our last sequence of examples is less obvious, but it illustrates a very important type of graphs which will occur frequently later on, the *Cayley graphs associated to finite groups*.

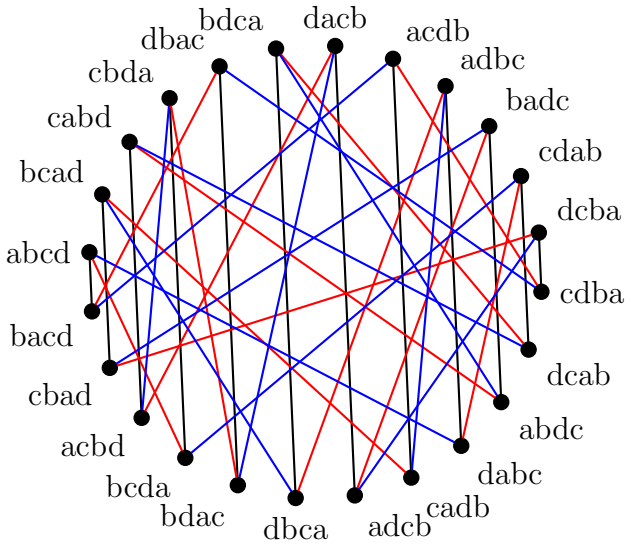
Following Diaconis and Saloff-Coste [26], we fix $n \geqslant 3$ and take as vertex set V_n all the possible arrangements of a deck D_n of n cards (so there are $n!$ elements in V_n). Then we define G_n as the simple graph where the vertex set is V_n and the edges correspond to either exchanging the top two cards (connecting, say, $(a, b, c, d) \in V_4$, to (b, a, c, d)), or bringing the bottom card to the top, or conversely (connecting, say $(a, b, c, d) \in V_4$ to (d, a, b, c) – bottom to top – and (a, b, c, d) to (b, c, d, a) – top to bottom.)

Thus, by definition, G_n is a 3-regular graph for each $n \geqslant 3$, with $n!$ vertices. Here is an illustration of G_3, with the deck $D_3 = \{a, b, c\}$, and in Figure 1.1 one of G_4, with deck $D_4 = \{a, b, c, d\}$ (it is by far the most complicated graph we will draw...).



As often in mathematics, once we have defined some types of "objects", it is important to discuss relations between them, which are encoded formally in certain "morphisms".

FIGURE 1.1. The graph G_4



Definition 1.5 (Maps of graphs)**.** Let Γ_1 and Γ_2 be graphs. A *morphism*, or *graph map*, from Γ_1 to Γ_2 is a pair (f, f_*) where

$$f : V_{\Gamma_1} \longrightarrow V_{\Gamma_2}$$

is a map between the vertex sets and

$$f_* : E_{\Gamma_1} \longrightarrow E_{\Gamma_2}$$

is a map between the edges, such that

$$\mathrm{ep}(f_*(\alpha)) = f(\mathrm{ep}(\alpha)) \tag{1.1}$$

for all $\alpha \in E_{\Gamma_1}$. In other words: an edge α between x and y is sent to an edge $f_*(\alpha)$ with extremities $f(x)$ and $f(y)$. We most often simply write f for such a map, using f_* for the edge map.

If the graphs are simple, then the companion edge-map f_* is uniquely specified by f itself: in that case, whenever there is an edge e between x and y, it is unique, and there must also be an edge between $f(x)$ and $f(y)$, which determines $f_*(e)$. However, in the presence of multiple edges, we must specify where each individual edge between x and y goes.

Let Γ be a graph. The *identity map* $\Gamma \to \Gamma$ of Γ is the pair $(\mathrm{Id}_V, \mathrm{Id}_E)$, and is denoted Id_Γ. For any graphs Γ_1, Γ_2, Γ_3 and maps

$$\Gamma_1 \overset{(f,f_*)}{\longrightarrow} \Gamma_2 \overset{(g,g_*)}{\longrightarrow} \Gamma_3,$$

the *composite map* is defined by the pair $(g \circ f, g_* \circ f_*)$, and is simply denoted $g \circ f$. Then

$$h \circ (g \circ f) = (h \circ g) \circ f$$

for any three maps that can be composed, and if $f : \Gamma_1 \longrightarrow \Gamma_2$, we have

$$f \circ \mathrm{Id}_{\Gamma_1} = f, \qquad \mathrm{Id}_{\Gamma_2} \circ f = f.$$

More definitions:

Definition 1.6 (Isomorphism, automorphism, embedding)**.** (1) A graph map $f : \Gamma_1 \to \Gamma_2$ is an *isomorphism* with inverse g if and only if $f \circ g = \mathrm{Id}_{\Gamma_2}$ and $g \circ f = \mathrm{Id}_{\Gamma_1}$. If $\Gamma = \Gamma_1 = \Gamma_2$, then f is called an automorphism of Γ.

(2) The inverse of an isomorphism is unique and is denoted f^{-1}. In fact, a morphism (f, f_*) is an isomorphism if and only if f and f_* are both bijections, and then $(f, f_*)^{-1} = (f^{-1}, f_*^{-1})$. In particular, the inverse of (f, f_*) is also an isomorphism. Moreover, the composite of two isomorphisms is also an isomorphism; hence the set of automorphisms of Γ, with the composition law, is a group, which is denoted $\mathrm{Aut}(\Gamma)$.

(3) An *embedding* $\Gamma_1 \hookrightarrow \Gamma_2$ is a graph map (f, f_*) such that f and f_* are both injective. If Γ_1 and Γ_2 and both simple, it suffices that the vertex map $f\colon V_1 \to V_2$ is injective.

Example 1.7. (1) The path P_k, for $k \geqslant 1$, has a non-trivial automorphism f (in fact an involution, i.e., we have $f \circ f = \mathrm{Id}$) which is intuitively given by "reversing the path", and can be defined formally by

$$f(i) = m - i, \qquad f_*(j) = m + 1 - j$$

for any vertex $i \in V_m = \{0, \dots, m\}$ and edge $j \in E_m = \{1, \dots, m\}$.

(2) [Subgraphs] Let $\Gamma = (V, E, \mathrm{ep})$ be a graph. For any subset $V' \subset V$ of vertices, and any subset $E' \subset E$ of edges with extremities lying in V' (i.e., such that $\mathrm{ep}(\alpha) \subset V'$ for any $\alpha \in E'$), the pair of inclusions $(V' \hookrightarrow V, E' \hookrightarrow E)$ is an embedding of the graph (V', E', ep) inside (V, E, ep). We then say that (V', E', ep) is a *subgraph* of Γ.

If E' is the set of *all* edges with extremities in V', i.e., if E' is defined to be

$$E' = \{\alpha \in E \mid \mathrm{ep}(\alpha) \subset V'\},$$

we say that (V', E', ep) is a *full subgraph* of Γ. Such subgraphs are therefore in one-to-one correspondence with subsets of V.

Embeddings or other graph maps can frequently be used to define invariants and distinguish special families of graphs. Here is an important example:

Definition 1.8 (Girth)**.** Let $\Gamma = (V, E, \mathrm{ep})$ be a graph.

(1) For $m \geqslant 1$, a *cycle of length* m in Γ is an embedding $C_m \to \Gamma$.

(2) The *girth* of Γ is the smallest integer $m \geqslant 1$ such that there exists at least one cycle of length m in Γ, or $+\infty$ if no cycle exists at all in Γ. We denote this integer $\mathrm{girth}(\Gamma)$.

Example 1.9. The girth of the cycle C_m itself is equal to m. Moreover, Γ has girth 1 if and only if Γ has at least one loop, and it has girth 2 if and only if it has no loop, but there are two distinct vertices which are joined by at least two edges. Similarly, having girth 3 means there are no loops, no multiple edges, but there exists a *triangle* in Γ, i.e., three distinct vertices x_1, x_2, x_3 and three edges α_1, α_2 and α_3 with α_1 joining x_1 and x_2, α_2 joining x_2 and x_3 and finally α_3 joining x_1 and x_3. (This is also equivalent to being a simple graph with an embedding of $K_3 = C_3$). For instance, the girth of K_m is infinite for $m = 1$ or 2, and is equal to 3 for $m \geqslant 3$. The reader is invited to check all these assertions...

Example 1.10 (Trees and forests)**.** Graphs with infinite girth have a name:

Definition 1.11 (Forests (and trees))**.** A graph Γ with infinite girth (i.e., there is no embedding $C_m \longrightarrow \Gamma$, for any $m \geqslant 1$) is called a *forest*. Anticipating the definition of connected graphs, a connected forest is called a *tree*.

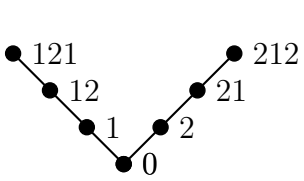
In particular, forests (and trees) are simple graphs. An example is the path P_k of length $k \geqslant 1$. Here are some more interesting examples. Fix some integers $d \geqslant 2$ and $k \geqslant 1$. The *finite rooted tree of degree d and depth k*, denoted $T_{d,k}$, is a simple graph defined by taking V to be the set of all words of length $\leqslant k$ (including the empty word,

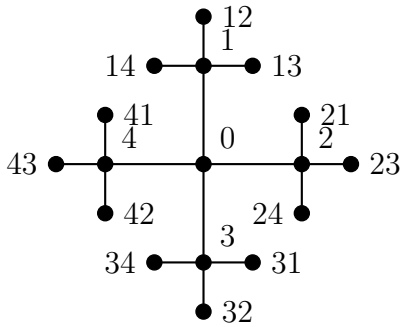
of length 0, which is called the "root" vertex of the tree) in the alphabet $A = \{1, \dots, d\}$ with no letter repeated twice in a row, i.e.

$$V = \bigcup_{0 \leqslant j \leqslant k} \{(s_1, \dots, s_j) \in A^j \mid s_i \neq s_{i+1} \text{ for } 1 \leqslant i \leqslant j-1\},$$

with edges between "neighboring" words, where w_1 is a neighbor of w_2 if w_2 can be obtained from w_1 either by adding a letter on the right (chosen among the $d-1$ letters distinct from the rightmost letter of w_1), or by removing the last letter.

Here are pictures of $T_{2,3}$ and $T_{4,2}$, with the vertices labeled with the corresponding words, which should clarify the matter. (Note that $T_{d,k}$ is *not* d-regular.)





One can extend this construction to infinite depth: the *d-regular tree* T_d, for $d \geqslant 2$, is the infinite graph with vertices given by all words of length $\geqslant 0$, without repeated letter, in the alphabet $\{1, \dots, d\}$, and with edges described in the same way using neighboring words.

One can also try to distinguish special graphs using (surjective) maps *to* another fixed one. Here is a classical notion that can be interpreted in this manner:

Definition 1.12 (Bipartite graph)**.** A graph Γ is *bipartite* if there exists a partition $V_\Gamma = V_0 \cup V_1$ of the vertex set in two disjoint subsets, so that any edge has one extremity in V_0, and one in V_1, i.e., such that

$$\mathrm{ep}(\alpha) \cap V_0 \neq \emptyset, \qquad \mathrm{ep}(\alpha) \cap V_1 \neq \emptyset$$

for each $\alpha \in E_\Gamma$. One sometimes says that V_0 is the set of "inputs" and V_1 the set of "outputs".

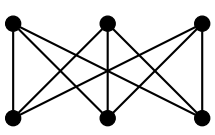
Example 1.13. The complete bipartite graph $K_{m,n}$ with $m \geqslant 1$ inputs and $n \geqslant 1$ outputs is the simple bipartite graph defined by the vertices

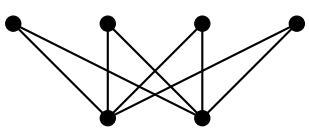
$$V_0 = \mathbf{Z}/m\mathbf{Z}, \qquad V_1 = \mathbf{Z}/n\mathbf{Z}, \qquad V = V_0 \cup V_1$$

(a disjoint union) and edges

$$E = \{\{x_0, x_1\} \subset V \mid x_0 \in V_0, \quad x_1 \in V_1\}.$$

Here are pictures of $K_{3,3}$ and $K_{2,4}$:





The reader can check, for instance, that the girth of $K_{m,n}$ is equal to 4 for $m, n \geqslant 2$, while it is infinite for $m = 1$ or $n = 1$.

1.2. **Distance and diameter.** Our edges have, for the moment, not been really used, except as abstract elements. Of course, an edge is intuitively supposed to represent a way of going from one extremity to another. And if one goes from x to an adjacent vertex (or neighbor) y, there is no reason to stop there. Going further on longer adventures along the edges of a graph will lead us to the topic of expansion. But first, we explain how to measure how far we can go:

Definition 1.14 (Paths and distance on a graph)**.** Let $\Gamma = (V, E, \mathrm{ep})$ be a graph.

(1) A *path of length* $k \geqslant 0$ in Γ is a *graph map* $P_k \xrightarrow{\gamma} \Gamma$, i.e., an ordered sequence $(x_0, \ldots, x_k)$ of vertices of Γ, and an ordered sequence $(\alpha_1, \ldots, \alpha_k)$ of edges of Γ such that

$$\mathrm{ep}(\alpha_i) = \{x_{i-1}, x_i\}$$

for $1 \leqslant i \leqslant k$. If $k \geqslant 1$, the *extremities* of the path γ are the vertices $x = \gamma(0)$, $y = \gamma(k)$, where 0 and k denote the distinguished vertices of P_k which have a single adjacent vertex. One says that γ is a path from x to y, and one writes $\ell(\gamma) = k$ for its length.

(2) For any two vertices x, $y \in V$, the *distance on* Γ *between* x *and* y, denoted $d_\Gamma(x, y)$ is defined as the minimum length of a path between x and y, if such a path exists, or $+\infty$ otherwise, i.e.,

$$d_\Gamma(x, y) = \min\{\ell(\gamma) \mid \gamma \text{ is a path from between } x \text{ and } y\} \in \{0, 1, \ldots\} \cup \{+\infty\}.$$

(3) The graph is *connected* if and only if $d_\Gamma(x, y)$ is finite for all x and $y \in V$, i.e., any two points can be joined by at least one path.

(4) A *geodesic* in Γ is a path γ such that the length of γ is equal to the distance in Γ between the extremities of γ.

Note that a path is allowed to "backtrack", since edges are unoriented, and that the vertices x_i might not be distinct. On the other hand, to compute the length, we need only look at paths that do not involve twice the same edge in succession.

Definition 1.15. Let Γ be a graph. A path $\gamma\colon P_k \to \Gamma$ of length $k \geqslant 0$ in Γ is *non-backtracking* if $\gamma_*(i) \neq \gamma_*(i+1)$ for $1 \leqslant i \leqslant k-1$, i.e., if the ordered sequence of edges corresponding to γ does not contain consecutively the same edge.

Proposition 1.16. (1) *If* Γ *is a connected graph, the distance function* d_Γ *is a metric on* V*, i.e., it is non-negative and satisfies*

$$d_\Gamma(x, y) = d_\Gamma(y, x),$$
$$d_\Gamma(x, y) = 0 \text{ if and only if } x = y,$$
$$d_\Gamma(x, y) \leqslant d_\Gamma(x, z) + d_\Gamma(z, y)$$

for all vertices x*,* y*,* $z \in V$*.*

(2) *If we define an equivalence relation on* V *by*

$$x \sim y \iff d_\Gamma(x, y) < +\infty,$$

then the full subgraph of Γ *corresponding to an equivalence class* $V' \subset V$ *is a connected graph such that the distance* $d_{\Gamma'}$ *is the restriction of* d_Γ *to* $V' \times V'$*, and there are no edges with an extremity in* V' *and another outside* V'*. These subgraphs are called the* connected components *of* Γ*.*

Proof. Part (1) is intuitively clear, but we give details. The symmetry is because a path P_k can be reversed using the automorphism f of P_k (Example 1.7, (2); note in passing that this depends on the fact that the edges are unoriented). The map $\gamma \mapsto \gamma \circ f$ is then

an involution (since f is an involution) between paths of length k from x to y and paths of length k from y to x, which implies $d_\Gamma(x,y) = d_\Gamma(y,x)$.

Further, $d_\Gamma(x,y) = 0$ if and only if there exists a path of length 0 from x to y; but a path $\gamma\colon P_0 \to \Gamma$ of length 0 has only one extremity, so that this holds if and only if $x = y$. Finally, the triangle inequality comes from the possibility of concatenating a path of length $k_1 = d_\Gamma(x,z)$ between x and z with one of length $k_2 = d_\Gamma(z,y)$ between z and y to obtain one of length $k_1 + k_2$ between x and y, as seen above, which shows that $d_\Gamma(x,y) \leqslant k_1 + k_2 = d_\Gamma(x,z) + d_\Gamma(z,y)$.

For (2), the fact that $\sim$ is an equivalence relation is elementary, and if V' is an equivalence class, we note that any edge $\alpha \in E$ has either all or no extremities in V': if $\mathrm{ep}(\alpha) = \{x,y\}$ with $x \in V'$, then the edge α shows (by definition) that $d_\Gamma(x,y) \leqslant 1$, so that $y \sim x$ is also in V'. Thus, if E' is the set of edges with an extremity in V', the graph (V', E', ep) is a full subgraph of Γ. Using a base vertex $x \in V'$, so that any $y \in V'$ is at finite distance to x, and the triangle inequality, we see that any two points of V' are at finite distance, i.e., (V', E', ep) is connected.

Moreover, since one can not connect elements of V' in Γ using edges others than those in E', we also see that the distance in Γ' is the restriction to $V' \times V'$ of d_Γ. □

Because of this construction, a number of classical invariants from metric geometry can be immediately "imported" into graph theory. We will consider in particular the *diameter*, and we recall the definition:

Definition 1.17 (Diameter of a graph)**.** Let Γ be a graph. The diameter of Γ, denoted $\mathrm{diam}(\Gamma)$, is the largest distance between two vertices in Γ, i.e., we have

$$\mathrm{diam}(\Gamma) = \sup_{x,y \in V} d_\Gamma(x,y) \in \{0,1,2,\dots\} \cup \{+\infty\}.$$

Example 1.18. If Γ is a finite connected, graph, its diameter will be finite. One of the key questions that the concept of expander graphs (hence, this book!) addresses is: given certain connected finite graphs, what can one say about their diameters? In particular, is this diameter relatively *small*, compared with the number of vertices?

We can immediately treat the obvious examples, among the graphs which were already described in Example 1.4:

- The path P_k has diameter k;
- The complete graph K_m has diameter 1 for $m \geqslant 2$ ($K_1 = P_0$ has diameter 0);
- The diameter of the complete bipartite graph $K_{m,n}$ is 2 if either m or n is $\geqslant 2$, while $\mathrm{diam}(K_{1,1}) = 1$;
- The diameter of the cycle C_m is given by

$$\mathrm{diam}(C_m) = \begin{cases} \frac{m}{2} & \text{if } m \text{ is even} \\ \frac{m-1}{2} & \text{if } m \text{ is odd.} \end{cases}$$

Checking rigorously these values is left to the reader as an exercise. For the graphs G_n of Example 1.4, (4), computing the diameter is not so easy. In Exercise 1.8, the reader will be invited to prove that $\mathrm{diam}(G_n) \asymp n^2$. Since $|G_n| = n!$, this means that

$$\mathrm{diam}(G_n) \asymp (\log |G_n|)^2,$$

hence the diameter is here rather small compared with the number of vertices.

1.3. **Cayley graphs.** We will now define the *Cayley graphs*, which are used to get a geometric vision of groups and their properties. These are among the most important examples of graphs for applications to number theory.

Definition 1.19 (Cayley graph)**.** Let G be a group and let $S \subset G$ be any subset which is *symmetric*, in the sense that $s \in S$ if and only if $s^{-1} \in S$. The *Cayley graph* of G with respect to S is the graph (V, E, ep) where the set of vertices is $V = G$, the edges are given by

$$E = \{\{g, gs\} \mid g \in G,\ s \in S\} \subset V^{(2)}$$

and ep is the inclusion map $E \to V^{(2)}$. This graph is denoted $\mathcal{C}(G, S)$.

In other words, to draw $\mathcal{C}(G, S)$, we use the elements of the group as vertices, and draw an edge between x and y if and only if $x^{-1}y \in S$; since S is symmetric, this is equivalent with $y^{-1}x \in S$. This graph is not always a simple graph: although it has no multiple edges, it may have loops. In fact, this happens if and only if $1 \in S$, in which case there is a loop at every vertex.

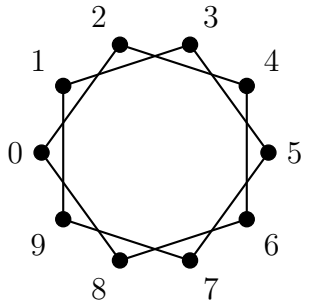
If S is finite, then $\mathcal{C}(G, S)$ is $|S|$-regular (there are $|S - \{1\}|$ edges from $g \in G$ with distinct extremities, because S is symmetric so $\{g, gs\} = \{gs, (gs)s^{-1}\}$, and one possible loop if $1 \in S$).

For a lively and insightful discussion of some of the many aspects of Cayley graphs that we will not discuss in this book, we refer to the book [39] of de la Harpe.

Example 1.20. (1) For $m \geqslant 3$, the cycle C_m can be seen as (i.e., it is isomorphic to) the Cayley graph $\mathcal{C}(\mathbf{Z}/m\mathbf{Z}, \{\pm 1\})$, as the reader is invited to check. For $m = 2$, this is not the case (because $1 = -1$ in $\mathbf{Z}/2\mathbf{Z}$); indeed, $\mathcal{C}(\mathbf{Z}/2\mathbf{Z}, \{1\})$ is isomorphic to P_2.

Similarly, for all $m \geqslant 2$, the complete graph K_m is also isomorphic to a Cayley graph of $\mathbf{Z}/m\mathbf{Z}$, but with respect to $S = \mathbf{Z}/m\mathbf{Z} - \{0\}$. This already shows that Cayley graphs can look quite different for the same group G when we change the set S.

(2) Here is a picture of the Cayley graph $\mathcal{C}(\mathbf{Z}/10\mathbf{Z}, \{\pm 2\})$:



Note that this graph is not connected.

(3) If $G = \mathbf{Z}$ and $S = \{\pm 1\}$, we obtain an infinite path (extending indefinitely in both directions).

(4) The graph G_n defined in Example 1.4, (4), is isomorphic to the Cayley graph of the symmetric group $\mathfrak{S}_n$ with respect to the (symmetric) subset

$$S_n = \{\tau, (1\ 2\ \cdots\ n)^{\pm 1}\}. \tag{1.2}$$

Indeed, if we use the deck of cards $D_n = \{1, \ldots, n\}$, the isomorphism (say f) maps $\sigma \in \mathfrak{S}_n$ to the arrangement $(\sigma(1), \ldots, \sigma(n))$ of the deck (read left-to-right as being top-to-bottom), which respects the edges: from

$$f(\sigma\tau) = (\sigma(2), \sigma(1), \sigma(3), \ldots, \sigma(n))$$

we see that the edge $\{\sigma, \sigma\tau\}$ corresponds to switching the first two cards, while

$$f(\sigma\sigma_n) = (\sigma(2), \sigma(3), \ldots, \sigma(n), \sigma(1))$$

and

$$f(\sigma\sigma_n^{-1}) = (\sigma(n), \sigma(1), \ldots, \sigma(n-1))$$

do correspond to putting the top card at the bottom, and conversely. We will simply refer to the graphs G_n as Cayley graphs from now on.

The reader should check visually that the graph G_4 is connected and bipartite. As we will soon see, these facts reflect some basic group-theoretic properties of $\mathfrak{S}_n$ and of S_n.

(5) Let $n \geqslant 2$ be an integer and let G be a free group on n generators $(a_1, \dots, a_n)$ (see for instance [39, Ch. II] for an introduction to free groups). The Cayley graph of G with respect to the symmetric set $S = \{a_1, a_1^{-1}, \dots, a_n, a_n^{-1}\}$ is isomorphic to the infinite $(2n)$-regular tree T_{2n} (Example 1.10). You should attempt to understand why this is so.

The geometric notions of the previous section are particularly interesting when applied to Cayley graphs. In particular, we have a group-theoretic interpretation of connectedness and of the distance in Cayley graphs:

Proposition 1.21 (Metric properties of Cayley graphs)**.** *Let G be a group and S a symmetric subset of G. Let $\Gamma = \mathcal{C}(G, S)$ be the corresponding Cayley graph.*

(1) *The Cayley graph Γ is connected if and only if S is a generating set of G.*

(2) *Denote $\|x\|_S = d_\Gamma(1, x)$. Then the distance d_Γ satisfies*

$$d_\Gamma(x, y) = \|x^{-1}y\|_S, \tag{1.3}$$

for all x, $y \in G = V_\Gamma$, and in particular it is left-invariant, i.e.

$$d_\Gamma(xy, xz) = d_\Gamma(y, z)$$

for all x, y, z in G. Moreover

$$\|x\|_S = \min\{k \geqslant 0 \mid x = s_1 \cdots s_k \text{ for some } s_i \in S\}, \tag{1.4}$$

which is called the word length *of x with respect to S.*

Proof. Statement (1) is intuitively clear, since paths in $\mathcal{C}(G, S)$ join two elements which differ by multiplication by an element in S, and we leave the proof to the reader.

(2) The formulas (1.3) and (1.4) are implicit in what was done before: given x, $y \in G$, there is for any $k \geqslant 0$ a bijection, which we just constructed, between paths $\gamma : P_k \longrightarrow \Gamma$ between x and y, and k-tuples $(s_1, \dots, s_k) \in S^k$ such that

$$y = xs_1s_2 \cdots s_k.$$

The minimal possible k for given x and y is the distance between x and y, so that (1.4) follows, and since the equation above is equivalent with $x^{-1}y = s_1 \cdots s_k$, this means also that

$$d_\Gamma(x, y) = \|x^{-1}y\|_S,$$

proving (1.3). □

Cayley graphs do not only give a geometric "representation" of groups, the construction is compatible with homomorphisms, i.e., with possible "relations" between groups: whenever we have a homomorphism

$$G \xrightarrow{f} H$$

of groups, and a subset $S \subset G$, we get an induced graph map

$$(f, f_*) : \mathcal{C}(G, S) \longrightarrow \mathcal{C}(H, f(S))$$

which is defined by the map f itself on the vertices, and by the definition

$$f_*(\{g, gs\}) = f(\{g, gs\}) = \{f(g), f(g)f(s)\}$$

(*"qui s'impose"*) for any edge $\{g, gs\} \in E_{\mathcal{C}(G,S)}$. Obviously, this association maps the identity to the identity of the Cayley graph, and is compatible with composition (in the

language of categories, it is a *functor*) on the category of groups with a subset. We also see that (f, f_*) is an embedding whenever f is injective.

Proposition 1.22. *Let G be a group, and let S be a symmetric generating set of G. The Cayley graph $\mathcal{C}(G, S)$ is bipartite if and only if there exists a surjective group homomorphism*

$$\varepsilon : G \longrightarrow \{\pm 1\}$$

such that $\varepsilon(s) = -1$ for all $s \in S$. (In particular, if $1 \in S$, the Cayley graph $\mathcal{C}(G, S)$ is not bipartite.)

The proof is left as an exercise.

Example 1.23. (1) Consider $G = \mathfrak{S}_n$, the symmetric group on n letters, and the generating set $S = \{$ transpositions in $G\}$. Then $\mathcal{C}(G, S)$ is bipartite, the corresponding homomorphism being the signature $\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}$.

(2) For the Cayley graphs $G_n = \mathcal{C}(\mathfrak{S}_n, S_n)$ discussed in Example 1.20, (3), note that we have $\varepsilon(\tau) = -1$, $\varepsilon((1\ 2 \cdots\ n)) = (-1)^{n-1}$, so that G_n is bipartite if and only if n is even. (For instance, this occurs for G_4, which we drew earlier.)

(3) The first two examples show that bipartiteness is not purely a condition on the group involved, but also depends on the choice of generators. In particular, in situations where having a bipartite graph is a problem (as happens with the behavior of random walks, as we will see in Section 1.5), one can often efficiently bypass the issue for a Cayley graph $\mathcal{C}(G, S)$ by considering instead $\mathcal{C}(G, S \cup \{1\})$, which is not bipartite. Graphically, adding 1 to S amounts to replacing the graph $\mathcal{C}(G, S)$ with the graph with the same vertices, but with an extra loop added at each vertex.

See Exercise 1.10 for the characterization of the girth of a Cayley graph.

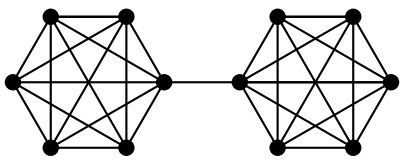
1.4. **Expansion.** In this section, we begin the study of *expansion properties* of graphs. This will lead to the definition of an expander family of graphs.

The goal is to find a quantitative invariant that can be used to measure a very high level of connectedness of a graph. Of course, assuming a graph is known to be connected, the diameter is the first natural invariant that comes to mind: for a fixed number of vertices, a graph with smaller diameter is "better connected".

However we also wish to be able to detect (using our invariant) that the graph is "robust", by which we mean that it can not be disconnected too easily.

For instance, consider a graph Γ_m given by taking the disjoint union of two copies Γ and Γ' of a complete graph K_m, for some $m \geqslant 2$, and adding a single edge between chosen vertices $x_1 \in \Gamma$ and $x_2 \in \Gamma'$:

(1.5)



We clearly have $\operatorname{diam}(\Gamma_m) = 3$, for any m, which shows that Γ_m has very small diameter. But if we remove the single additional edge between x_1 and x_2, we obtain a disconnected graph. This behavior is not desirable in many applications, and leads to the definition of the "expansion constant", or Cheeger constant, of a graph (the name is motivated by the geometric analogue defined by Cheeger in [22]).

Definition 1.24 (Expansion constant)**.** Let $\Gamma = (V, E, \mathrm{ep})$ be a finite graph.

(1) For any disjoint subsets of vertices V_1, $V_2 \subset V$, we denote by $\mathcal{E}(V_1, V_2)$ or $\mathcal{E}_\Gamma(V_1, V_2)$ the set of edges of Γ with one extremity in V_1 and one extremity in V_2,

$$\mathcal{E}(V_1, V_2) = \{\alpha \in E \mid \mathrm{ep}(\alpha) \cap V_1 \neq \emptyset, \quad \mathrm{ep}(\alpha) \cap V_2 \neq \emptyset\}.$$

and we denote by $\mathcal{E}(V_1)$ or $\mathcal{E}_\Gamma(V_1)$ the set $\mathcal{E}(V_1, V - V_1)$ of edges with one extremity in V_1, and one outside V_1.

(2) The *expansion constant* $h(\Gamma)$ is defined by

$$h(\Gamma) = \min\Big\{ \frac{|\mathcal{E}(W)|}{|W|} \in [0, +\infty[\;\Big|\; \emptyset \neq W \subset V \text{ and } |W| \leqslant \tfrac{1}{2}|\Gamma| \Big\},$$

with the convention that $h(\Gamma) = +\infty$ if Γ has at most one vertex.

In other words, $h(\Gamma)$ is the smallest possible ratio between the number of edges exiting from W and the size of W, when W is a set of vertices that is non-empty, but not too big. This will provide a measure of robustness, in the following sense: the larger $h(\Gamma)$ is, the more difficult it is to disconnect a largish subset of V from the rest of the graph. This is expressed in the following result:

Proposition 1.25. *Let $\Gamma = (V, E, \mathrm{ep})$ be a finite graph with at least two vertices, so that $h(\Gamma) < +\infty$.*

(1) We have $h(\Gamma) > 0$ if and only if Γ is connected.

(2) If $W \subset V$ is a subset of vertices with $|W| = \delta|V|$ where $0 < \delta \leqslant \frac{1}{2}$, one must remove at least $\delta h(\Gamma)|V|$ edges from Γ to disconnect W from the rest of the graph.

Proof. (1) The condition $h(\Gamma) = 0$ means that there exists some $W \subset V$, non-empty, of size $\leqslant |\Gamma|/2$, such that $\mathcal{E}(W)$ is empty. In particular $V - W$ is also of size $\geqslant 1$. Let $x \in W$ and $y \notin W$ be two vertices. Then there is no path in Γ between x and y, since such a path would have to cross from W to $V - W$ at some point (we leave as an exercise to make this rigorous). Therefore Γ is not connected.

Conversely, if Γ is not connected, there are at least two connected components in Γ, and at least one of them, say W, must have size $|W| \leqslant |\Gamma|/2$. Since W is not empty and $\mathcal{E}(W) = \emptyset$, we get $h(\Gamma) \leqslant |\mathcal{E}(W)|/|W| = 0$.

(2) Once we explain the meaning of the sentence, it will become clear: we say that removing a set C of edges disconnects W from $V - W$ if $\mathcal{E}(W) \subset C$, i.e., all edges that go from W to "somewhere else" are contained in C. Then since

$$|\mathcal{E}(W)| \geqslant h(\Gamma)|W| = \delta h(\Gamma)|V|,$$

by definition of $h(\Gamma)$, our statement is just a reformulation of the definition. □

Example 1.26. (1) Consider the complete graph K_m with $m \geqslant 2$ vertices. Any two subsets of the vertices with the same cardinality are equivalent (i.e., there is an automorphism of the graph mapping one to the other), and hence

$$h(K_m) = \min_{1 \leqslant j \leqslant m/2} \frac{1}{j} |\mathcal{E}(\{1, \dots, j\})| = \min_{1 \leqslant j \leqslant m/2} (m - j) = m - \left\lfloor \frac{m}{2} \right\rfloor$$

(since there are $j(m-j)$ edges in K_m from $\{1, \dots, j\}$ to its complement $\{j+1, \dots, m\}$).

(2) Consider now $\Gamma = C_m$, the cycle with $m \geqslant 2$ vertices. The subsets of size $\leqslant m/2$ that expand least are given by the images W of paths in C_m of length $\mathrm{diam}(C_m) = \lfloor \frac{m}{2} \rfloor \leqslant m/2$ (this is intuitively clear, and the proof is left as an exercise). In this case $\mathcal{E}(W)$ has two elements (one edge from each end of the path), and therefore

$$h(C_m) = \frac{2}{\lfloor \frac{m}{2} \rfloor} \leqslant \frac{4}{m-1}. \tag{1.6}$$

Note that the inequality $h(C_m) \leqslant 4/(m-1)$ follows, even if one does not know that paths are the least expanding subsets, since

$$h(C_m) \leqslant \frac{|\mathcal{E}(W)|}{|W|}$$

by definition for any subset W.

(3) Let Γ be a graph like the one in (1.5): two copies of K_m joined by a single edge α. Then if we take W to be the first copy of K_m, we see that $\mathcal{E}(W) = \{\alpha\}$, hence

$$h(\Gamma) \leqslant \frac{1}{m}.$$

(4) Let $T = T_{d,k}$ be a finite tree with degree $d \geqslant 3$ and depth $k \geqslant 1$. The expansion constant can be bounded from above by taking as subset W one of the subtrees "below a neighbor of the root", i.e., if x_0 is the root and x_1 is a vertex indexed with a single letter of the alphabet (e.g., $x_1 = 1$), we let

$$W = \bigcup_{2 \leqslant j \leqslant k} \{(1, s_2, \dots, s_j) \in V_T\}$$

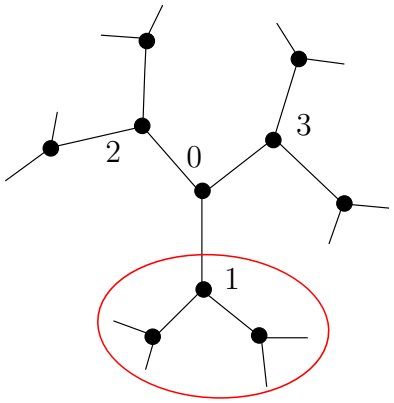
which (see Exercise 1.4, (4)), can be written equivalently as

$$W = \{y \in V_T \mid d_T(y, x_0) \geqslant d_T(y, 1)\}.$$

We then have $|W| = \frac{|T|-1}{d} \leqslant \frac{|T|}{2}$, and therefore

$$h(T) \leqslant \frac{|\mathcal{E}(W)|}{|W|}.$$

It is clear from the picture



that $\mathcal{E}(W)$ contains a *single* edge, the one joining 0 to 1 (in other words, to "escape" from the subtree induced by W, one *must* pass through the root), and therefore

$$h(T) \leqslant \frac{1}{|W|} = \frac{d}{|T|-1}.$$

These examples are already instructive. In particular, they show that $h(\Gamma)$ behaves in a way consistent with our goal: the "super"-connected complete graphs have $h(\Gamma)$ very large, while large, easily-disconnected graphs, like C_m or those of Example (3) have quite small expansion constants.

Although the arguments were highly elementary, they also show that it is much easier to give an upper-bound for $h(\Gamma)$ than a lower-bound: since the expansion constant is defined as a minimum, a single well-chosen subset W may lead to a good upper-bound, while we need to know which sets are the worst behaved in order to give a non-trivial lower-bound. This is confirmed by the wide gap in the following trivial bounds.

We now come to a proper result: we show that a large $h(\Gamma)$ implies that the diameter of a graph is relatively small. This means that the expansion constant does control this more natural-looking invariant.

Proposition 1.27 (Expansion and diameter)**.** *Let Γ be a finite non-empty connected graph. We have*

$$\operatorname{diam}(\Gamma) \leqslant 2\frac{\log \frac{|\Gamma|}{2}}{\log\Big(1+\frac{h(\Gamma)}{v}\Big)} + 3 \tag{1.7}$$

where $v = \max_{x\in V} \operatorname{val}(x)$ is the maximal valency.

The following lemma is the crucial step:

Lemma 1.28. *Let Γ be a finite non-empty connected graph and $x \in V$. For any $n \geqslant 0$, let $\mathcal{B}_x(n)$ be the ball of radius n around x, i.e.*

$$\mathcal{B}_x(n) = \{y \in V \mid d_\Gamma(x,y) \leqslant n\}.$$

Then, with v denoting the maximal valency of Γ, we have

$$|\mathcal{B}_x(n)| \geqslant \min\Big(\frac{|\Gamma|}{2}, \Big(1+\frac{h(\Gamma)}{v}\Big)^n\Big).$$

Proof. It is enough to show that if $n \geqslant 0$ is such that $|\mathcal{B}_x(n)| \leqslant |\Gamma|/2$, then we have

$$|\mathcal{B}_x(n+1)| \geqslant \Big(1+\frac{h(\Gamma)}{v}\Big)|\mathcal{B}_x(n)|,$$

since $\mathcal{B}_x(0) = \{x\}$. To prove this inequality, we observe simply that if $\alpha \in \mathcal{E}(\mathcal{B}_x(n))$ is an edge exiting from $\mathcal{B}_x(n)$, its extremity which is not in $\mathcal{B}_x(n)$ is in $\mathcal{B}_x(n+1) - \mathcal{B}_x(n)$, i.e., is at distance $n+1$ from x: this is a "new" point.

It is possible that multiple edges α starting from $\mathcal{B}_x(n)$ lead to the same y, but since all these edges share the extremity y, the maximal number of edges leading to y is $\operatorname{val}(y) \leqslant v$, so that

$$|\mathcal{B}_x(n+1) - \mathcal{B}_x(n)| \geqslant \frac{|\mathcal{E}(\mathcal{B}_x(n))|}{v} \geqslant \frac{h(\Gamma)}{v}|\mathcal{B}_x(n))|,$$

by definition of $h(\Gamma)$, using the assumption that $|\mathcal{B}_x(n)| \leqslant |\Gamma|/2$. Then we get

$$|\mathcal{B}_x(n+1)| = |\mathcal{B}_x(n)| + |\mathcal{B}_x(n+1) - \mathcal{B}_x(n)| \geqslant \Big(1+\frac{h(\Gamma)}{v}\Big)|\mathcal{B}_x(n)|,$$

as desired. □

Proof of Proposition 1.27. Let x, $y \in V$ be two arbitrary vertices; we are going to estimate $d_\Gamma(x,y)$ from above. For this, we denote

$$\beta = 1 + \frac{h(\Gamma)}{v},$$

and we denote by $n \geqslant 1$ the smallest integer such that

$$\beta^n \geqslant \frac{|\Gamma|}{2},$$

(which is possible since $\beta > 1$, in view of the connectedness of Γ). Then by Lemma 1.28, applied to x and y, we find that

$$|\mathcal{B}_x(n)| \geqslant \frac{|\Gamma|}{2}, \qquad |\mathcal{B}_y(n)| \geqslant \frac{|\Gamma|}{2}.$$

In fact, we must have $|\mathcal{B}_x(n+1)| > |\Gamma|/2$ (because either this is true for $\mathcal{B}_x(n)$, or else $|\mathcal{B}_x(n)| = |\Gamma|/2$ and then there are some vertices at distance $n+1$), and therefore

$$\mathcal{B}_x(n+1) \cap \mathcal{B}_y(n) \neq \emptyset,$$

which means that $d_\Gamma(x,y) \leqslant 2n+1$ by passing through an intermediate point z lying in this intersection...

Since x and y were arbitrary, we have $\operatorname{diam}(\Gamma) \leqslant 2n+1$, and since

$$n = \left\lceil \frac{\log \frac{|\Gamma|}{2}}{\log \beta} \right\rceil \leqslant \frac{\log \frac{|\Gamma|}{2}}{\log \beta} + 1,$$

we obtain the diameter bound that we stated. □

Now comes the most important definition of these lectures, that of expander graphs. This encapsulate the idea of graphs which are both relatively sparse and highly, and robustly, connected.

Definition 1.29 (Expander graphs)**.** A *family* $(\Gamma_i)_{i\in I}$ of finite non-empty connected graphs $\Gamma_i = (V_i, E_i, \mathrm{ep})$ is an *expander family*, or a *family of expanders*, if there exist constants $v \geqslant 1$ and $h > 0$, independent of i, such that:

(1) The number of vertices $|V_i|$ "tends to infinity", in the sense that for any $N \geqslant 1$, there are only finitely many $i \in I$ such that Γ_i has at most N vertices.

(2) For each $i \in I$, we have

$$\max_{x\in V_i} \mathrm{val}(x) \leqslant v,$$

i.e., the maximal valency of the graphs is bounded independently of i.

(3) For each $i \in I$, the expansion constant satisfies

$$h(\Gamma_i) \geqslant h > 0,$$

i.e., it is bounded away from 0 by a constant independent of i.

We will say that a pair (h, v) for which the two properties above hold are *expansion parameters* of the family.

Let us review these conditions. The first is, to some extent, a matter of convention: if Γ is a fixed non-empty connected graph, it has bounded valency, of course, as well as positive expansion constant, and hence a "constant" family with $\Gamma_i = \Gamma$ for all i would qualify as expanders if the number of vertices was allowed to remain bounded. But since our intuition is that a family of expanders should allow us to construct arbitrarily large graphs (measured with the number of vertices) which are "sparse" and "super-connected", it is not of interest to just repeat a single graph infinitely many times.

The second condition is our interpretation of sparsity. The point is that if the valency of vertices of a graph Γ is $\leqslant k$, the number of edges is controlled by the number of vertices, namely

$$|E_\Gamma| \leqslant k|V_\Gamma|.$$

The number of edges is seen here as a "cost" involved in constructing the graph. Bounding the valency means that we ensure that the cost scales linearly with the number of vertices.

Finally, the last condition is a connectedness and robustness assertion. It is natural in view of our examples and of Proposition 1.27. It is the best to hope for, since (for a graph with bounded valency), the Cheeger constant cannot not be unbounded.

The first important property of expander graphs is that they have small diameter:

Corollary 1.30 (Diameter of expanders)**.** *Let (Γ_i) be an expander family of graphs. Then we have*

$$\operatorname{diam}(\Gamma_i) \ll \log(3|\Gamma_i|)$$

for all i, where the implied constant depends only on the expansion parameters (h, v) of the family. [1]

Note that the examples of finite trees $T_{d,k}$, with $d \geqslant 3$ fixed, show that the converse to this statement is not true: the sequence $(T_{d,k})_{k\geqslant 1}$ is a sequence of graphs which have valency bounded by d, and diameter $2k \ll \log|T_{d,k}|$, but they are not expanders.

Proof. Let J be the set of the (finitely many) indices $i \in I$ such that $|\Gamma_i| \leqslant \frac{1}{3}e^3$. We apply Proposition 1.27: denoting

$$v = \max_{i\in I} \max_{x\in\Gamma_i} \operatorname{val}(x) < +\infty, \qquad h = \inf_{i\in I} h(\Gamma_i) > 0,$$

and

$$\xi = \frac{1}{\log(1 + h/v)} > 0,$$

we get first

$$\begin{aligned}\operatorname{diam}(\Gamma_i) \leqslant 2\xi \log(\tfrac{1}{2}|\Gamma_i|) + 3 &\leqslant 2\xi \log(\tfrac{1}{2}|\Gamma_i|) + \log(3|\Gamma_i|)\\ &\leqslant (2\xi + 1)\log(3|\Gamma_i|),\end{aligned}$$

for $i \notin J$. We can then get an estimate valid for all i, e.g., by writing $\operatorname{diam}(\Gamma_i) \leqslant C\log(3|\Gamma_i|)$ with

$$C = \max(2\xi + 1, \max_{j\in J} \operatorname{diam}(\Gamma_j)) \tag{1.8}$$

for all $i \in I$. □

This estimate is best possible, since it is not difficult to prove (see Exercise 1.12) that the diameter of a graph with bounded valency can not grow slower than the logarithm of the number of vertices.

Thus we see that, *if they exist*, expander families are essentially optimal graphs when it comes to combining sparsity and strong connectedness (or expansion) properties.

At this point, the most pressing question is: *do expanders really exist*? In all the easy examples of graphs (with bounded valency) for which we computed the expansion constant, it tends to 0 as the number of vertices goes to infinity, even in the case of finite trees where the diameter, at least, has the right order of magnitude. A pessimist's attitude might be that this is a bad sign.

An optimist might observe that, in the case of the "best" candidates so far (the finite trees $T_{d,k}$ with $d \geqslant 3$ fixed and $k \to +\infty$), there are many subsets of vertices which *do* have large expansion ratio $|\mathcal{E}(W)|/|W|$. Roughly speaking, as long as W is a set of vertices that only contains a few elements at the maximal distance k from the root of the tree, there will be many edges "escaping" further away from the root, in fact typically as many as the size of W. In other words, one might imagine that adding an edges to each of the far vertices, reconnecting them to the middle of the tree, *might* have a chance of producing graphs with good expansion constant.

We will not actually proceed this way; but, indeed, the optimists are in the right here: expanders do exist, and in fact exist in cheerful abundance. We will survey this

[1] We use $3|\Gamma_i|$ to avoid any problem with the possible exceptional i's where $|\Gamma_i| = 1$, and because $\log 3 \geqslant 1$; this is old analytic number theory lore...

in Lecture 3 using three different methods, in particular using probabilistic methods, as originally done by Barzdin and Kolmogorov [5], and independently by Pinsker [69].

However, what we will first do in the next lecture is to provide another equivalent definition of expander graphs, which is often more easily applicable and more natural in applications.

1.5. **Exercises.**

Exercise 1.1. (1) Let Γ be a finite d-regular graph with girth $g \geqslant 3$. Prove that

$$|\Gamma| \geqslant d(d-1)^{\lfloor (g-3)/2 \rfloor}.$$

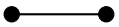
(2) Show that the girth of a finite graph d-regular graph Γ with $d \geqslant 3$ is $\ll \log(|\Gamma|)$, where the implied constant depends only on d.

Exercise 1.2. Show that the number of vertices and edges of the finite tree $T_{d,k}$ are given by

$$|T_{d,k}| = d\frac{(d-1)^k - 1}{d-2} + 1, \quad |E_{d,k}| = |T_{d,k}| - 1 = d\frac{(d-1)^k - 1}{d-2}$$

if $d \geqslant 3$, and $|T_{2,k}| = 2k+1$, $|E_{2,k}| = 2k$.

Exercise 1.3. Show that a graph $\Gamma = (V, E, \mathrm{ep})$ is bipartite if and only if there exists a graph map $\Gamma \longrightarrow P_1$, where P_1 is the path of length 1:



Exercise 1.4. We consider here some specific features of trees, which we recall are connected forests.

(1) Show that the diameter of a finite tree $T_{d,k}$ with $d \geqslant 2$ and $k \geqslant 0$ is equal to $2k$, and is achieved by the distance between any two distinct vertices labeled with words $(s_1, \ldots, s_k)$ and $(s'_1, \ldots, s'_k)$ of (maximal) length k with $s_1 \neq s'_1$.

(2) Show that if T is a tree, then for any two vertices x and y, there exists a unique geodesic on T with extremities x and y (the image of all paths of length $d_T(x,y)$ between two vertices x and y of T is the same).

(3) If $T = T_{d,k}$ with "root" vertex $x_0 = \emptyset$ and $0 \leqslant j \leqslant k$, show that

$$V' = \{x \in V_T \mid d_T(x_0, x) \leqslant j\}$$

induces a full subgraph isomorphic to $T_{d,j}$.

(4) If $T = T_{d,k}$ with root x_0 and $x \in T$ is any vertex, show that

$$V'' = \{y \in V_T \mid d_\Gamma(y, x_0) \geqslant d_\Gamma(y, x)\}$$

induces a full subgraph T'' of T which is also a tree.

(5) Let Γ be any graph with girth $\ell \geqslant 1$, and let $x_0 \in V$. Show that the subgraph of Γ induced by

$$V' = \left\{x \in V \mid d_\Gamma(x_0, x) < \frac{\ell}{2}\right\}$$

is a tree.

Exercise 1.5. Let Γ_1 and Γ_2 be graphs, and let $f : \Gamma_1 \longrightarrow \Gamma_2$ be a graph map. Show that f is always distance-decreasing, i.e., we have

$$d_{\Gamma_2}(f(x), f(y)) \leqslant d_{\Gamma_1}(x, y) \tag{1.9}$$

for any x, $y \in \Gamma_1$. In particular, if f is surjective on vertices, the diameter of Γ_2 is at most that of Γ_1, and if f is an isomorphism, it is isometric.

Exercise 1.6. Here is an application of graphs and connected components to group theory, due to Bauer and Knutson (see [33, Lemma, p. 98]). Let $k \geqslant 2$ be an integer, $G = \mathfrak{S}_k$ the symmetric group on k letters. We suppose given a subgroup H of G such that: (i) H acts transitively on $\{1, \ldots, k\}$; (ii) H contains at least one transposition; (iii) H contains a cycle of length $p > k/2$ such that p is *prime*. The goal is to prove that, in fact, we have $H = G = \mathfrak{S}_k$.

Let $\Gamma = (V, E)$ be the simple graph with $V = \{1, \ldots, k\}$ and with an edge between any pair $(i, j) \in V \times V$ such that $i \neq j$ and the transposition $(i\ j)$ is in H. Assumption (ii) means that the edge set is not empty.

(1) Show that any connected component in Γ is a complete graph.

(2) Show that it is enough to show that Γ is connected in order to prove that $H = G$.

(3) Show that the action of G on $\{1, \ldots, k\}$ induces an action of G on Γ by automorphisms. Show then that G acts transitively on the set of all connected components of Γ. Deduce that all such components are isomorphic.

(4) Show that a p-cycle $\sigma \in H$ as in (iii) must fix (globally, not necessarily pointwise) each component of Γ, and conclude from this.

Exercise 1.7 (Uniqueness of bipartite decompositions)**.** (1) Let Γ be a connected *bipartite* graph with a bipartite decomposition $V = V_0 \cup V_1$. If $x_0 \in V_0$, show that

$$V_0 = \{y \in V \mid \text{there is a path of even length joining } x \text{ to } y\}. \tag{1.10}$$

(2) Deduce that the partition of edges $V = V_0 \cup V_1$ which exhibits the bipartiteness of a connected bipartite graph is unique (i.e., if $W_0 \cup W_1$ is another such partition, we have $(W_0, W_1) = (V_0, V_1)$ or $(W_0, W_1) = (V_1, V_0)$).

(3) Let Γ be an arbitrary connected graph, and define W by the right-hand side in (1.10). Compute W when Γ is *not* bipartite.

(4) Show that a forest is always bipartite.

(5) Show that if a graph Γ is finite and *not* bipartite, then its girth is finite. In fact, show that $\mathrm{girth}(\Gamma) \leqslant 2\,\mathrm{diam}(\Gamma) + 1$, and that this is best possible.

Exercise 1.8. Prove that the set S_n given by (1.2) generates $\mathfrak{S}_n$, and hence that the graphs G_n of Example 1.20, (3), are all connected. In fact, show that there exist constants $c > 0$ and $C > 0$ such that the diameter of G_n satisfies

$$cn^2 \leqslant \mathrm{diam}(G_n) \leqslant Cn^2 \tag{1.11}$$

for all $n \geqslant 3$. [Hint: This is a fairly classic exercise. As described by Diaconis and Saloff-Coste [26, §3, Ex. 1], it can be convenient to think of this in terms of card shuffling.]

Exercise 1.9. Let G be a group, and let S be a symmetric generating set of G. Show that $\mathcal{C}(G, S)$ is bipartite if and only if there exists a surjective group homomorphism

$$\varepsilon : G \longrightarrow \{\pm 1\}$$

such that $\varepsilon(s) = -1$ for all $s \in S$. (In particular, if $1 \in S$, the Cayley graph $\mathcal{C}(G, S)$ is not bipartite.)

Exercise 1.10. Let G be a group and $S \subset G$ a symmetric subset *which does not contain a non-trivial involution*.

(1) Let $\Gamma = \mathcal{C}(G, S)$ be the corresponding Cayley graph. Show that the girth of Γ is then equal to the length of the shortest non-trivial relation among the elements of S, namely $\mathrm{girth}(\Gamma)$ is the smallest $m \geqslant 1$ for which there exist $(s_1, \ldots, s_m)$ in S, with $s_i s_{i+1} \neq 1$ for all i, such that $s_1 s_2 \cdots s_m = 1$. (In particular, if G is finite, the girth of the Cayley graph Γ is finite.)

(2) Show that the restriction on S is needed (a very simple example suffices).

Exercise 1.11. For any finite connected graph Γ with at least two vertices, show that

$$\frac{2}{|\Gamma|} \leqslant h(\Gamma) \leqslant \min_{x \in V} \mathrm{val}(x).$$

Exercise 1.12. Let Γ be a non-empty finite graph with maximal valency $\leqslant k$, where $k \geqslant 1$ is an integer. Show that

$$\mathrm{diam}(\Gamma) \geqslant \frac{\log(|\Gamma|)}{\log k}.$$

Exercise 1.13. Let (Γ_i) be an expander family. Show that the metric balls in Γ_i are uniformly exponentially expanding, in the sense that there exists $\gamma > 1$, independent of i, such that for any graph Γ_i in the family, we have

$$|\mathcal{B}_x(n)| \geqslant \min\Big(\frac{|\Gamma|}{2}, \gamma^n\Big),$$

for all $x \in \Gamma_i$ and $n \geqslant 0$.

Exercise 1.14 (Some Cayley graphs of $\mathfrak{S}_n$)**.** We consider again the Cayley graphs $G_n = \mathcal{C}(\mathfrak{S}_n, S_n)$ of Example 1.20. Could (G_n) be an expander family? For the moment, we only know an upper bound (1.11) for the diameter that is a bit too weak, but is not very far off from the estimate

$$\mathrm{diam}(G_n) \ll \log|G_n| \ll n \log n$$

that would be necessary for an expander. However, we will see here concretely that (G_n) is *not* an expander.

It is convenient here to see $\mathfrak{S}_n$ as acting by permutations of $\mathbf{Z}/n\mathbf{Z}$. With this interpretation, the generators σ_n and σ_n^{-1} act on $\mathbf{Z}/n\mathbf{Z}$ by

$$\sigma_n(i) = i + 1, \qquad \sigma_n^{-1}(i) = i - 1$$

for $i \in \mathbf{Z}/n\mathbf{Z}$.

Define then

$$W_n = \{\sigma \in \mathfrak{S}_n \mid \text{ there is no } i \in \mathbf{Z}/n\mathbf{Z} \text{ such that } \sigma(i+1) = \sigma(i) + 1\} \subset \mathfrak{S}_n.$$

(1) Show that

$$\frac{|\mathcal{E}(W_n)|}{|\mathfrak{S}_n|} \ll \frac{1}{n}.$$

(2) Show that

$$\frac{1}{3} \leqslant \liminf_{n \to +\infty} \frac{|W_n|}{|\mathfrak{S}_n|} \leqslant \limsup_{n \to +\infty} \frac{|W_n|}{|\mathfrak{S}_n|} \leqslant \frac{1}{2},$$

and conclude that $h(G_n)) \ll n^{-1}$. [Hint: You can use inclusion-exclusion.]

Lecture 2: spectral definition

In this second lecture, we explain a different equivalent (or essentially equivalent) definition of expander graphs, based on discrete spectral theory. There are in fact two very closely related variants of this definition, depending on the way one wishes to normalize the underlying analogue of the Laplace operator. We concentrate on the approach based on the so-called Markov operator, which is very closely related to probabilistic aspects (especially random walks on graphs), although we will not discuss this in detail.

We will consider spectral theory only finite graphs for simplicity.

2.1. **The Markov operator.**

Definition 2.1 (Measure and functions on a graph)**.** Let $\Gamma = (V, E, \mathrm{ep})$ be a finite graph with V and E non-empty, without isolated vertex.

(1) The (normalized) graph measure on Γ is the probability measure on V defined by

$$\mu_\Gamma(\{x\}) = \frac{\mathrm{val}(x)}{N}$$

for all $x \in V$, where

$$N = \sum_{x \in V} \mathrm{val}(x) > 0.$$

(2) The space of functions on Γ is the space $L^2(\Gamma, \mu_\Gamma)$, i.e., it is the vector space of all functions $\varphi : \Gamma \to \mathbf{C}$, with the inner product

$$\langle \varphi_1, \varphi_2 \rangle = \frac{1}{N} \sum_{x \in V} \mathrm{val}(x) \varphi_1(x) \overline{\varphi_2(x)}.$$

Remark 2.2. (1) If Γ is d-regular for some $d \geqslant 1$, then the measure μ_Γ is simply the normalized probability counting measure on V, namely

$$\mu_\Gamma(W) = \frac{|W|}{|V|}$$

for all $W \subset V$. This case will in fact occur very often, so the reader may read the remainder of this lecture with this case in mind. Note the comparison relation

$$\frac{v_-}{v_+} \frac{|W|}{|V|} \leqslant \mu_\Gamma(W) \leqslant \frac{v_+}{v_-} \frac{|W|}{|V|} \tag{2.1}$$

for all $W \subset V$, where

$$v_- = \min_{x \in V} \mathrm{val}(x), \qquad v_+ = \max_{x \in V} \mathrm{val}(x).$$

(2) Finally, we will also have the occasion to use the supremum norm

$$\|\varphi\|_\infty = \max_{x \in V} |\varphi(x)|$$

for $\varphi \in L^2(\Gamma, \nu_\Gamma)$.

Note that we can compare the two norms by

$$\|\varphi\| \leqslant \|\varphi\|_\infty \leqslant \Big(\frac{N}{v_-}\Big)^{1/2} \|\varphi\|, \tag{2.2}$$

where the left-hand inequality is a classical fact which holds for any probability measure, while the right-hand inequality follows from

$$\max |\varphi(x)|^2 \leqslant \frac{1}{v_-} \sum_{x \in V} \mathrm{val}(x) |\varphi(x)|^2 = \frac{N}{v_-} \|\varphi\|^2.$$

Definition 2.3. Let $\Gamma = (V, E, \mathrm{ep})$ be a finite graph with no isolated vertex. The *Markov averaging operator* on $L^2(\Gamma, \mu_\Gamma)$ is the linear map

$$M_\Gamma \ : \ \left\{ \begin{array}{ccc} L^2(\Gamma,\mu_\Gamma) & \longrightarrow & L^2(\Gamma,\mu_\Gamma) \\ \varphi & \mapsto & M_\Gamma\varphi \end{array} \right.$$

such that

$$(M_\Gamma\varphi)(x) = \frac{1}{\mathrm{val}(x)} \sum_{\substack{\alpha\in E \\ \mathrm{ep}(\alpha)=\{x,y\}}} \varphi(y) = \frac{1}{\mathrm{val}(x)} \sum_{\substack{y\in V \\ d_\Gamma(x,y)\leqslant 1}} a(x,y)\varphi(y).$$

We will often simply write M instead of M_Γ when only one graph is involved.

We note that the condition $d_\Gamma(x, y) \leqslant 1$ can be omitted in the second expression for $M\varphi$, since the quantity

$$a(x, y) = |\{\alpha \in E \mid \mathrm{ep}(\alpha) = \{x, y\}\}|$$

is zero unless $d_\Gamma(x, y) \leqslant 1$.

The choice of the measure μ_Γ on a graph is important, because the self-adjointness property of M depends on it.

Proposition 2.4 (Spectral properties of the Markov operator)**.** *Let $\Gamma = (V, E, \mathrm{ep})$ be a finite graph with no isolated vertex. Let M be the Markov averaging operator for Γ.*

(1) *For any function $\varphi \in L^2(\Gamma, \mu_\Gamma)$, we have*

$$\langle(\mathrm{Id} - M)\varphi, \varphi\rangle_\Gamma = \frac{1}{2N} \sum_{x,y\in V} a(x, y)|\varphi(x) - \varphi(y)|^2, \tag{2.3}$$

$$\langle(\mathrm{Id} + M)\varphi, \varphi\rangle_\Gamma = \frac{1}{2N} \sum_{x,y\in V} a(x, y)|\varphi(x) + \varphi(y)|^2. \tag{2.4}$$

(2) *The operator M is self-adjoint of norm $\leqslant 1$. It is bounded from above by the identity and from below by minus the identity.*

Part (2) combines three assertions: first, we have

$$\langle M\varphi_1, \varphi_2\rangle_\Gamma = \langle\varphi_1, M\varphi_2\rangle_\Gamma$$

for any functions φ_1, $\varphi_2 \in L^2(\Gamma, \mu_\Gamma)$ (self-adjointness), next, we have $\|M\varphi\|_\Gamma \leqslant \|\varphi\|$ for $\varphi \in L^2(\Gamma, \mu_\Gamma)$ (norm at most 1), and finally we have

$$-\langle\varphi, \varphi\rangle_\Gamma \leqslant \langle M\varphi, \varphi\rangle_\Gamma \leqslant \langle\varphi, \varphi\rangle_\Gamma \tag{2.5}$$

for all $\varphi \in L^2(\Gamma, \mu_\Gamma)$.

Proof. We start by proving the self-adjointness, which is a key property (ultimately, it relates to the fact that we are working with *unoriented* graphs). We have by definition

$$\begin{aligned} \langle M\varphi_1, \varphi_2\rangle_\Gamma &= \frac{1}{N} \sum_{x\in V} \mathrm{val}(x)(M\varphi_1)(x)\overline{\varphi_2(x)} \\ &= \frac{1}{N} \sum_{x\in V} \overline{\varphi_2(x)} \sum_{y\in V} \varphi_1(y)a(x, y) \\ &= \frac{1}{N} \sum_{x,y\in V} a(x, y)\varphi_1(y)\overline{\varphi_2(x)} \end{aligned} \tag{2.6}$$

and since $a(x, y) = a(y, x)$, this is also $\langle\varphi_1, M\varphi_2\rangle_\Gamma$.

We now prove the formulas (2.3) and (2.4). Both are very similar and we deal only with the first one. Using (2.17), the symmetry of the adjacency matrix and (2.6), we have

$$2N(\langle\varphi,\varphi\rangle_\Gamma - \langle M\varphi,\varphi\rangle_\Gamma) = 2\sum_{x,y\in V} a(x,y)|\varphi(x)|^2 - 2\sum_{x,y\in V} a(x,y)\varphi(x)\overline{\varphi(y)}$$

$$= \sum_{x,y\in V} a(x,y)|\varphi(x)|^2 + \sum_{x,y\in V} a(x,y)|\varphi(y)|^2 - 2\sum_{x,y\in V} a(x,y)\varphi(x)\overline{\varphi(y)}$$

which is equal to

$$\sum_{x,y\in V} a(x,y)|\varphi(x)-\varphi(y)|^2$$

These formulas (2.3) and (2.4) immediately imply (2.5). From this, we get

$$|\langle M\varphi,\varphi\rangle_\Gamma| \leqslant \|\varphi\|^2$$

for all $\varphi \in L^2(\Gamma,\mu_\Gamma)$, and since it is standard that

$$\|M\| = \sup_{\varphi\neq 0} \frac{|\langle M\varphi,\varphi\rangle_\Gamma|}{\|\varphi\|^2}$$

for a self-adjoint operator, this gives $\|M\| \leqslant 1$. □

Corollary 2.5. *Let $\Gamma = (V,E,\mathrm{ep})$ be a finite graph with no isolated vertex.*

(1) *The Markov operator M is diagonalizable in an orthonormal basis of $L^2(\Gamma,\mu_\Gamma)$, its eigenvalues are real numbers, and all eigenvalues have absolute value at most 1. For $\varphi \in L^2(\Gamma,\mu_\Gamma)$, we have*

$$\langle M\varphi_1,\varphi_2\rangle = \frac{1}{N}\sum_{x,y\in V} a(x,y)\varphi_1(y)\overline{\varphi_2(x)}. \tag{2.7}$$

(2) *The 1-eigenspace $\ker(M-1)$ of M has dimension equal to the number of connected components of Γ, and is spanned by the characteristic functions of these connected components. In particular, if Γ is connected, then we have $\ker(M-1) = \mathbf{C}$, spanned by constant functions.*

(3) *If Γ is connected, the (-1)-eigenspace $\ker(M+1)$ is zero* unless *Γ is bipartite. In that case, it is one-dimensional and spanned by a function $\varepsilon_\pm$ equal to 1, resp. -1, on the set of inputs, resp. outputs, of a bipartite decomposition of V.*

(4) *If Γ is bipartite, then the spectrum of M is symmetric: if λ is an eigenvalue of M, then so is $-\lambda$.*

Proof. (1) Since Γ is finite, the space $L^2(\Gamma,\mu_\Gamma)$ is finite-dimensional, so by linear algebra, the endomorphism M is diagonalizable in an orthonormal basis of $L^2(\Gamma,\mu_\Gamma)$, and its eigenvalues are real. The formula (2.7) restates (2.6).

(2) We next investigate the structure of $\ker(M-1)$ using (2.3), though there is a nice "geometric" computation also (see the exercise below). If $M\varphi = \varphi$, we get immediately the identity

$$\sum_{x,y\in V} a(x,y)|\varphi(x)-\varphi(y)|^2 = 0,$$

from (2.3). By positivity, this is equivalent with $\varphi(x) = \varphi(y)$ whenever $a(x,y) \neq 0$, i.e., φ has the same value at all extremities of any edge. If we fix any $x_0 \in V$, and use induction on $d_\Gamma(x_0,x)$, we get $\varphi(x) = \varphi(x_0)$ for all x reachable by a path from x_0. This means that φ is constant on each connected component of Γ. The converse is easy: if φ is constant

on each connected component, the definition shows that it does satisfy $M\varphi = \varphi$. Hence $\ker(M-1)$ is the space spanned by characteristic functions of connected components in the graph.

(3) We deal similarly with the possible -1 eigenvalue, for which we restrict our attention to connected graphs for simplicity. The reader should first check that, if Γ is bipartite, then the function $\varepsilon_\pm$ defined in the statement of the theorem is indeed in $\ker(M+1)$. We now proceed to show that it generates the (-1)-eigenspace.

Let φ be such that $M\varphi = -\varphi$. We get from (2.4) that

$$\varphi(x) = -\varphi(y)$$

for all x and y connected by an edge. If $\gamma : P_2 \longrightarrow \Gamma$ is any path of length 2 with $\gamma(0) = x$, $\gamma(2) = y$, it follows that

$$\varphi(x) = -\varphi(\gamma(1)) = \varphi(y).$$

Iterating, we obtain $\varphi(x) = \varphi(\gamma(2k))$ for any path γ of even length $2k$. Now we fix some $x_0 \in V$, and let W be the set of vertices in Γ which are the other extremity of a path $\gamma : P_{2k} \longrightarrow \Gamma$ of even length with $\gamma(0) = x_0$ (in particular, $x_0 \in W$ using a path of length 0). We see that φ is constant, equal to $\varphi(x_0)$, on all of W. If $W = V$, it follows that φ is constant, hence $M\varphi = \varphi = -\varphi$, so $\varphi = 0$.

On the other hand, if $W \neq V$, we claim that $V_0 = W$, $V_1 = V - W$ is a bipartite partition of V. Indeed, let $\alpha \in E$ be an edge with extremities $\{x_1, x_2\}$. It is not possible that x_1 and x_2 are both in V_0: if that were to happen, then given any $y \in V_1$, we would get a path of even length joining x_0 to y by (1) going from x_0 to x_1 with a path of even length $2\ell_1$ (possible since $x_1 \in V_0$); (2) going to x_1 to x_2 by the path of length 1 given by α; (3) going from x_2 to x_0 with a path of even length $2\ell_2$ (again, because $x_2 \in V_0$); (4) going from x_0 to y, which is possible since Γ is connected, and possible with odd length $2\ell_3 + 1$ since $y \notin V_0$: the total length is

$$2\ell_1 + 1 + 2\ell_2 + 2\ell_3 + 1 \equiv 0 \,(\mathrm{mod}\, 2).$$

This contradicts the fact that $V_0 = W \neq V$. Similarly, we see that x_1, x_2 can not both be in V_1, and this concludes the proof that Γ is bipartite. It is now easy to finish determining φ: it is constant, equal to $\varphi(x_0)$, on V_0, and for any $x \in V_1$, finding $y \in V_0$ connected by an edge, we get $\varphi(y) = -\varphi(x) = -\varphi(x_0)$. Thus it is equal to $\varphi(x_0)\varepsilon_\pm$.

(4) Assume that Γ is bipartite with bipartite partition $V = V_1 \cup V_2$. Whenever $\varphi : V \to \mathbf{C}$ is a λ-eigenfunction of M, it follows that $\tilde{\varphi}$ defined by $\tilde{\varphi}(x) = \varphi(x)$ for $x \in V_1$ and $\tilde{\varphi}(x) = -\varphi(x)$ for $x \in V_2$ is a $-\lambda$-eigenfunction of M. □

We following invariant will turn out to provide the tool to characterize expanders.

Definition 2.6 (Equidistribution radius)**.** Let $\Gamma = (V, E, \mathrm{ep})$ be a connected non-empty finite graph without isolated vertices. The *equidistribution radius* of Γ, denoted ϱ_Γ, is the maximum of the absolute values $|\lambda|$ for λ an eigenvalue of M which is different from ± 1. Equivalently, ϱ_Γ is the spectral radius of the restriction of M to the subspace

$$L^2_0(\Gamma, \mu_\Gamma) = (\ker(M-1) \oplus \ker(M+1))^\perp,$$

i.e., (1) if Γ is not bipartite, the restriction to the space of $\varphi \in L^2(\Gamma, \mu_\Gamma)$ such that

$$\langle \varphi, 1 \rangle = \frac{1}{N} \sum_{x \in V} \mathrm{val}(x)\varphi(x) = 0,$$

and (2) if Γ is bipartite with bipartite partition $V_0 \cup V_1 = V$, the restriction to the space of $\varphi \in L^2(\Gamma, \mu_\Gamma)$ such that

$$\frac{1}{N}\sum_{x\in V} \mathrm{val}(x)\varphi(x) = 0, \qquad \frac{1}{N}\sum_{x\in V_0} \mathrm{val}(x)\varphi(x) = \frac{1}{N}\sum_{x\in V_1} \mathrm{val}(x)\varphi(x).$$

The equivalence of the stated definitions of ϱ_Γ, and of the subspace $L^2_0(\Gamma, \mu_\Gamma)$, are direct consequences of Proposition 2.4 (taking into account the assumption that Γ is connected). The following are also almost part of the definition:

Lemma 2.7. *Let $\Gamma = (V, E, \mathrm{ep})$ be a connected, non-empty, finite graph without isolated vertices. We have $0 \leqslant \varrho_\Gamma < 1$ and ϱ_Γ is given by*

$$\varrho_\Gamma = \max_{0\neq\varphi\in L^2_0(\Gamma,\mu_\Gamma)} \frac{|\langle M\varphi, \varphi\rangle|}{\|\varphi\|^2}. \tag{2.8}$$

Proof. The inequality $\varrho_\Gamma < 1$ simply expresses the fact that M is self-adjoint with real eigenvalues of absolute value at most 1, so that, on the orthogonal complement $L^2_0(\Gamma, \mu_\Gamma)$ of the space spanned by the eigenspaces for ± 1, all eigenvalues have modulus < 1.

Similarly, the restriction of the self-adjoint operator M to $L^2_0(\Gamma, \mu_\Gamma)$ is self-adjoint, and its norm is ϱ_Γ. The formula (2.8) is then a standard property of endomorphisms of Hilbert spaces. □

2.2. **The Markov operator and expansion.** As promised, we will now describe the precise link between the expansion constant $h(\Gamma)$ and the equidistribution radius ϱ_Γ of a finite graph. As we mentioned already, there is a technical point to address. Indeed, being or not bipartite (or "very close", in the sense that there is an eigenvalue of the Markov operator M that is very close to -1) is a property essentially unrelated to being an expander, but it affects ϱ_Γ. This is clarified by the next definition:

Definition 2.8 ("Absolute Expanders")**.** Let (Γ_i) be a family of finite, non-empty, connected graphs $\Gamma_i = (V_i, E_i, \mathrm{ep})$ with maximal valency $\leqslant v$ for all i, such that the number of vertices of Γ_i tends to infinity, in the same sense as in Definition 1.29. We say that (Γ_i) is a family of *absolute expanders* if and only if there exists $\varrho < 1$ such that

$$\varrho_{\Gamma_i} \leqslant \varrho < 1 \tag{2.9}$$

for all $i \in I$.

The precise link between expanders and absolute expanders is the content of the following result:

Theorem 2.9 (Spectral definition of expanders)**.** (1) *A family of absolute expanders is an expander family.*

(2) *Conversely, let (Γ_i) be an expander family with $\Gamma_i = (V_i, E_i, \mathrm{ep})$. Let $\widetilde{\Gamma}_i$ be the "relaxed" graphs obtained from Γ_i by adding a loop at each vertex, i.e.,*

$$\widetilde{\Gamma}_i = (V_i, E_i \cup V_i, \mathrm{ep}')$$

with $\mathrm{ep}'(\alpha) = \mathrm{ep}(\alpha)$ for $\alpha \in E_i$ and $\mathrm{ep}'(x) = \{x\}$ for $x \in V_i$. Then $(\widetilde{\Gamma}_i)$ is a family of absolute expanders.

Remark 2.10. Since the vertices do not change, and only loops are added to the edges of the relaxed graphs, which has no effect on the value of $\mathcal{E}(W_1, W_2)$ for any subsets W_1, $W_2 \subset V$, we have $h(\widetilde{\Gamma}_i) = h(\Gamma_i)$.

Moreover, we only add one loop for each vertex, so that the maximal valency of the relaxed graphs has only been increased by 1. In particular, we see that (Γ_i) is an expander

family *if and only if* $(\widetilde{\Gamma}_i)$ is an expander family. On the other hand, because we added loops, $\widetilde{\Gamma}_i$ is not bipartite, and hence -1 is not an eigenvalue of M. In fact, having added loops to all vertices allows us quite easily to show that there is no eigenvalue of M too close to -1, and this explains why the relaxed family behaves better with respect to ϱ_Γ.

In fact, more is true: there are quantitative two-sided inequalities relating $h(\Gamma)$ and ϱ_Γ, from which the statement will immediately follow with relations between the expansion and equidistribution parameters.

By definition, ϱ_Γ is either the largest eigenvalue < 1 of M, or the negative of the smallest eigenvalue which is > -1. A convenient way to express this is to give names to the distance of the largest and smallest eigenvalues to 1 and -1.

Definition 2.11 (Normalized spectral gaps)**.** Let Γ be a finite non-empty connected graph. The *normalized spectral gap* $\boldsymbol{\lambda}_1(\Gamma)$ is the smallest non-zero eigenvalue of $\mathrm{Id} - M$. The *complementary normalized spectral gap* $\boldsymbol{\mu}_1(\Gamma)$ is the smallest non-zero eigenvalue of $\mathrm{Id} + M$.

The largest eigenvalue < 1 of M is therefore $1 - \boldsymbol{\lambda}_1$, and the smallest > -1 is $-1 + \boldsymbol{\mu}_1$. Thus we have

$$\varrho_\Gamma = \max(1 - \boldsymbol{\lambda}_1(\Gamma), \boldsymbol{\mu}_1(\Gamma) - 1).$$

Moreover we have

$$\boldsymbol{\lambda}_1(\Gamma) = \min_{0 \neq \varphi \perp 1} \frac{\langle (\mathrm{Id} - M)\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle} \tag{2.10}$$

$$= \min_{\varphi \text{ not constant}} \frac{\langle (\mathrm{Id} - M)\varphi, \varphi \rangle}{\|\varphi - \langle \varphi, \varphi \rangle\|^2}, \tag{2.11}$$

where the equality between these two characterizations follows from the fact that

$$\langle (\mathrm{Id} - M)\varphi, \varphi \rangle = \langle (\mathrm{Id} - M)\varphi_0, \varphi_0 \rangle$$

for $\varphi_0 = \varphi - \langle \varphi, 1 \rangle$, which is orthogonal to 1, so that the range of values in the minimum in the second definition is in fact identical to the one in the first.

The link between $h(\Gamma)$ and equidistribution becomes visible here. First by comparing with the definition of the expansion constant, also as a minimum, and then by using (2.3) which shows that the numerator is determined by the difference in values of φ on adjacent vertices, so that suitable choices of φ lead to the quantity $\mathcal{E}(W)$, as the following lemma shows:

Lemma 2.12. *Let Γ be a finite non-empty graph without isolated vertices. Let $W \subset V$ be a subset of vertices, $W' = V - W$, and let*

$$\varphi = \mathbf{1}_W - \mu_\Gamma(W),$$

the "centered" characteristic function of W. Then

$$\langle (\mathrm{Id} - M)\varphi, \varphi \rangle = \langle (\mathrm{Id} - M)\mathbf{1}_W, \mathbf{1}_W \rangle = \frac{|\mathcal{E}(W)|}{N}$$

and $\|\varphi\|^2 = \mu_\Gamma(W)\mu_\Gamma(W')$.

Proof. The formula (2.3) gives

$$\langle (\mathrm{Id} - M)\varphi, \varphi \rangle = \frac{1}{2N} \sum_{x,y \in V} a(x,y)(\varphi(x) - \varphi(y))^2$$

hence

$$\langle (\mathrm{Id} - M)\varphi, \varphi\rangle = \frac{1}{2N}\sum_{x,y\in V} a(x,y)(\mathbf{1}_W(x) - \mathbf{1}_W(y))^2.$$

The only non-zero terms in this sum are those where, on the one hand, x and y are adjacent, and on the other hand, one of them is in W and the other is not. The two cases $x \in W$, $y \notin W$ and $x \notin W$, $y \in W$ have equal contribution, and hence

$$\langle (\mathrm{Id} - M)\varphi, \varphi\rangle = \frac{1}{N}\sum_{\substack{x\in W\\ y\notin W}} a(x,y) = \frac{|\mathcal{E}(W)|}{N}.$$

The formula for $\|\varphi\|^2$ is a simple computation: since φ is orthogonal to constants, we have

$$\|\varphi\|^2 = \|\mathbf{1}_W\|^2 - \mu_\Gamma(W)^2 = \mu_\Gamma(W) - \mu_\Gamma(W)^2 = \mu_\Gamma(W)\mu_\Gamma(W').$$

□

We can now immediately prove (1) in Theorem 2.9. Indeed, it follows from the next proposition, which is the analogue for graphs of the Cheeger inequality for manifolds [22].

Proposition 2.13 (Discrete Cheeger inequality)**.** *Let $\Gamma = (V, E, \mathrm{ep})$ be a connected, non-empty, finite graph without isolated vertices. We have*

$$1 - \varrho_\Gamma \leqslant \boldsymbol{\lambda}_1(\Gamma) \leqslant \Big(\frac{2v_+}{v_-^2}\Big) h(\Gamma) \tag{2.12}$$

where, as before, we denote

$$v_- = \min_{x\in V} \mathrm{val}(x), \qquad v_+ = \max_{x\in V} \mathrm{val}(x).$$

In particular, if Γ is d-regular, then we have

$$1 - \varrho_\Gamma \leqslant \boldsymbol{\lambda}_1(\Gamma) \leqslant \frac{2}{d} h(\Gamma).$$

Proof. Because of (2.10), we can estimate $\boldsymbol{\lambda}_1(\Gamma)$ from above by

$$\boldsymbol{\lambda}_1(\Gamma) \leqslant \frac{\langle (\mathrm{Id} - M)\varphi, \varphi\rangle}{\langle \varphi, \varphi\rangle}$$

for any suitable function φ orthogonal to 1. Applying Lemma 2.12 to a non-empty subset $W \subset V$ with $|W| \leqslant |\Gamma|/2$ such that $h(\Gamma) = |\mathcal{E}(W)|/|W|$, we get

$$\boldsymbol{\lambda}_1(\Gamma) \leqslant \frac{|\mathcal{E}(W)|}{N}\frac{1}{\|\varphi\|^2} = \frac{1}{N}\frac{|\mathcal{E}(W)|}{\mu_\Gamma(W)\mu_\Gamma(W')}.$$

We now use (2.1) in order to make the exact ratio $|\mathcal{E}(W)|/|W|$ appear, obtaining

$$N\mu_\Gamma(W)\mu_\Gamma(W') \geqslant v_-|W| \times \frac{v_-}{v_+}\frac{|W'|}{|V|} \geqslant \frac{v_-^2}{2v_+}|W|,$$

and the inequality (2.12) follows. □

Remark 2.14. The Cheeger inequality is very often the best way to obtain lower bounds for the expansion constant of a graph. It is also useful numerically: since $\boldsymbol{\lambda}_1(\Gamma)$ is an eigenvalue of the linear operator $\mathrm{Id} - M$ acting on $L^2(\Gamma)$, which is a finite-dimensional vector space, of dimension $|V|$, the problem of determining $\boldsymbol{\lambda}_1(\Gamma)$ (or indeed ϱ_Γ itself) is a problem *of linear algebra*. Of course, if V has enormous size, it might not be feasible to find all eigenvalues, but the fact that ϱ_Γ is the largest absolute value of any eigenvalue on $L^2_0(\Gamma, \mu_\Gamma)$ also leads to the possibility of applying various approximation algorithms for this specific problem.

We will now investigate the converse of (2.12). We may note already that it can not be a simple relation stating that $\boldsymbol{\lambda}_1$ (or $1-\varrho$) is of the same order of magnitude as the expansion constant up to constant factors, since for the cycles, we have found in (1.6) that $h(C_m) \asymp 1/m$ for m large, while $1-\varrho_{C_m} \asymp 1/m^2$ by Exercise 2.6, which is much smaller. However, this is essentially as bad as it can get, as shown by the following bound, which is the discrete analogue of an inequality of Buser in the context of the geometric Cheeger constant [19]:

Proposition 2.15 (Discrete Buser inequality)**.** *Let $\Gamma = (V, E, \mathrm{ep})$ be a connected, non-empty, finite graph without isolated vertices. We have*

$$h(\Gamma) \leqslant v_+ \sqrt{2\,\boldsymbol{\lambda}_1(\Gamma)}. \tag{2.13}$$

We will prove this by following an argument of L. Trevisan [80, Handout 4], which highlights a practical algorithmic interpretation of this inequality. The idea is to study the expansion of sets of the type

$$W_{\varphi,t} = \varphi^{-1}(]-\infty, t]) = \{x \in V \mid \varphi(x) \leqslant t\}$$

for a real-valued function $\varphi : V \longrightarrow \mathbf{R}$ and a real number t, and to show that some of them satisfy

$$\frac{|\mathcal{E}(W_{\varphi,t})|}{|W_{\varphi,t}|} \leqslant v_+ \sqrt{2\,\boldsymbol{\lambda}_1(\Gamma)},$$

while containing at most $|V|/2$ vertices. The idea, to begin with, is to compute the average (over t) of the size of the sets $\mathcal{E}(W_{\varphi,t})$ for a given function, and deduce the existence of sets with certain expansion ratio. The following lemma performs this computation:

Lemma 2.16 (Expansion of sublevel sets)**.** *Let $\Gamma = (V, E, \mathrm{ep})$ be a finite non-empty connected graph and let $\varphi : V \longrightarrow \mathbf{R}$ be a real-valued non-constant function on V. Let*

$$a = \min_{x \in V} \varphi(x), \qquad b = \max_{x \in V} \varphi(x),$$

and let $t_0 \in \mathbf{R}$ be such that[2]

$$|W_{\varphi,t}| \leqslant \frac{|V|}{2}$$

if and only if $t < t_0$.

Then for any choice of a probability measure ν on $\mathbf{R}$ supported on $[a, b]$ and without atoms, we can find $t \in \mathbf{R}$ such that either $W = W_{\varphi,t}$ or $W = V - W_{\varphi,t}$ satisfies $|W| \leqslant |V|/2$ and

$$\frac{|\mathcal{E}(W)|}{|W|} \leqslant \frac{A}{B}$$

where

$$A = \frac{1}{2} \sum_{x,y \in V} a(x,y)\nu([\varphi(x), \varphi(y)]),$$

$$B = \sum_{x \in V} \nu([t_0, \varphi(x)])$$

using the convention that $\nu([a, b]) = \nu([\min(a, b), \max(a, b)])$.

[2] This means that t_0 is a "median" of the values of φ.

Proof. We denote $W_t = W_{\varphi,t}$ for simplicity. An edge α with $\mathrm{ep}(\alpha) = \{x, y\}$ is in $\mathcal{E}(W_t)$ if and only if t lies in the interval I_α between $\varphi(x)$ and $\varphi(y)$ where the largest is excluded, i.e., $I_\alpha = [\min(\varphi(x), \varphi(y)), \max(\varphi(x), \varphi(y))[$. Thus we may compute the average of $|\mathcal{E}(W_t)|$ as

$$\begin{aligned}\int_{\mathbf{R}} |\mathcal{E}(W_t)| d\nu(t) &= \sum_{\alpha\in E} \nu\{t \mid t \text{ is in the interval } I_\alpha\} \\ &= \sum_{\alpha\in E} \nu(I_\alpha) = \frac{1}{2}\sum_{x,y\in V} a(x,y)\nu([\varphi(x),\varphi(y)]) = A,\end{aligned}$$

since ν has no atom.

We want to compare this with the number of elements of W_t, or rather with the minimum $\min(|W_t|, |V - W_t|) \leqslant |V|/2$ (with the idea of using either W_t or $V - W_t$ to test the expansion constant).

Since the size of W_t is non-decreasing as a function of t, a real number t_0 such that $|W_t| \leqslant |V|/2$ if and only if $t < t_0$ exists. Then (again using the fact that ν has no atoms) we have

$$\begin{aligned}\int_{\mathbf{R}} \min(|W_t|, |V - W_t|) d\nu(t) &= \int_{t<t_0} |W_t| d\nu(t) + \int_{t\geqslant t_0} |V - W_t| d\nu(t) \\ &= \sum_{x\in V} \nu\{t \mid \varphi(x) \leqslant t < t_0\} + \sum_{x\in V} \nu\{t \mid t_0 \leqslant t \leqslant \varphi(x)\} \\ &= \sum_{x\in V} \nu([t_0, \varphi(x)]) = B.\end{aligned}$$

We now argue simply that since

$$\int_{\mathbf{R}} \Big(B|\mathcal{E}(W_t)| - A\min(|W_t|, |V - W_t|)\Big) d\nu(t) = 0,$$

there must exist some $t \in [a, b]$ for which

$$B|\mathcal{E}(W_t)| - A\min(|W_t|, |V - W_t|) \leqslant 0,$$

which is the desired conclusion! □

We are now led to an attempt to select a measure ν and then find a function φ to minimize the ratio A/B. The most natural-looking choice seems to be the uniform probability measure on $[a, b]$, with $d\nu(t) = dt/(b - a)$. In this case, we get

$$A = \frac{1}{2}\sum_{x,y\in V} a(x,y)\frac{|\varphi(x) - \varphi(y)|}{b-a}, \qquad B = \sum_{x\in V} \frac{|\varphi(x) - t_0|}{b-a}, \tag{2.14}$$

and the problem looks similar, in a rather more L^1-ish sense, to the computation of $\boldsymbol{\lambda}_1$ using the minimization characterization (2.10). However, because the L^1-norm is much less flexible and accessible than the L^2-norm, this does not seem easy to work out (as mentioned by Trevisan [81]; see Example 2.8 below for an instance of this). So we use instead, as in [80], the measure ν defined by

$$d\nu(t) = \frac{1}{S}|t - t_0| dt,$$

where S is the normalizing factor that makes this a probability measure on $[a, b]$. We have then

$$\nu([t_0, \varphi(x)]) = \frac{1}{2S}|\varphi(x) - t_0|^2$$

for all x and a second's thought shows that

$$\nu([\varphi(x),\varphi(y)]) \leqslant \frac{1}{2S}|\varphi(x)-\varphi(y)| \times (|\varphi(x)-t_0|+|\varphi(y)-t_0|).$$

Hence we find in this way a set W for which

$$h(\Gamma) \leqslant \frac{|\mathcal{E}(W)|}{|W|} \leqslant \frac{\widetilde{A}}{\widetilde{B}}$$

where

$$\widetilde{A} = \frac{1}{2}\sum_{x,y\in V} a(x,y)\{|\varphi(x)-t_0|+|\varphi(y)-t_0|\}|\varphi(x)-\varphi(y)|,$$

$$\widetilde{B} = \sum_{x\in V}|\varphi(x)-t_0|^2.$$

We can now estimate further in terms of quantities related to M. First, we write

$$\widetilde{B} = \sum_{x\in V}|\varphi(x)-t_0|^2 \geqslant \frac{1}{v_+}\sum_{x\in V}\mathrm{val}(x)|\varphi(x)-t_0|^2 = \frac{N}{v_+}\|\varphi-t_0\|^2$$

while, by the Cauchy-Schwarz inequality and the formulas (2.3) and (2.4), we have

$$\begin{aligned}(\widetilde{A})^2 &\leqslant \Big(\frac{1}{2}\sum_{x,y} a(x,y)|\varphi(x)-\varphi(y)|^2\Big)\Big(\frac{1}{2}\sum_{x,y} a(x,y)\{|\varphi(x)-t_0|+|\varphi(y)-t_0|\}^2\Big)\\ &= N\langle(\mathrm{Id}-M)\varphi,\varphi\rangle \times N\langle(\mathrm{Id}+M)|\varphi-t_0|,|\varphi-t_0|\rangle.\end{aligned}$$

Since $\|\mathrm{Id}+M\| \leqslant 2$, we obtain

$$\frac{\widetilde{A}}{\widetilde{B}} \leqslant v_+\Big(\frac{2\langle(\mathrm{Id}-M)\varphi,\varphi\rangle}{\|\varphi-t_0\|^2}\Big)^{1/2}.$$

We finally select φ to be an eigenfunction of $\mathrm{Id}-M$ with eigenvalue λ_1. Since φ is orthogonal to the constants, it is the orthogonal projection of $\varphi-t_0$ to the orthogonal complement of the constants, so $\|\varphi-t_0\| \geqslant \|\varphi\|$, and we get the inequality

$$h(\Gamma) \leqslant v_+\sqrt{2\lambda_1}$$

(note that there always exists a real-valued eigenfunction of $\mathrm{Id}-M$, since the real and imaginary parts of an eigenfunction φ are still eigenfunctions with the same eigenvalue, and one at least must be non-zero if $\varphi \neq 0$...) This finishes the proof of the discrete Buser inequality.

We can now also conclude the proof of part (2) in Theorem 2.9. Given a family (Γ_i) of expanders, we see from the discrete Buser inequality that the relaxed graph satisfy

$$v\sqrt{2\,\boldsymbol{\lambda}_1(\widetilde{\Gamma}_i)} \geqslant h(\widetilde{\Gamma}_i) = h(\Gamma_i).$$

This shows that the normalized spectral gap is bounded away from zero. Hence it is now enough to prove that $\widetilde{\Gamma}_i$ can not have an eigenvalue too close to -1. But the definition of $\widetilde{\Gamma}_i$ with its added loops leads to the formula

$$\begin{aligned}\langle(\mathrm{Id}+\widetilde{M}_i)\varphi,\varphi\rangle &= \frac{1}{2\widetilde{N}_i}\sum_{x,y\in V_i}\widetilde{a}(x,y)|\varphi(x)+\varphi(y)|^2\\ &= \frac{1}{2\widetilde{N}_i}\Big(\sum_{x,y\in V_i} a(x,y)|\varphi(x)+\varphi(y)|^2 + 4\sum_{x\in V_i}|\varphi(x)|^2\Big)\end{aligned}$$

and since $\widetilde{N}_i = N_i + |V_i| \leqslant 2N_i$ and $\mathrm{val}(x) \leqslant v_+ \leqslant v$, we get by positivity

$$\langle (\mathrm{Id} + \widetilde{M}_i)\varphi, \varphi\rangle \geqslant \frac{1}{N}\sum_{x\in V_i} |\varphi(x)|^2 \geqslant \frac{1}{v}\|\varphi\|^2,$$

which implies that $\widetilde{M}_i$ has no eigenvalue $< -1 + v^{-1}$. Hence we derive

$$\varrho_{\widetilde{\Gamma}_i} \leqslant 1 - \min\Big(\frac{h^2}{2v}, \frac{1}{v}\Big) < 1$$

for all i, giving equidistribution parameters of the relaxed graphs in terms of the expansion parameters (h, v) of (Γ_i). (Typically, $h^2/2$ is less than 1, of course, so we can replace this expression by $1 - h^2/(2v)$.)

2.3. **The expander mixing lemma.** The following proposition holds in general, but it is in the setting of expanders that it is especially useful, and is called "expander mixing lemma".

Proposition 2.17. *Let $\Gamma = (V, E, \mathrm{ep})$ be a finite graph with no isolated vertices. For any subsets V_1 and V_2 of V, we have*

$$\Big|\frac{|\mathcal{E}(V_1, V_2)|}{N} - \mu_\Gamma(V_1)\mu_\Gamma(V_2)\Big| \leqslant \tilde{\varrho}_\Gamma\sqrt{\mu_\Gamma(V_1)\mu_\Gamma(V_2)},$$

where $\tilde{\varrho}_\Gamma$ is the spectral radius of M restricted to the orthogonal of the constant functions in $L^2(\Gamma, \mu_\Gamma)$. In particular, if Γ is connected and not bipartite, we have $\tilde{\varrho}_\Gamma = \varrho_\Gamma$, and if Γ is d-regular for some $d \geqslant 2$, then we have

$$\Big||\mathcal{E}(V_1, V_2)| - \frac{d|V_1||V_2|}{|V|}\Big| \leqslant d\tilde{\varrho}_\Gamma\sqrt{|V_1||V_2|}.$$

Proof. For $i = 1, 2$, let φ_i be the characteristic function of V_i. Since these are real-valued, by (2.7), we have

$$\langle M\varphi_1, \varphi_2\rangle = \frac{1}{N}\sum_{x,y\in V} a(x, y)\varphi_1(y)\varphi_2(x)$$

and by definition of $a(x, y)$, this is equal to $|\mathcal{E}(V_1, V_2)|/N$.

On the other hand, we write $\varphi_i = \langle\varphi_i, 1\rangle + \varphi_{i,0}$, where $\varphi_{i,0}$ is orthogonal to the constants. By orthogonality of the eigenvectors, it follows that

$$\langle M\varphi_1, \varphi_2\rangle = \langle\varphi_1, 1\rangle\langle\varphi_2, 1\rangle + \langle M\varphi_{1,0}, \varphi_{2,0}\rangle.$$

The first term is equal to $\mu(V_1)\mu(V_2)$, whereas the second satisfies

$$|\langle M\varphi_{1,0}, \varphi_{2,0}\rangle| \leqslant \tilde{\varrho}_\Gamma\|\varphi_{1,0}\|\|\varphi_{2,0}\| \leqslant \tilde{\varrho}_\Gamma\|\varphi_1\|\|\varphi_2\| = \tilde{\varrho}_\Gamma\sqrt{\mu(V_1)\mu(V_2)}.$$

Comparing this with the first formula gives the desired statement. If Γ is d-regular, then $\mu_\Gamma(V_i) = |V_i|/|V|$ and $N = d|V|$, hence the second inequality follows. □

This result gives a good idea of the virtues of expander graphs: if $\tilde{\varrho}_\Gamma$ is relatively small, but the sets V_1 and V_2 are pretty large, then we obtain a very precise estimate on the size of $\mathcal{E}(V_1, V_2)$. The result also fits with the often-stated philosophy that an expander behaves like a random graph in many ways: indeed, if we consider a random graph with vertex set V and edges added independently between each pair of vertices, with the same probability for each edge, adjusted so that the average degree is d, then it is elementary that the expected value of $|\mathcal{E}(V_1, V_2)|$ is $d|V_1||V_2|/|V|$.

2.4. **The discrete Laplace operator.** In the course of Section 1.5, we have in fact seen that the spectral gap of a connected graph controls the expansion constant. This leads to a characterization of expanders using only the operator $\mathrm{Id} - M$.

Definition 2.18. Let $\Gamma = (V, E, \mathrm{ep})$ be a finite graph. The *normalized Laplace operator* of Γ, denoted $\boldsymbol{\Delta}_\Gamma$, is the linear operator

$$\boldsymbol{\Delta}_\Gamma \left\{ \begin{array}{ccc} L^2(\Gamma) & \longrightarrow & L^2(\Gamma) \\ \varphi & \mapsto & (\mathrm{Id} - M)\varphi \end{array} \right.$$

where M is the Markov operator of Γ. If Γ is d-regular for some $d \geqslant 1$, then the *Laplace operator* of Γ is defined by $\underline{\Delta}_\Gamma = d\boldsymbol{\Delta}_\Gamma$, and its spectral gap $\underline{\lambda}_1(\Gamma)$ is its smallest non-zero eigenvalue. It is equal to $d\,\boldsymbol{\lambda}_1(\Gamma_1)$.

Here is a summary of the results of the previous section in terms of the combinatorial Laplace operator, for regular graphs.

Proposition 2.19 (Properties of $\underline{\Delta}_\Gamma$)**.** *Let $\Gamma = (V, E, \mathrm{ep})$ be a finite connected d-regular graph without isolated vertex.*

(1) *The Laplace operator is self-adjoint and non-negative; its kernel is one-dimensional and spanned by the constant functions. Moreover we have*

$$\langle \underline{\Delta}_\Gamma \varphi, \varphi \rangle = \frac{1}{2|V|} \sum_{x,y \in V} a(x,y)|\varphi(x) - \varphi(y)|^2$$

for all $\varphi \in L^2(\Gamma)$.

(2) *We have*

$$\underline{\lambda}_1(\Gamma) = \min_{\substack{\varphi \in L^2(\Gamma) \\ \langle \varphi, 1 \rangle = 0}} \frac{\langle \underline{\Delta}_\Gamma \varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle}$$

and

$$\frac{\underline{\lambda}_1(\Gamma)}{2} \leqslant h(\Gamma) \leqslant \sqrt{2d\,\underline{\lambda}_1(\Gamma)}. \tag{2.15}$$

These are immediate consequences of the previous discussion. Similarly, we state for completeness the characterization of expander graphs in terms of $\boldsymbol{\lambda}_1(\Gamma)$ and $\underline{\lambda}_1(\Gamma)$.

Theorem 2.20 (Spectral definition of expanders)**.** *Let $(\Gamma_i)_{i \in I}$ be a family of connected finite graphs with $|\Gamma_i| \to +\infty$ and bounded valency $\max_i \max_x \mathrm{val}(x) \leqslant v$. Then (Γ_i) is an expander family if and only if there exists $\lambda > 0$ such that*

$$\boldsymbol{\lambda}_1(\Gamma_i) \geqslant \lambda > 0$$

for all $i \in I$.

If each Γ_i is d-regular for a fixed $d \geqslant 3$, then $(\Gamma_i)_{i \in I}$ is an expander family if and only if there exists $\lambda' > 0$ such that

$$\underline{\lambda}_1(\Gamma_i) \geqslant \lambda' > 0$$

for all $i \in I$.

We call (λ, v), or (λ', d), the spectral expansion parameters *of the family. For d-regular graphs, one can take $\lambda' = d\lambda$.*

The definition of expanders using the Laplace operator is qualitatively equivalent to that based on the expansion constant, and choosing one instead of the other may be a matter of personal taste. In concrete applications, on the other hand, it may well be the case that one requires that a family of graph satisfy specifically one of the two conditions (or three, if random walks are considered as slightly different). Even then, if the actual

values of the expansion parameters (λ, v) or (h, v) are not important, there is no problem in using either definition.

But it can very well happen that one wishes to have expanders according to, say, the spectral definition, and that the explicit value $\lambda > 0$ of the spectral gap plays a role in the results (for instance, this matters enormously for applications of expander graphs involving sieve methods in number theory, as we will sketch in Lecture 4). In such cases, starting from the "wrong" definition and translating the parameters from the expansion constant to the spectral gap might lead to serious loss of precision, since the order of magnitude of $h(\Gamma)$ and $\underline{\lambda}_1(\Gamma)$ might differ quite significantly.

As a final remark, the spectral theory of graphs is a very useful and powerful tool in graph theory, well beyond simply giving a characterization of expansion. It is especially interesting in concrete applications because it is algorithmically very manageable to compute eigenvalues of the Markov operator or of the discrete Laplace operator, even for rather large graphs (because it is a problem of linear algebra). Hence any problem that can be reduced (even if only approximately) to spectral properties can be studied quite deeply. Examples are given in Trevisan's notes [80] on spectral partitioning. Another illustration is the paper of Varshney, Chen, Paniagua, Hall and Chklovskii [83] on the spectral properties of the graph of the nervous system of the worm *c. elegans* (the only animal whose full neural network has been mapped in detail; it has 302 neurons, i.e., vertices, and about 8000 synapses, i.e. edges).

2.5. **Expansion of Cayley graphs.** When we specialize the general definitions and results of the previous sections to the case of a Cayley graph, we obtain group-theoretic reformulation of the definitions, which are as follows:

(1) Let G be a finite group, and $S \subset G$ is a non-empty[3] symmetric generating set. For the Cayley graph $\Gamma = \mathcal{C}(G, S)$, we have

$$h(\Gamma) = \min_{\substack{\emptyset \neq W \subset G \\ |W| \leqslant |G|/2}} \frac{|\mathcal{E}(W)|}{|W|}$$

with

$$|\mathcal{E}(W)| = |\{(g, s) \in W \times S \mid gs \notin W\}|$$

(a bijection from $\mathcal{E}(W)$ and the set on the right is $(g, s) \mapsto \{g, gs\} \in E_\Gamma$).

(2) The space $L^2(\Gamma, \mu_\Gamma)$ coincides with the space $L^2(G)$ of complex-valued functions on G, with the inner-product corresponding to the uniform probability measure on G, namely

$$\langle \varphi_1, \varphi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi_1(g)\overline{\varphi_2(g)}$$

for φ_1 and φ_2 in $L^2(G)$. The Markov averaging operator is given by

$$M\varphi(g) = \frac{1}{|S|} \sum_{s \in S} \varphi(gs),$$

[3]It could only be empty if G is trivial.

for $\varphi \in L^2(G)$ and $g \in G$. Therefore we have

$$\underline{\Delta}_\Gamma \varphi(g) = |S|\varphi(g) - \sum_{s\in S} \varphi(gs),$$

$$\langle \underline{\Delta}_\Gamma \varphi, \varphi\rangle = \frac{1}{2|G|} \sum_{\substack{g\in G\\ s\in S}} |\varphi(gs) - \varphi(g)|^2$$

for all $\varphi \in L^2(G)$ and, as usual, the minimization formula

$$\underline{\lambda}_1(\Gamma) = |S|\, \boldsymbol{\lambda}_1(\Gamma) = \min_{\varphi\perp 1} \frac{\langle \underline{\Delta}_\Gamma \varphi, \varphi\rangle}{\|\varphi\|^2}.$$

A remarkable non-trivial features of Cayley graphs, which is related to their symmetries, is that the diameter already gives a rather good control of the spectral gap, and hence of the expansion constant.

Proposition 2.21 (Bounding the spectral gap from the diameter)**.** *Let G be a finite group, $S \subset G$ a non-empty finite symmetric generating set of G. For the Cayley graph $\Gamma = \mathcal{C}(G, S)$, we have*

$$\underline{\lambda}_1(\Gamma) \geqslant \frac{1}{\operatorname{diam}(\Gamma)^2},$$

and hence

$$h(\Gamma) \geqslant \frac{1}{2\operatorname{diam}(\Gamma)^2}.$$

We omit the proof (see [52, Cor. 3.5.3]).

Example 2.22. The result is essentially sharp, as shown by the case of the cycles $C_m = \mathcal{C}(\mathbf{Z}/m\mathbf{Z}, \{\pm 1\})$, for which we have $\operatorname{diam}(C_m) \sim m/2$ and

$$\underline{\lambda}_1(\Gamma_m) \sim \frac{4\pi^2}{m^2} \sim \frac{\pi^2}{(\operatorname{diam} C_m)^2}$$

as $m \to +\infty$ by Example 2.5 (2) (taking into account that C_m is 2-regular.)

Example 2.23. Let $G_n = \mathcal{C}(\mathfrak{S}_n, S_n)$ for $n \geqslant 3$ as in Example 1.20, where we see again $\mathfrak{S}_n$ as acting on $\mathbf{Z}/n\mathbf{Z}$. We already know that $\operatorname{diam}(G_n) \ll n^2$ (by Exercise 1.8), and therefore we derive

$$\underline{\lambda}_1(G_n) \gg \frac{1}{n^4} \gg \frac{1}{(\log |G_n|)^4}$$

by Corollary 2.21. We also know (Exercise 1.14) that (G_n) is not an expander, since $h(G_n) \ll n^{-1}$.

2.6. **Equidistribution for Cayley graphs.** We explain now another important basic application of the spectral definition of expander graphs, which is particularly relevant to arithmetic applications in the context of Cayley graphs. The proper framework would involve random walks, but we will assume for simplicity that the graph is a Cayley graph, in which case there is a simple concrete interpretation.

Proposition 2.24. *Let G be a finite group and S a symmetric generating set of G such that $1 \in S$.*

For any element $g \in G$, and for $n \geqslant 1$, we have

$$\frac{1}{|S|^n} |\{(s_1, \dots, s_n) \in S^n \mid s_1 \cdots s_n = g\}| = \frac{1}{|G|} + O(\varrho^n)$$

where $\varrho = \varrho_\Gamma$ for $\Gamma = \mathcal{C}(G, S)$. In fact, the modulus of the difference is $\leqslant \varrho_\Gamma^n$.

Proof. Note that the condition that $1 \in S$ implies that the graph Γ is not bipartite. Let

$$p_n = \frac{1}{|S|^n}|\{(s_1, \dots, s_n) \in S^n \mid s_1 \cdots s_n = g\}|$$

for $n \geqslant 1$. Let φ denote the characteristic function of the point g, so that we can write

$$p_n = \frac{1}{|S|^n} \sum_{(s_1,\dots,s_n)\in S^n} \varphi(s_1 \cdots s_n).$$

If we further define

$$\varphi_0 = \varphi - \frac{1}{|G|},$$

so that $\varphi_0 \in L^2_0(\Gamma)$ (again because Γ is not bipartite), then we see that

$$p_n = \frac{1}{|G|} + q_n$$

where

$$q_n = \frac{1}{|S|^n} \sum_{(s_1,\dots,s_n)\in S^n} \varphi_0(s_1 \cdots s_n),$$

and we need to estimate q_n from above.

The basic formula, where the Markov operator enters the picture, is the fact that for any function $\psi \in L^2(\Gamma)$, and $n \geqslant 1$, we have

$$\frac{1}{|S|^n} \sum_{(s_1,\dots,s_n)\in S^n} \psi(s_1 \cdots s_n) = \frac{1}{|S|^{n-1}} \sum_{(s_1,\dots,s_{n-1})\in S^{n-1}} (M_\Gamma \psi)(s_1 \cdots s_{n-1}). \tag{2.16}$$

We will prove this later, and conclude first the proof, assmuing that this is correct. We apply the basic formula to $\psi = \varphi_0$, and then inductively to $M_\Gamma\varphi_0$, $\dots$, $M^n_\Gamma\varphi_0$. We obtain

$$\begin{aligned} q_n &= \frac{1}{|S|^n} \sum_{(s_1,\dots,s_n)\in S^n} \varphi_0(s_1 \cdots s_n) \\ &= M^n_\Gamma(\varphi_0)(1) \end{aligned}$$

(the 1 is the neutral element of G, the "empty product" of 0 elements of S). But then

$$0 \leqslant q_n \leqslant \|M^n_\Gamma\varphi_0\|_\infty \leqslant |G|^{1/2}\|M^n_\Gamma\varphi_0\| \leqslant \varrho^2_\Gamma|G|^{1/2}\|\varphi_0\| = \varrho^n_\Gamma.$$

It remains to prove (2.16). This is elementary: by the definition of Cayley graphs, we have

$$M_\Gamma\psi(g) = \frac{1}{|S|}\sum_{s\in S} \psi(gs),$$

and hence, if we split the sum on the left-hand side of (2.16) according to the value of $s_n \in S$, we get

$$\begin{aligned} \frac{1}{|S|^n} \sum_{(s_1,\dots,s_n)\in S^n} \psi(s_1 \cdots s_n) &= \frac{1}{|S|^{n-1}} \sum_{(s_1,\dots,s_{n-1})\in S^{n-1}} \frac{1}{|S|}\sum_{s_n\in S} \psi((s_1 \dots, s_{n-1})s_n) \\ &= \frac{1}{|S|^{n-1}} \sum_{(s_1,\dots,s_{n-1})\in S^{n-1}} (M_\Gamma\psi)(s_1 \cdots s_{n-1}), \end{aligned}$$

as claimed. □

Remark 2.25. (1) If you are familiar with probabilistic language, the previous computation is interpreted as follows. We are considering a simple (nearest neighbor) random walk $(X_n)_{n\geqslant 0}$ on G, defined by $X_0 = 1$ and $X_n = \xi_1 \cdots \xi_n$ for $n \geqslant 1$, where $(\xi_n)_{n\geqslant 1}$ is a sequence of independent random variables uniformly distributed in the finite set S. Then

$$\frac{1}{|S|^n} \sum_{(s_1,\dots,s_n)\in S^n} \psi(s_1 \cdots s_n)$$

is the same as the expectation (on the underlying probability space on which the random variables are defined) of $\psi(X_n)$. The basic formula (2.16) becomes

$$\mathbf{E}(\psi(X_n)) = \mathbf{E}((M_\Gamma \psi)(X_{n-1}))$$

for $n \geqslant 1$. The proposition can be interpreted as a simple special case of the general theory of finite Markov chains (convergence of the random walk to the equilibrium measure, which here is uniform on G).

(2) The meaning of the proposition, for a given graph, is that the products $s_1 \cdots s_n$ become "equidistributed" when n is large: they are about equally as likely to represent every element in G. Moreover, the "speed of convergence" is measure by ϱ_Γ. Since this quantity is < 1, the convergence is exponentially fast, but it only starts having effect when ϱ_Γ^n is (say) less than $1/(2|G|)$ (so that the inequality implies that the left-hand side, which is the probability that X_n is equal to g, is at least $1/(2|G|)$), which means when n is larger than about $\log(2|G|)/\log(1/\varrho)$.

This implies yet another interpretation of expander families: for Cayley graphs $\mathcal{C}(G_i, S_i)$, with S_i of bounded size, the expander property means that the "mixing" towards equilibrium is happening uniformly fast over all i.

2.7. **Exercises.**

Exercise 2.1. Let $\Gamma = (V, E, \mathrm{ep})$ be a finite graph.

(1) For $\varphi \in L^2(\Gamma, \mu_\Gamma)$, show that

$$\|\varphi\|^2 = \frac{1}{N} \sum_{x,y\in V} a(x,y)|\varphi(x)|^2. \tag{2.17}$$

(2) Let $\varphi \in L^2(\Gamma, \mu_\Gamma)$ be a function such that $\langle \varphi, 1\rangle = 0$ (i.e., a function which averages to 0). Show that

$$\|\varphi\|^2 = \frac{1}{2N^2} \sum_{x,y\in V} \mathrm{val}(x)\,\mathrm{val}(y)|\varphi(x) - \varphi(y)|^2. \tag{2.18}$$

Exercise 2.2. This exercise gives a different proof of the fact that $\|M\| \leqslant 1$.

(1) Explain why the norm of M is the maximum of the absolute values of its eigenvalues.

(2) If λ is an eigenvalue, show directly that $|\lambda| \leqslant 1$. [Hint: Use the maximum norm instead of the L^2-norm.]

Exercise 2.3 (Maximum modulus principle)**.** This exercise discusses the "geometric" computation of $\ker(M-1)$. We assume that Γ is a finite graph without isolated vertices.

(1) Show that if φ is the characteristic function of a connected component of Γ, we have $M\varphi = \varphi$.

(2) Show that, in order to prove that these characteristic functions span $\ker(M-1)$, it is enough to prove that a real-valued element of $\ker(M-1)$ is constant on each connected component of Γ.

(3) Let $W \subset V$ be a connected component. Let φ be a real-valued element of $\ker(M-1)$, let m be the maximum value of $\varphi(x)$ on W, and $x_0 \in W$ a vertex where $\varphi(x_0) = m$. Show that $\varphi(x) = m$ for all x connected to x_0 by at least one edge.

(4) Deduce that φ is equal to m on all of W and conclude.

(5) Using similar methods, determine $\ker(M+1)$.

Exercise 2.4 (Both sides have equal weight)**.** Let Γ be a connected non-empty finite bipartite graph without isolated vertices, partitioned as $V = V_0 \cup V_1$ with all edges between V_0 and V_1. Show that

$$\mu_\Gamma(V_0) = \mu_\Gamma(V_1) = \frac{1}{2}.$$

Exercise 2.5. Let $m \geqslant 3$ and consider the complete graph K_m on m vertices.

(1) Show that the Markov operator is given by

$$(M\varphi)(x) = \frac{1}{m-1}\Big(\sum_y \varphi(y) - \varphi(x)\Big) = -\frac{1}{m-1}\varphi(x).$$

$\varphi \in L^2_0(K_m)$.

(2) Deduce the spectrum and the value of ϱ_{K_m}.

Exercise 2.6. Let $m \geqslant 2$ and let $\Gamma = C_m$, with vertex set $\mathbf{Z}/m\mathbf{Z}$.

(1) Show that for

$$\varphi : \mathbf{Z}/m\mathbf{Z} \longrightarrow \mathbf{C}$$

we have

$$M\varphi(x) = \frac{1}{2}(\varphi(x-1) + \varphi(x+1)).$$

(2) Consider the discrete Fourier transform on $\mathbf{Z}/m\mathbf{Z}$, which is the linear map

$$\left\{ \begin{array}{ccc} L^2(C_m) & \longrightarrow & L^2(C_m) \\ \varphi & \mapsto & \widehat{\varphi} \end{array} \right.$$

defined by

$$\widehat{\varphi}(a) = \frac{1}{m}\sum_{x \in \mathbf{Z}/m\mathbf{Z}} \varphi(x) e\Big(-\frac{ax}{m}\Big)$$

for $a \in \mathbf{Z}/m\mathbf{Z}$, where $e(z) = e^{2i\pi z}$ for $z \in \mathbf{C}$.

For $a \in \mathbf{Z}/m\mathbf{Z}$, define χ_a to be the function on Γ such that $\chi_a(x) = e(ax/m)$.

Show that

$$\widehat{M\varphi}(a) = \cos\Big(\frac{2\pi a}{m}\Big)\widehat{\varphi}(a).$$

for any function φ on Γ and any a.

(3) Show that

$$M\chi_b = \cos\Big(\frac{2\pi b}{m}\Big)\chi_b$$

and that (χ_b) is an orthonormal basis of $L^2(\Gamma)$.

(4) If m is odd, show that each eigenvalue, except 1, has a 2-dimensional eigenspace spanned by χ_b and χ_{-b}. If m is even, show that all eigenvalues except for 1 and -1 (which have 1-dimensional eigenspaces) have a 2-dimensional eigenspace.

(5) Deduce that

$$\varrho_{C_m} = \cos\Big(\frac{2\pi}{m}\Big) = 1 - \frac{2\pi^2}{m^2} + O(m^{-4})$$

for $m \geqslant 2$.

Exercise 2.7. Let G_3 be the Cayley graph $\mathcal{C}(\mathfrak{S}_3, S_3)$ which we drew in Example 1.4.

(1) Compute the matrix of the Markov operator of G_3 in the basis of characteristic functions of single points, and compute its spectrum and the equidistribution radius.

(2) Compute an orthonormal basis of $L^2(G_3)$ of eigenfunctions of M.

Exercise 2.8 (The cycles again)**.** Let $\Gamma = C_m$ with $m \geqslant 2$ even (so that Exercise 2.6 shows that $\boldsymbol{\lambda}_1(C_m) = 1 - \cos(2\pi/m) \sim (2\pi^2)/m^2$ as $m \to +\infty$, while Example 1.26 implies that $h(C_m) \sim 4/m$).

(1) Consider the real-valued $\boldsymbol{\lambda}_1$-eigenfunction given by

$$\varphi(x) = \mathrm{Re}\Big(e\Big(\frac{x}{m}\Big)\Big) = \cos\Big(\frac{2\pi x}{m}\Big)$$

for $x \in \mathbf{Z}/m\mathbf{Z}$. Apply Lemma 2.16 with the uniform probability measure to deduce that there exists some set W with

$$h(C_m) \leqslant \frac{|\mathcal{E}(W)|}{|W|} \leqslant \frac{A}{B}$$

where

$$A = \sum_{0 \leqslant x \leqslant m-1} \Big|\cos\Big(\frac{2\pi x}{m}\Big) - \cos\Big(\frac{2\pi(x+1)}{m}\Big)\Big|,$$

$$B = \sum_{0 \leqslant x \leqslant m-1} \Big|\cos\Big(\frac{2\pi x}{m}\Big)\Big|.$$

(2) Show that $A \to 4$ as $m \to +\infty$, and $B \sim \frac{2}{\pi} m$. Thus the bound $h(C_m) \leqslant A/B \sim 2\pi/m$ is of the right order of magnitude in that case.

Exercise 2.9. Let $\Gamma = (V, E)$ be a finite simple graph. The *chromatic number* χ_Γ is the smallest integer $k \geqslant 0$ such that there is a k-coloring of V where no adjacent vertices have the same color (i.e., such that there is a function $f\colon V \to \{1, \dots, k\}$ such that $f(x) \neq f(y)$ whenever x and y are connected by an edge). The *independence number* i_Γ is the largest $k \geqslant 0$ such that there exists $Y \subset V$ with the property that elements of Y are never connected.

(1) Show that $\chi_\Gamma i_\Gamma \geqslant |\Gamma|$.

(2) If Γ is d-regular with $d \geqslant 2$, then show that $i_\Gamma \leqslant \varrho_\Gamma |\Gamma|$.

Lecture 3: expanders exist

In this third lecture, we will finally explain that expanders exist, and in fact provide various constructions, each of which is important in its own right. These by no means exhaust the known examples of expanders!

3.1. **Probabilistic existence of expanders.** The first approach to construct expander graphs is to use random constructions. This is the idea was used originally by Barzdin and Kolmogorov and by Pinsker [69, Lemma 1]. It turns out, in fact, that for many models of random graphs, there is a high probability that they are expanders, in the sense that there is a positive lower bound for the Cheeger constant, valid with high probability.

We will state a standard version of this result, involving bipartite expanders. Fix some integer $d \geqslant 3$. For any fixed $n \geqslant 1$ and any d-tuple $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_k)$ of permutations of $\{1, \dots, n\}$, we define a graph $\Gamma_{\boldsymbol{\sigma}}$ with vertex set

$$V = \{(i, 0) \mid 1 \leqslant i \leqslant n\} \cup \{(i, 1) \mid 1 \leqslant i \leqslant n\} = V_0 \cup V_1,$$

(independent of σ) and with edges joining $(i, 0)$ to $(\sigma_j(i), 1)$ for $1 \leqslant j \leqslant d$: formally, we take

$$E_{\boldsymbol{\sigma}} = \{(i, \sigma_j(i)) \mid 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant d\},$$

and $\mathrm{ep}((i, \sigma_j(i))) = \{(i, 0), (\sigma_j(i), 1)\}$. These graphs are bipartite and d-regular, and they may have multiple edges.

We view these graphs as *random graphs* by thinking of the permutations σ_i as taken independently and uniformly at random in $\mathfrak{S}_n$. Thus the *probability that the graphs Γ_σ satisfy a property $\mathcal{P}(\Gamma)$* of graphs, denoted $\mathbf{P}(\Gamma_\sigma \text{ has } \mathcal{P})$, is simply

$$\mathbf{P}(\Gamma_\sigma \text{ has } \mathcal{P}) = \frac{1}{|\mathfrak{S}_n|^d} |\{\boldsymbol{\sigma} \in \mathfrak{S}_n^d \mid \Gamma_\sigma \text{ has } \mathcal{P}\}| = \frac{1}{(n!)^d} |\{\boldsymbol{\sigma} \in \mathfrak{S}_n^d \mid \Gamma_\sigma \text{ has } \mathcal{P}\}|.$$

Then the following results holds:

Theorem 3.1. *Fix $d \geqslant 3$. There exists $h_d > 0$ such that*

$$\lim_{n \to +\infty} \mathbf{P}(h(\Gamma_{\boldsymbol{\sigma}}) < h_d) = 0.$$

In particular, for all n large enough, some Γ_σ satisfies $h(\Gamma_\sigma) \geqslant h_d$.

Remark 3.2. Here is one justification for hoping that such a result could be true. Recall that we suggested at the end of Section 1.4 that a possible way of constructing expanders would be to start with the finite trees $T_{d,k}$ of depth $k \geqslant 1$ with $d \geqslant 3$ fixed and $k \to +\infty$, and attempt to add some edges connecting the leaves of the tree to vertices "in the core" of the tree, and in particular to vertices on other branches from the root. Some elementary attempts of defining a family of edges of this type turn out to fail – either because the resulting graphs are again too easily disconnected, or because they seem hard to analyze. But these attempts might suggest that the best chance is to "throw edges at random". However, at this point, one can also simply decide that *all* edges should be placed randomly, to avoid dealing with two types of edges. This might naturally lead to the graphs of the type we consider here.

3.2. **Ramanujan graphs.** The definition of an expander family exhibits the remarkable feature of being quantitative in some sense (it refers to quantitative properties of the expansion constant) and qualitative in another (it asks for the existence of *some* positive lower bounds for the expansion constants). In applications, as we will see in Lecture 4, it happens frequently however that the value of this lower bound plays a role (in the random walk definition, this is obviously related to the speed of convergence to a uniform

measure). It is natural to ask if the expansion or equidistribution constants can have a meaning, or in a related way, how good can equidistribution be in the best possible world.

Although (to the author's knowledge) the values and limits of the expansion constant for expander families do not have any special property or interpretation, it turns out that the spectral data (Definition 2.8) can have some meaning, and in particular that it is natural to consider optimal cases: these are known as *Ramanujan graphs*.

Definition 3.3. Let $d \geqslant 2$ be an integer. A d-regular connected finite graph Γ is called a *Ramanujan graph* if all the eigenvalues λ of the Markov operator M of Γ satisfy either $\lambda \in \{-1, 1\}$ or $|\lambda| \leqslant \frac{2\sqrt{d-1}}{d}$, or in other words, if $\varrho_\Gamma \leqslant \frac{2\sqrt{d-1}}{d}$.

There is a good theoretical motivation for this definition, depending on the notion of the universal cover of a graph, which in the case of a d-regular graph is an infinite d-regular tree. For such an infinite graph, one can also define a Markov operator, and Kesten proved that the spectrum of the Markov operator is interval

$$\Big[-\frac{2\sqrt{d-1}}{d}, \frac{2\sqrt{d-1}}{d}\Big]$$

This means that the definition of a Ramanujan graph states that all "non-trivial" eigenvalues of M are contained in the spectrum of the universal cover of Γ.

In addition, a result of Alon-Boppana (see, e.g. [42, Th. 5.3] or [74, Prop. 3.2.7]) shows that this is the strongest possible restriction for an infinite family of graphs: if $(\Gamma_i)_{i\in I}$ is any family of d-regular connected graphs with $|\Gamma_i| \to +\infty$, then we have

$$\limsup_i \varrho_{\Gamma_i} \geqslant \frac{2\sqrt{d-1}}{d}.$$

Example 3.4. (1) Let $d \geqslant 3$. The complete graph K_d is a Ramanujan graph: indeed by Example 2.5, we have $\varrho_{K_d} = 1/(d-1) \leqslant 2\sqrt{d-1}/d$.

(2) Let $d \geqslant 3$ and let $K_{d,d}$ be the complete bipartite graph with input set $V_0 = \mathbf{Z}/d\mathbf{Z}$ and output set $V_1 = \mathbf{Z}/d\mathbf{Z}$ (Example 1.13, (2)). Then $K_{d,d}$ is also a Ramanujan graph. Indeed, since $K_{d,d}$ is bipartite, both 1 and -1 are eigenvalues of the Markov operator. But also, the kernel of the Markov operator is the space of $f \in L^2(K_{d,d})$ such that

$$\sum_{x\in V_0} f(x) = \sum_{x\in V_1} f(x) = 0,$$

which has codimension 2 in $L^2(K_{d,d})$. This means that 0 is the only eigenvalue of the Markov operator on $L^2_0(K_{d,d})$.

Since Ramanujan graphs are, individually, the best-possible graphs from the point of view of the Markov operator, one can ask if they can form expanders. In other words, does there exist an infinite family of Ramanujan graphs with bounded valency and increasing size? This turns out to be a rather subtle question. The paper where Ramanujan graphs were first defined by Lubotzky, Phillips and Sarnak [59] contains explicit examples of infinite families of d-regular Ramanujan graphs (also discovered independently by Margulis [61], both constructions relying on deep arithmetic input due to Deligne and Drinfeld), but only when $d = p + 1$ for some prime number p. This essential restriction was related to the specific arithmetic origin of these graphs. Further examples, always relying on number theory, produced examples with $d = p^\nu \pm 1$ for $\nu \geqslant 1$, always with p prime. Only quite recently have Marcus, Spielman and Srivastava [60] constructed Ramanujan graphs of arbitrary degree:

Theorem 3.5. *Let $d \geqslant 3$ be an integer. There exists a family $(\Gamma_i)_{i\geqslant 0}$ of* bipartite *d-regular Ramanujan graphs with $|\Gamma_i| = d2^i$.*

The proof uses a probabilistic argument, but in very different manner than Section 3.1: the idea is to show that given any starting d-regular bipartite Ramanujan graph Γ, there exists another bipartite Ramanujan graph Γ' with $|\Gamma'| = 2|\Gamma|$ which is a "2-covering" of Γ. This property had been conjectured by Bilu and Linial. Applied inductively, starting with the "trivial" example of the complete bipartite graph $K_{d,d}$ (Example 3.4, (2)), the theorem follows. (For generalizations to other coverings, see the paper [38] of Hall, Puder and Sawin.)

3.3. **Cayley graphs of finite linear groups.** For many of the applications of expander graphs that we will discuss in Chapter 3.5, the most important families of graphs are those arising from Cayley graphs of finite linear groups. Considerable progress has been made in recent years in understanding the expansion properties of these graphs.

There are two general, related, constructions of such families. We may consider a family (G_i) of finite groups, with $|G_i| \to +\infty$, given with symmetric generating subsets $S_i \subset G_i$ of fixed cardinality k, and the family $(\mathcal{C}(G_i, S_i))$. (For example, consider $\mathrm{SL}_2(\mathbf{F}_p)$ with generating set

$$\left\{\begin{pmatrix} 1 & \pm(p-1)/2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm(p-1)/2 & 1 \end{pmatrix}\right\}$$

for p prime $\geqslant 3$). Alternatively, we may consider an *infinite* finitely generated group G, with a fixed symmetric finite set of generators $S \subset G$, and a family K_i of normal subgroups $K_i \lhd G$ with finite index $[G : K_i] \to +\infty$, and consider the relative Cayley graphs $\mathcal{C}(G/K_i, S)$. (For example, take $G = \mathrm{SL}_2(\mathbf{Z})$ with

$$S = \left\{\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix}\right\}$$

and K_p, for p prime, the kernel of reduction modulo p).

Note that the second case is essentially a special case of the first one (taking S_i to be the image of S modulo K_i), but the first case is much more mysterious.

The question we wish to address is, quite generally: *under which type of condition is it true that a family of Cayley graphs as above is an expander family?*

Up to now, only two examples of sequences of Cayley graphs have appeared in this book, but these are not representative of the general case: the cycles C_m for $m \geqslant 2$ (which are 2-regular Cayley graphs of $G_m = \mathbf{Z}/m\mathbf{Z}$) or the graphs $G_n = \mathcal{C}(\mathfrak{S}_n, S_n)$ of Example 1.20 (4)). In both cases, we have seen that these are *not* expanders (though the second is not too far). But it turns out that, for many interesting sequences of "complicated" non-abelian groups, the answer to the question is positive, or conjectured to be so. For instance, in Section 3.4, we will give a fairly detailed sketch of the proof of the case $m = 3$ of the following theorem that combines results of Kazhdan and Margulis:

Theorem 3.6 (Kazhdan, Margulis)**.** *Let $m \geqslant 3$ be an integer. For any finite symmetric generating set S of $\mathrm{SL}_m(\mathbf{Z})$, the family of relative Cayley graphs*

$$(\mathcal{C}(\mathrm{SL}_m(\mathbf{Z})/H, S))_{H\lhd \mathrm{SL}_3(\mathbf{Z})},$$

where H runs over all finite index normal subgroups of $\mathrm{SL}_m(\mathbf{Z})$, is an expander family.

This is an important and useful result, but the method of proof shows that the groups concerned are fairly special. In particular, it does not apply to $\mathrm{SL}_2(\mathbf{Z})$ (and indeed, the analogue statement is false for $\mathrm{SL}_2(\mathbf{Z})$).

On the other hand, there is an important theorem, proved by Bourgain and Gamburd [10] for $m = 2$ and by Varjú [82] for $m \geqslant 3$ concerning expansion of quotients of much more general subgroups of $\mathrm{SL}_m(\mathbf{Z})$. The price in this generalization is that we must restrict the family of quotients that are expanding.

Theorem 3.7 (Expansion in Zariski-dense subgroups of $\mathrm{SL}_m(\mathbf{Z})$)**.** *Let $m \geqslant 2$ be an integer. Let $S \subset \mathrm{SL}_m(\mathbf{Z})$ be any finite symmetric subset and let G be the subgroup generated by S. Assume that G is Zariski-dense in SL_m. For prime numbers p, let $\Gamma_p = \mathcal{C}(\mathrm{SL}_m(\mathbf{F}_p), S)$ be the relative Cayley graph of the finite quotient group $\mathrm{SL}_m(\mathbf{F}_p)$ with respect to the reduction modulo p of the set S. Then there exists p_0 such that the family $(\Gamma_p)_{p \geqslant p_0}$ is an expander family.*

Remark 3.8. (1) The difference with Theorem 3.6 is that the previous result holds for *any* collection of finite index subgroups, not only for a specific family such as the kernels of reduction modulo primes, or even modulo any integer.

(2) In the special case of $\mathrm{SL}_2(\mathbf{Z})$, although Theorem 3.6 does not hold, there were important special cases of Theorem 3.7 that had been proved much earlier, and that were of great importance (both in terms of applications and of history). In particular, when $G = \mathrm{SL}_2(\mathbf{Z})$ itself, Theorem 3.7 follows from a crucial result of Selberg concerning the spectral gap of the hyperbolic Laplace operator and a comparison principle of Brooks and Burger. This is related to Lubotzky's Property (τ), and we refer to [56, §4.4] for more discussion. The most general result along these lines is due to Clozel [23].

In the setting of Theorem 3.7, the condition that G is Zariski-dense has a very simple equivalent formulation: it means that for all primes p large enough, the reduction modulo p maps G *surjectively* to $\mathrm{SL}_m(\mathbf{F}_p)$. In terms of graphs, it therefore means that there exists p_0 such that $\mathcal{C}(\mathrm{SL}_m(\mathbf{F}_p), S)$ is connected for all primes $p > p_0$, which is clearly a necessary condition for the expansion! It is also an elementary condition to check in many cases. For example, we obtain the following corollary:

Corollary 3.9 (Bourgain–Gamburd)**.** *Let $k \geqslant 1$ be an integer, let*

$$S = \left\{ \begin{pmatrix} 1 & \pm k \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm k & 1 \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbf{Z}),$$

and for p prime, let S_p denote the image of S modulo p. Then the family of Cayley graphs $\mathcal{C}(\mathrm{SL}_2(\mathbf{F}_p), S_p)$ for $p \nmid k$ is an expander family.

For $k = 1$ or $k = 2$, this result was part of the special cases known classically that we mentioned above. However, for $k \geqslant 3$, this was a notorious open question until the results of Bourgain–Gamburd led to a general proof. The difference between these two cases is that S generates a *finite index* subgroup of $\mathrm{SL}_2(\mathbf{Z})$ for $k = 1$ or $k = 2$, but an *infinite index* subgroup if $k \geqslant 3$. These groups are examples of what are now often known as "thin" subgroups of $\mathrm{SL}_2(\mathbf{Z})$ (see the book [13] for many aspects of the fascinating properties of these groups).

As we will also explain, a crucial step in the proof of Theorem 3.7 is a very important theorem that was proved by Helfgott [40] for SL_2 and SL_3 (and "almost" for SL_m), and then generalized by Pyber–Szabó [71] and Breuillard–Green–Tao [14] independently. The latter immediately implies for instance the following diameter bound:

Theorem 3.10. *Let $m \geqslant 2$ be an integer. For any prime number p, let $S_p \subset \mathrm{SL}_m(\mathbf{F}_p)$ be a symmetric generating set of $\mathrm{SL}_m(\mathbf{F}_p)$, and assume that*

$$|S_p| \leqslant k$$

for some fixed $k \geqslant 1$. Then there exist $c > 0$ and $A \geqslant 0$ such that the family of Cayley graphs $(\mathcal{C}(\mathrm{SL}_m(\mathbf{F}_p), S_p))$ satisfies

$$\lambda_1(\mathcal{C}(\mathrm{SL}_m(\mathbf{F}_p), S_p)) \geqslant \frac{c}{(\log p)^A}.$$

Remark 3.11. The following example shows that for certain families of finite groups, there may exist families of generators for which the associated Cayley graphs are expanders, and others for which they are not. The Cayley graphs $G_n = \mathcal{C}(\mathfrak{S}_n, S_n)$ of Example 1.20 (4) are *not* expanders, but a remarkable result of Kassabov [45] shows that there exist (effectively computable) generating sets T_n of $\mathfrak{S}_n$, of bounded size as $n \to +\infty$, such that the Cayley graphs $(\mathcal{C}(\mathfrak{S}_n, T_n))$ do form an expander. Hence, for symmetric groups at least, the expansion property is not purely group-theoretical.

The restriction to subgroups of $\mathrm{SL}_m(\mathbf{Z})$ and to reduction modulo primes in Theorem 3.7, and to subgroups of $\mathrm{SL}_m(\mathbf{F}_p)$ for Theorem 3.10, is only present for the sake of simplicity. Much successful work was done from 2010 to around 2014 to generalize these results to other groups and to reduction modulo other integers, and the current state of knowledge goes much further. To state these extensions requires the use of the language of algebraic groups; the reader who is not familiar with the terminology need only know that the groups SL_m for $m \geqslant 2$ and Sp_{2g} for $g \geqslant 2$ satisfy the conditions of both theorems we will now state.

The general version of Theorem 3.10 was proved by Pyber and Szabó [71] and Breuillard–Green–Tao [14] independently. Precisely we have:

Theorem 3.12. *Let $\mathbf{G}$ be a semisimple almost-simple linear algebraic group over $\mathbf{Q}$. For p prime, let $S_p \subset \mathbf{G}(\mathbf{F}_p)$ be a symmetric generating set of $\mathbf{G}(\mathbf{F}_p)$. Assume that there exists an integer $k \geqslant 1$ such that $|S_p| \leqslant k$ for all p. Then there exist $c > 0$ and $A \geqslant 0$ such that the family of Cayley graphs $(\mathcal{C}(\mathbf{G}(\mathbf{F}_p), S_p))$ satisfies*

$$\lambda_1(\mathcal{C}(\mathrm{SL}_m(\mathbf{G}(\mathbf{F}_p), S_p)) \geqslant \frac{c}{(\log p)^A}.$$

For expanders, Salehi-Golsefidy and Varjú [72] proved the following remarkable result, where the last addition corresponding to SL_m is due to Bourgain and Varjú [12].

Theorem 3.13. *Let $\mathbf{G}$ be a semisimple almost-simple linear algebraic group over $\mathbf{Q}$. Let Γ be a Zariski-dense finitely generated discrete subgroup of $\mathbf{G}(\mathbf{Z})$. Let S be a finite symmetric generating set of Γ. There exists an integer $N \geqslant 1$ such that the family of relative Cayley graphs $\mathcal{C}(\mathbf{G}(\mathbf{Z}/n\mathbf{Z}), S)$ for n squarefree and coprime to N is an expander family.*

If $\mathbf{G} = \mathrm{SL}_m$, then the same holds for the family $\mathcal{C}(\mathbf{G}(\mathbf{Z}/n\mathbf{Z}), S)$ for all integers $n \geqslant 1$ coprime to N.

The case of $\mathbf{G} = \mathrm{SL}_2$ and squarefree n is due to Bourgain, Gamburd and Sarnak [11].

3.4. **Property** (T)**.** In the 1960's, Kazhdan [46] introduced an important property of locally compact groups, related to their unitary representations. A few years later, it was realized by Margulis that this led to examples of expanders from Cayley graphs of finite quotients of discrete groups satisfying Kazhdan's property.

We first explain this result of Margulis, taking a practical point of view where we specialize the definitions from the outset to discrete groups.

Definition 3.14 (Kazhdan's Property (T))**.** Let G be a discrete group. One says that G has Property (T) if there exists a finite subset S of G and a positive real number $\delta > 0$ such that for any unitary representation

$$\varrho\colon G \to \mathrm{U}(E),$$

where E is a Hilbert space, either there exists a non-zero vector $v \in E$ fixed by ϱ (i.e., $\varrho(g)v = v$ for all $g \in G$) or for all $v \neq 0$, we have

$$\max_{s\in S} \|\varrho(g)v - v\| \geqslant \delta\|v\|.$$

One then says that (S, δ) is a *Kazhdan pair* for G. If S is fixed, δ is said to be a *Kazhdan constant*.

The shorthand for this definition is: G has Property (T) if, whenever G acts linearly by unitary transformations on a Hilbert space, either it has a (non-zero) invariant vector, or it doesn't even have "almost" invariant vectors: any vector is moved by a non-trivial amount by some element of S.

Theorem 3.15 (Margulis)**.** *Let G be a discrete group with Property* (T)*. Let (S, δ) be a Kazhdan pair for G such that S generates G. Let X be the family of all finite index normal subgroups of G. For all $H \in X$, we have*

$$h(\mathcal{C}(G/H, S)) \geqslant \delta^2.$$

In particular, if X contains elements of arbitrarily large index in G, the family of Cayley graphs of G/H, with respect to the image of S, is an expander family.

Proof. Let $H \in X$ and denote $\Gamma = \mathcal{C}(G/H, S)$. We consider the (finite-dimensional) Hilbert space $E = L^2(G/H)$ (i.e., the L^2-space for the Cayley graph Γ, where the inner product is defined by

$$\langle f_1, f_2, \rangle = \frac{1}{|G/H|} \sum_{x\in G/H} f_1(x)\overline{f_2(x)}$$

for $f_1,\ f_2\colon G/H \to \mathbf{C}$) and the homomorphism $G \to \mathrm{U}(E)$ defined by

$$\varrho(g)f(x) = f(xg)$$

(where we write $xg = x\pi(g)$ in terms of the projection $\pi\colon G \to G/H$). It is indeed elementary to check that ϱ is a homomorphism, and that $\varrho(g)$ is unitary.

Let E_0 be the orthogonal complement of the constant functions in E. Since the constant functions are invariant, under ϱ, and the representation is unitary, the subspace E_0 is also invariant. Thus ϱ induces a unitary representation $\varrho_0\colon G \to \mathrm{U}(E_0)$. Since S generates G, there is no function in E_0 invariant under the action of G.

Let now $W \subset G/H$ be a set of vertices of Γ with $|W| \leqslant \frac{1}{2}|G/H|$, and let

$$f = \mathbf{1}_W - \frac{|W|}{|G/H|}$$

be its normalized characteristic function. Then f belongs to E_0, and Kazhdan's Property (T) therefore implies that there exists $s \in S$ such that $\|\varrho(s)f - f\|^2 \geqslant \delta^2\|f\|^2$. However we have

$$\|\mathbf{1}_W\|^2 = \frac{|W|}{|G/H|}$$

and

$$\|\varrho(s)f - f\|^2 = \|\varrho(s)\mathbf{1}_W - \mathbf{1}_W\|^2 = \frac{1}{|G/H|}\sum_{x\in G/H} |\mathbf{1}_W(xs) - \mathbf{1}_W(x)|^2$$
$$= \frac{1}{|G/H|}\Big(\sum_{\substack{x\in W\\ xs\notin W}} 1 + \sum_{\substack{x\notin W\\ xs\in W}} 1\Big) \leqslant \frac{|\mathcal{E}(W)|}{|G/H|}.$$

It follows that

$$|\mathcal{E}(W)| \geqslant \delta^2|W|.$$

Taking the minimum over W, we see that the Cheeger constant of Γ is $\geqslant \delta^2$. □

Remark 3.16. One can show (see, e.g., [6, Prop. 1.3.2]) that in fact, for a discrete group G with Property (T), any Kazhdan pair (S, δ) has the property that S generates G. Note that this implies that G is finitely generated; this fact was one of the motivating applications of Property (T), since Kazhdan was able to prove Property (T) for certain groups that were not previously known to be finitely generated. Conversely, for any finite generating set S of G, one can show that there exists $\delta > 0$ (a Kazhdan constant for S) such that (S, δ) is a Kazhdan pair.

The following important theorem of Kazhdan implies Theorem 3.6.

Theorem 3.17 (Kazhdan)**.** *For any integer $m \geqslant 3$, the group $\mathrm{SL}_m(\mathbf{Z})$ has Property* (T)*. In particular, for any finite symmetric generating set S of $\mathrm{SL}_m(\mathbf{Z})$, the family of Cayley graphs*

$$(\mathcal{C}(\mathrm{SL}_m(\mathbf{Z})/H, S))_{H\lhd \mathrm{SL}_3(\mathbf{Z})},$$

where H runs over all finite index normal subgroups of $\mathrm{SL}_3(\mathbf{Z})$, is an expander family.

3.5. **Exercises.**

Exercise 3.1. Let $n \geqslant 2$. Let $S_n = \{\mathrm{Id} + E_{i,j} \mid 1 \leqslant i \neq j \leqslant n\}$ be the generating set of elementary matrix of $\mathrm{SL}_n(\mathbf{Z})$. Consider the unitary representation of $\mathrm{SL}_n(\mathbf{Z})$ on $L^2(\mathbf{Z}^n - \{0\})$ by $\varrho(g)\varphi(m) = \varphi(g^{-1}m)$ for $g \in \mathrm{SL}_n(\mathbf{Z})$, $\varphi \in L^2(\mathbf{Z}^n - \{0\})$ and $m \in \mathbf{Z}^n$. Let φ be the characteristic function of the n canonical basis vectors in $\mathbf{Z}^n - \{0\}$. Show that

$$\max_{s\in S} \|\varrho(s)\varphi - \varphi\| \geqslant \sqrt{\frac{2}{n}}\,\|\varphi\|.$$

(This result is also due to Żuk, and is reported in [76, p. 149]; it shows that the best possible Kazhdan constant for the generating set of elementary matrices must depend on n, and tends to 0 with n).

The following exercises are first steps in the direction of sieve-type arithmetic applications of expander graphs.

Exercise 3.2. Let $G = \mathrm{SL}_3(\mathbf{Z})$ and let S be a finite symmetric generating set of G containing 1.

(1) Show that there exists a constant $c \geqslant 0$ such that for primes p, we have

$$\frac{1}{|\mathrm{SL}_3(\mathbf{F}_p)|}|\{g \in \mathrm{SL}_3(\mathbf{F}_p) \mid \mathrm{Tr}(g) = 0\}| \leqslant \frac{c}{p}.$$

(2) Deduce that

$$\lim_{n\to+\infty} \frac{1}{|S|^n}|\{(s_1, \dots, s_n) \in S^n \mid \mathrm{Tr}(s_1 \cdots s_n) = 0\}| = 0.$$

(It may be useful to distinguish the cases $g_{3,3} = 0$ and $g_{3,3} \neq 0$.) Does this use the fact that $\mathrm{SL}_3(\mathbf{Z})$ has Property (T)?

Exercise 3.3. Let $S \subset G = \mathrm{SL}_3(\mathbf{Z})$ be a finite symmetric generating set of G containing 1.

Let $n \geqslant 1$ be an integer, $Q \geqslant 2$ be a parameter and define for p prime

$$b_p(s_1, \ldots, s_n) = 1$$

if $\mathrm{Tr}(s_1 \cdots s_n) \pmod p$ is a *not* square modulo p, and

$$b_p(s_1, \ldots, s_n) = 0$$

otherwise.

(1) For $Q \geqslant 2$, let

$$N_Q = \sum_{p \leqslant Q} b_p.$$

Show that

$$\frac{1}{|S|^n}|\{(s_1, \ldots, s_n) \in S^n \mid \mathrm{Tr}(s_1, \ldots, s_n) \text{ is a square in } \mathbf{Z}\}| \leqslant \frac{1}{|S|^n}|\{(s_1, \ldots, s_n) \mid N_Q(s_1, \ldots, s_n) = 0\}|.$$

(2) Show that

$$\frac{1}{|S|^n}|\{(s_1, \ldots, s_n) \mid N_Q(s_1, \ldots, s_n) = 0\}| \leqslant \frac{V_Q}{E_Q^2}$$

where

$$E_Q = \frac{1}{|S|^n} \sum_{(s_1,\ldots,s_n) \in S^n} N(s_1, \ldots, s_n),$$

$$V_Q = \frac{1}{|S|^n} \sum_{(s_1,\ldots,s_n) \in S^n} N(s_1, \ldots, s_n)^2 - E_Q^2.$$

(3) Show that there exists $\delta > 0$ such that

$$\frac{1}{|\mathrm{SL}_3(\mathbf{F}_p)|}|\{g \in \mathrm{SL}_3(\mathbf{F}_p) \mid \mathrm{Tr}(g) \text{ is a square}\}| \geqslant \delta$$

if $p \geqslant 5$.

(4) Using expansion, show that there exists $A > 1$ and $\delta > 0$ such that

$$E_{A^n} \geqslant \delta \pi(A^n),$$

where $\pi(A^n)$ is the number of primes up to A^n.

(5) If $p_1 \neq p_2$ are distinct primes, show that there is an isomorphism of groups

$$\mathrm{SL}_3(\mathbf{F}_{p_1}) \times \mathrm{SL}_3(\mathbf{F}_{p_1}) \simeq \mathrm{SL}_3(\mathbf{Z}/p_1p_2\mathbf{Z}).$$

(6) Using expansion again and (5), show that there exists $B > 1$ and $c > 0$ such that

$$V_{B^n} \leqslant c\pi(B^n)$$

(this is more difficult; expand the square in $N^2(s_1, \ldots, s_n)$ as sum over pairs (p_1, p_2) of primes $\leqslant Q$, and handle separately the cases $p_1 = p_2$ and $p_1 \neq p_2$.)

(7) Deduce that

$$\lim_{n \to +\infty} \frac{1}{|S|^n}|\{(s_1, \ldots, s_n) \in S^n \mid \mathrm{Tr}(s_1, \ldots, s_n) \text{ is a square in } \mathbf{Z}\}| = 0.$$

(8) How far do you think you might generalize this type of statement?

Lecture 4: some applications of expander graphs

This lecture presents, mostly in a survey style, some of the applications of expander graphs. This is very far from exhaustive – the reader will find many more applications, especially to combinatorics and theoretical computer science, in [42], and to "pure" mathematics in the books and lectures of Lubotzky [56], [57] and of Sarnak [74].

References

[1] D. Abramovich: *A linear lower bound on the gonality of modular curves*, International Math. Res. Notices 20 (1996), 1005–1011.

[2] D. Abramovich and F. Voloch: *Lang's conjectures, fibered powers, and uniformity*, New York J. of Math. 2 (1996), 20–34.

[3] M. Agrawal, N. Kayal and N. Saxena: *PRIMES is in P*, Annals of Math. 160 (2004), 781–793.

[4] M. Aschenbrenner, S. Friedl and H. Wilton: 3*-manifold groups*, EMS Lectures in Math., E.M.S Publ. House, 2015.

[5] Ya.M. Barzdin and A.N. Kolmogorov: *On the realization of networks in three-dimensional space*, in Selected Works of Kolmogorov, Volume 3, Kluwer Academic Publishers, Dordrecht, 1993. 18

[6] B. Bekka, P. de la Harpe and A. Valette: *Kazhdan's Property* (T), New Math. Monographs 11, Cambridge Univ. Press (2008). 45

[7] N. Bergeron: *Variétés en expansion*, Séminaire Bourbaki, exposé 1132 (June 2017).

[8] J.A. Bondy and U.S.R. Murty: *Graph theory*, Graduate Texts Math. 244, Springer, 2008. 3

[9] N. Bourbaki: *Topologie algébrique*, Springer (2016).

[10] J. Bourgain and A. Gamburd: *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbf{F}_p)$, Ann. of Math. 167 (2008), 625–642. 42

[11] J. Bourgain, A. Gamburd and P. Sarnak: *The affine linear sieve*, Invent. math. 179 (2010), 559–644. 43

[12] J. Bourgain and P. Varjú: *Expansion in* $\mathrm{SL}_d(\mathbf{Z}/q\mathbf{Z})$*,* q *arbitrary*, Invent. math. 188 (2012), 151–173. 43

[13] E. Breuillard and H. Oh (editors): *Thin groups and super-strong-approximation*, MSRI Publications 61, Cambridge (2014). 42

[14] E. Breuillard, B. Green and T. Tao: *Approximate subgroups of linear groups*, GAFA 21 (2011), 774–819; arXiv:1005.1881. 42, 43

[15] E. Breuillard, B. Green and T. Tao: *The structure of approximate groups*, Publ. Math. IHÉS 116 (2012), 115–221.

[16] R. Brooks: *The spectral geometry of a tower of coverings*, J. Diff. Geometry 23 (1986), 97–107.

[17] M. Burger: *Petites valeurs propres du Laplacien et topologie de Fell*, doctoral thesis (1986), Econom Druck AG (Basel).

[18] M. Burger: *Kazhdan constants for* $SL(3,\mathbf{Z})$, J. reine angew. Math. 413 (1991), 36–67.

[19] P. Buser: *A note on the isoperimetric constant*, Ann. Sci. École Norm. Sup. 15 (1982), 213–230. 28

[20] P. Buser: *Geometry and spectra of compact Riemann surfaces*, Modern Birkhäuser Classics, 2010.

[21] I. Chavel: *Eigenvalues in Riemannian geometry*, Academic Press, 1984.

[22] J. Cheeger: *A lower bound for the smallest eigenvalue of the Laplacian*, in "Problems in analysis (Papers dedicated to Salomon Bochner, 1969)", Princeton Univ. Press. 1970, 195–199. 12, 27

[23] L. Clozel: *Démonstration de la conjecture* τ, Invent. math. 151 (2003), 297–328. 42

[24] D. Cox: *Primes of the form* x^2+my^2, Wiley 1989.

[25] G. Davidoff, P. Sarnak, and A. Valette: *Elementary number theory, group theory, and Ramanujan graphs*, LMS Student Text 55, Cambridge University Press 2003.

[26] P. Diaconis and L. Saloff-Coste: *Comparison techniques for random walk on finite groups*, Annals of Prob. 21 (1993), 2131–2156. 4, 19

[27] J. Ellenberg, C. Hall and E. Kowalski: *Expander graphs, gonality and variation of Galois representations*, Duke Math. Journal 161 (2012), 1233–1275.

[28] J. Ellenberg: *Superstrong approximation for monodromy groups*, in "Thin groups and super-strong-approximation", MSRI Publications 61, Cambridge (2014), edited by E. Breuillard and H. Oh.

[29] G. Faltings: *Diophantine approximation on abelian varieties*, Annals of Math. 133 (1991), 549–576.

[30] G. Farkas: *Brill–Noether loci and the gonality stratification of* $\mathcal{M}_g$, J. reine angew. Math. 539 (2001), 185–200.

[31] H. Farkas and I. Kra: *Riemann surfaces*, 2nd edition, Grad. Texts in Math. 71, Springer 1992.

[32] G. Frey: *Curves with infinitely many points of fixed degree*, Israel J. Math. 85 (1994), 79–83.

[33] P.X. Gallagher: *The large sieve and probabilistic Galois theory*, in Proc. Sympos. Pure Math., Vol. XXIV, Amer. Math. Soc. (1973), 91–101. 19
[34] A. Gamburd: *On the spectral gap for infinite index "congruence" subgroups of* $\mathrm{SL}_2(\mathbf{Z})$, Israel J. Math. 127 (2002), 157-–200.
[35] W.T. Gowers: *Quasirandom groups*, Comb. Probab. Comp. 17 (2008), 363–387.
[36] M. Gromov: *Filling Riemannian manifolds*, J. Differential Geom. 18 (1983), 1–147.
[37] M. Gromov and L. Guth: *Generalizations of the Kolmogorov-Barzdin embedding estimates*, Duke Math. J. 161 (2012), 2549–2603; arXiv:1103.3423.
[38] C. Hall, D. Puder and W. Sawin: *Ramanujan coverings of graphs*, preprint arxiv:1506.02335; abridged version in STOC 2016, 48th annual ACM SIGACT Symposium in the Theory of Computing, 533–541, 2016. 41
[39] P. de la Harpe: *Topics in Geometric Group Theory*, Chicago Lectures in Math., Univ. of Chicago Press (2000). 10, 11
[40] H. Helfgott: *Growth and generation in* $\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$, Ann. of Math. 167 (2008), 601–623. 42
[41] H.M. Hilden: *Three-fold branched coverings of* $\mathbf{S}^3$, Amer. J. Math. 98 (1976), 989–997.
[42] S. Hoory, N. Linial and A. Wigderson: *Expander graphs and their applications*, Bull. Amer. Math. Soc. 43 (2006), 439–561. 40, 48
[43] K. Ireland and M. Rosen: *A Classical Introduction to Modern Number Theory*, 2nd Edition, GTM 84, Springer-Verlag (1990).
[44] H. Iwaniec and E. Kowalski: *Analytic number theory*, Colloq. Publ. 53, Amer. Math. Soc. (2004).
[45] M. Kassabov: *Symmetric groups and expander graphs*, Inventiones math. 170 (2007), 327–354. 43
[46] D. Kazhdan: *Connection of the dual space of a group with the structure of its closed subgroups*, Funct. Anal. Appl. 1 (1967), 63–65. 43
[47] A. Kontorovich: *From Apollonius to Zaremba: Local-Global phenomena in thin orbits*, Bull. AMS 50, (2013), 187–228.
[48] E. Kowalski: *Elliptic curves, rank in families and random matrices*, in *Ranks of Elliptic Curves and Random Matrix Theory*, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, LMS Lecture Note 341, (Cambridge University Press 2007).
[49] E. Kowalski: *Crible en expansion*, Séminaire Bourbaki, exposé 1028, November 2010, Astérisque 348, Soc. Math. France (2012), 17–64.
[50] E. Kowalski: *The large sieve and its applications*, Cambridge Tracts in Math., vol 175, C.U.P (2008).
[51] E. Kowalski: *Explicit growth and expansion for* SL_2, International Math. Res. Notices. 2012; doi:10.1093/imrn/rns214
[52] E. Kowalski: *An introduction to expander graphs*, Cours Spécialisés 26, S.M.F (2019). 34
[53] E. Kowalski: *Sieve in discrete groups, especially sparse*, in "Thin groups and super-strong-approximation", MSRI Publications 61, Cambridge (2014), edited by E. Breuillard and H. Oh.
[54] M. Lackenby: *Heegaard splittings, the virtually Haken conjecture and property* (τ), Invent. math. 164 (2006), 317–359.
[55] P. Li and S.T. Yau: *A new conformal invariant and its applications to the Willmore conjecture and the first eigenvalue of compact surfaces*, Invent. math. 69 (1982), 269–291.
[56] A. Lubotzky: *Discrete groups, expanding graphs and invariant measures*, Progress in Math. 125, Birkaüser (1994). 42, 48
[57] A. Lubotzky: *Expander graphs in pure and applied mathematics*, Bulletin AMS 49 (2012), 113–162. 48
[58] A. Lubotzky and C. Meiri: *Sieve methods in group theory, I: powers in linear groups*, Journal A.M.S 25 (2012), 1119–1148.
[59] A. Lubotzky, R. Phillips and P. Sarnak: *Ramanuajan graphs*, Combinatorica 8 (1988), 261–277. 40
[60] A. Marcus, D.A. Spielman and N. Srivastava: *Interlacing families, I: bipartite Ramanuajan graphs of all degrees*, Ann. of Math. (2) 182 (2015), 307–325. 40
[61] G. Margulis: *Explicit group theoretic constructions of combinatorial schemes and their applications for the construction of expanders and con- centrators*, J. of Problems of Information Transmission, 24 (1988), 39–46. 40
[62] J. McCarthy: *Recursive functions of symbolic expressions and their computations by machines, I*, Communications of the A.C.M 3 (1960), 184–195.

[63] R. Miranda: *Riemann surfaces*, Grad. Studies in Math. 5 (A.M.S), 1995.
[64] J.M. Montesinos: *Three-manifolds as 3-fold branched covers of* $\mathbf{S}^3$, Quart. J. Math. Oxford Ser. (2) 27 (1976), 85–94.
[65] T. Netzer and A. Thom: *Kazhdan's property* (T) *via semidefinite optimization*, Exp. Math. 24 (2015), 371–374.
[66] M. Orr: *Unlikely intersections with Hecke translates of a special subvariety*, preprint (2017), arXiv:1710.04092.
[67] N. Ozawa: *Noncommutative real algebraic geometry of Kazhdan's property* (T), J. Inst. Math. Jussieu 15 (2016), 85–90.
[68] J. Pardon: *On the distorsion of knots on embedded surfaces*, Annals of Math. 174 (2011), 637–646.
[69] M. Pinsker: *On the complexity of a concentrator*, in "7th International Telegrafic Conference", pages 318/1–318/4, 1973. 18, 39
[70] B. Poonen: *Gonality of modular curves in characteristic p*, Math. Res. Lett. 14, no. 4 (2007), 691–701.
[71] L. Pyber and E. Szabó: *Growth in finite simple groups of Lie type of bounded rank*, Journal A.M.S 29 (2016), 95–146. 42, 43
[72] A. Salehi Golsefidy and P. Varjú: *Expansion in perfect groups*, G.A.F.A 22 (2012), 1832–1891, 43
[73] P. Sarnak and X. Xue: *Bounds for multiplicities of automorphic representations*, Duke Math. J. 64, (1991), 207–227.
[74] P. Sarnak: *Some applications of modular forms*, Cambridge Tracts in Math. 99, Cambridge Univ. Press 1990. 40, 48
[75] J-P. Serre: *A course in arithmetic*, Grad. Texts in Math. 7, Springer 1973.
[76] Y. Shalom: *Bounded generation and Kazhdan's property (T)*, Publ. Math I.H.É.S 90 (1999), 145–168. 45
[77] J. Silverman: *The arithmetic of elliptic curves*, Grad. Texts in Math 106, Springer Verlag (1986).
[78] R. Solovay and V. Strassen: *A fast Monte-Carlo test for primality*, SIAM J. Comput. 6 (1977), 84–85.
[79] T. Tao: *Expansion in finite simple groups of Lie type*, Grad. Studies Math. 164, AMS (2015).
[80] L. Trevisan: *Graph partitioning and expander*, 2011 lectures notes available at theory.stanford.edu/~trevisan/cs359g/index.html. 28, 29, 33
[81] L. Trevisan: *The Spectral Partitioning algorithm*, blog post available at lucatrevisan.wordpress.com/2008/05/11/the-spectral-partitioning-algorithm/ 29
[82] P. Varjú: *Expansion in* $\mathrm{SL}_d(\mathcal{O}_K/I)$*, I square-free*, J. Eur. Math. Soc. (JEMS) 14 (2012), 273–305. 42
[83] L.R. Varshney, B.L. Chen, E. Paniagua, D.H. Hall and D.B. Chklovskii: *Structural Properties of the Caenorhabditis elegans Neuronal Network*, PLoS Comput Biol 7(2) (2011): e1001066; doi.org/10.1371/journal.pcbi.1001066. 33
[84] J. G. White, E. Southgate, J. N. Thomson and S. Brenner: *The Structure of the Nervous System of the Nematode Caenorhabditis elegans*, Phil. Trans. R. Soc. Lond. B 314 (1986), 1–340; DOI:10.1098/rstb.1986.0056.
[85] P. Zograf: *Small eigenvalues of automorphic Laplacians in spaces of cusp forms*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 134 (1984), 157–168, English translation in Journal of Math. Sciences 36, Number 1, 106–114, DOI:10.1007/BF01104976.