# An Overview

In this book, we shall consider graphs $X = (V, E)$, where $V$ is the set of vertices and $E$ is the set of edges of $X$. We shall assume that $X$ is undirected; most of the time, $X$ will be finite. A *path* in $X$ is a sequence $v_1\, v_2 \ldots v_k$ of vertices, where $v_i$ is adjacent to $v_{i+1}$ (i.e., $\{v_i, v_{i+1}\}$ is an edge). A graph $X$ is *connected* if every two vertices can be joined by a path.

For $F \subseteq V$, the *boundary* $\partial F$ is the set of edges connecting $F$ to $V - F$. Consider for example the graph in Figure 0.1 (this is the celebrated Petersen graph): it has 10 vertices and 15 edges; three vertices have been surrounded by squares: this is our subset $F$; the seven "fat" edges are the ones in $\partial F$.

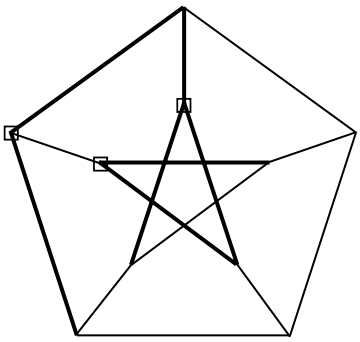

Figure 0.1

The *expanding constant*, or *isoperimetric constant* of $X$, is

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

If we view $X$ as a network transmitting information (where information retained by some vertex propagates, say in 1 unit of time, to neighboring vertices), then $h(X)$ measures the "quality" of $X$ as a network: if $h(X)$ is large,

information propagates well. Let us consider two extreme examples to illustrate this.

**0.1.1. Example.** The *complete graph* $K_m$ on $m$ vertices is defined by requiring every vertex to be connected to any other, distinct vertex: see Figure 0.2 for $m = 5$.

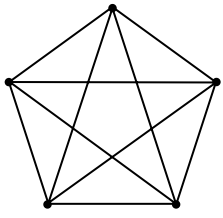

Figure 0.2

It is clear that, if $|F| = \ell$, then $|\partial F| = \ell(m - \ell)$, so that $h(K_m) = m - \left[\frac{m}{2}\right] \sim \frac{m}{2}$.

**0.2.2. Example.** The *cycle* $C_n$ on $n$ vertices: see Figure 0.3 for $n = 6$. If $F$ is a half-cycle, then $|\partial F| = 2$, so $h(C_n) \leq \frac{2}{\left[\frac{n}{2}\right]} \sim \frac{4}{n}$; in particular $h(C_n) \to 0$ for $n \to +\infty$.

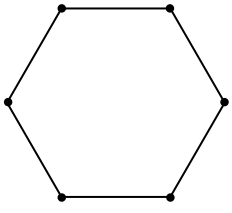

Figure 0.3

From these two examples, wee see that the highly connected complete graph has a large expanding constant that grows proportionately with the number of vertices. On the other hand, the minimally connected cycle graph has a small expanding constant that decreases to zero as the number of vertices grows. In this sense, $h(X)$ does indeed provide a measure of the "quality," or connectivity of $X$ as a network.

We say that a graph $X$ is *$k$-regular* if every vertex has exactly $k$ neighbors, so that the Petersen graph is 3-regular, $K_m$ is $(m-1)$-regular, and $C_n$ is 2-regular.

**0.3.3. Definition.** Let $(X_m)_{m\geq 1}$ be a family of graphs $X_m = (V_m, E_m)$ indexed by $m \in \mathbb{N}$. Furthermore, fix $k \geq 2$. Such a family $(X_m)_{m\geq 1}$ of finite, connected,

$k$-regular graphs is a *family of expanders* if $|V_m| \to +\infty$ for $m \to +\infty$, and if there exists $\varepsilon > 0$, such that $h(X_m) \geq \varepsilon$ for every $m \geq 1$.

Because an optimal design for a network should take economy of transmission into account, we include the assumption that $X_m$ is $k$-regular in Definition 0.3.3. This assures that the number of edges of $X_m$ grows linearly with the number of vertices. Without that assumption, we could just take $X_m = K_m$ for good connectivity. However, note that $K_m$ has $\frac{m(m-1)}{2}$ edges, which quickly becomes expensive when transmission lines are made of either copper or optical fibers. Hence, the "optimal" network for practical purposes arises from a graph that provides the best connectivity from a minimal number of edges.

Indeed such expander graphs have become basic building blocks in many engineering applications. We cite a few such applications, taken from Reingold, Vadhan and Wigderson [55]: to network designs [53], to complexity theory [66], to derandomization [50], to coding theory [63], and to cryptography [30].

**0.4.4. Main Problem.** Give explicit constructions for families of expanders.

We shall solve this problem algebraically, by appealing to the *adjacency matrix* $A$ of the graph $X = (V, E)$; it is indexed by pairs of vertices $x, y$ of $X$, and $A_{xy}$ is the number of edges between $x$ and $y$.

When $X$ has $n$ vertices, $A$ is an $n$-by-$n$, symmetric matrix, which completely determines $X$. By standard linear algebra, $A$ has $n$ real eigenvalues, repeated according to multiplicities that we list in decreasing order:

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

In section 1.1 we shall prove the following.

**0.5.5. Proposition.** If $X$ is a $k$-regular graph on $n$ vertices, then

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

Moreover,

(a) $\mu_0 > \mu_1$ if and only if $X$ is connected.
(b) Suppose $X$ is connected. The equality $\mu_{n-1} = -k$ holds if and only if $X$ is bicolorable. (A graph $X$ is *bicolorable* if it is possible to paint the vertices of $X$ in two colors in such a way that adjacent vertices have distinct colors.)

It turns out that the expanding constant can be estimated spectrally by means of a double inequality (due to Alon & Milman [3] and to Dodziuk [22]) that we shall prove in section 1.2.

**0.6.6. Theorem.** Let $X$ be a finite, connected, $k$-regular graph. Then

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

This allows for an equivalent formulation of 0.4.4.

**0.7.7. Rephrasing of the Main Problem.** Give explicit constructions for families $(X_m)_{m\geq 1}$ of finite, connected, $k$-regular graphs with the following properties: (i) $|V_m| \to +\infty$ for $m \to +\infty$, and (ii) there exists $\varepsilon > 0$ such that $k - \mu_1(X_m) \geq \varepsilon$ for every $m \geq 1$.

Therefore, to have good quality expanders, the *spectral gap* $k - \mu_1(X_m)$ has to be as large as possible. However, the spectral gap cannot be too large as was observed independently by Alon and Boppana [10] and Serre [62] (see also Grigorchuk & Zuk [31]). In fact, we have the bound implied by the following result.

**0.8.8. Theorem.** Let $(X_m)_{m\geq 1}$ be a family of finite, connected, $k$-regular graphs with $|V_m| \to +\infty$ as $m \to +\infty$. Then

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

This asymptotic threshold will be discussed in section 1.3 and proved in section 1.4. Now Theorem 0.8.8 singles out an extremal property on the eigenvalues of the adjacency matrix of a $k$-regular graph; this motivates the definition of a Ramanujan graph.

**0.9.9. Definition.** A finite, connected, $k$-regular graph $X$ is *Ramanujan* if, for every eigenvalue $\mu$ of $A$ other than $\pm k$, one has

$$|\mu| \leq 2\sqrt{k-1}\,.$$

So, if for some $k \geq 3$ we succeed in constructing an infinite family of $k$-regular Ramanujan graphs, we will get a solution of our main problem 0.7.7 (hence, also of 0.4) which is optimal from the spectral point of view.

**0.10.10. Theorem.** For the following values of $k$, there exist infinite families of $k$-regular Ramanujan graphs:

- $k = p + 1$, where $p$ is an odd prime ([42], [46]).
- $k = 3$ [14].
- $k = q + 1$, where $q$ is a prime power [48].

Our purpose in this book is to describe the Ramanujan graphs of Lubotzky et al. [42] and Margulis [46]. While the description of these Ramanujan graphs (given in section 4.2) is elementary, the proof that they have the desired properties is not. For example, the proofs in [42] and [41] make free use of the theory of algebraic groups, modular forms, theta correspondences, and the Riemann Hypothesis for curves over finite fields. Our aim here is to give elementary and self-contained proofs of most of the properties enjoyed by these graphs, results the reader will find in sections 4.3 and 4.4. Actually, our elementary methods will not give us the full strength of the Ramanujan bound for these graphs, though they do have that property. Nevertheless, we will be able to prove that they form a family of expanders with a quite good explicit asymptotic estimate on the spectral gap. This estimate is strong enough to provide explicit solutions to two outstanding problems in graph theory that we describe as follows:

**0.11.11. Definition.** Let $X$ be a graph.

(a) The *girth* of $X$, denoted by $g(X)$, is the length of the shortest circuit in $X$.
(b) The *chromatic number* of $X$, denoted by $\chi(X)$, is the minimal number of colors needed to paint the vertices of $X$ in such a way that adjacent vertices have different colors.

The problem of the existence of finite graphs with large girth and at the same time large chromatic number has a long history (see [7]). The problem was first solved by Erdös [24], whose solution shows that the "random graph" has this property; this construction is recalled in section 1.7. (This paper was the genesis of the "random method" and theory of random graphs. See the monograph [4].) We shall see in section 4.4 that the graphs $X^{p,q}$ presented in Chapter 4 provide explicit solutions to this problem.

**0.12.12. Definition.** Let $(X_m)_{m\geq 1}$ be a family of finite, connected, $k$-regular graphs, with $|V_m| \to +\infty$ as $m \to +\infty$. We say that this family has *large girth* if, for some constant $C > 0$, one has $g(X_m) \geq (C + o(1)) \log_{k-1} |V_m|$, where $o(1)$ is a quantity tending to 0 for $m \to +\infty$.

It is easy to see that, necessarily, $C \leq 2$. By counting arguments, Erdös and Sachs [25] proved the existence of families of graphs with large girth and with $C = 1$. In the Appendix, we give a beautiful explicit construction due to Margulis [45], leading to $C = \frac{1}{3} \frac{\log 3}{\log\left(1+\sqrt{2}\right)} = 0.415\ldots$. In section 4.3, we shall see that the graphs $X^{p,q}$, with $p$ not a square modulo $q$, provide a family

with large girth and that $C = \frac{4}{3}$ which, asymptotically, is the largest girth known.

We claimed previously that our constructions are "elementary": since there is no general agreement on the meaning of this word, we feel committed to clarify it somewhat. In 1993, the first two authors wrote up a set of unpublished Notes that were circulated under the title "An elementary approach to Ramanujan graphs." In 1998–99, the third author based an undergraduate course on these Notes; in the process he was able to simplify the presentation even further. This gave the impetus for the present text. We assume that our reader is familiar with linear algebra, congruences, finite fields of prime order, and some basic ring theory. The relevant number theory is presented in Chapter 2; and the group theory, including representation theory, in Chapter 3.

Other than these topics, we have attempted to present here a self-contained treatment of the construction and proofs involved. To do this we have borrowed some of our exposition from well-known sources, adapting and tailoring those to give a more concise presentation of the contexts and specific theoretical tools we need. In all such cases, we hope that we have provided clear and complete attribution of sources for those readers who wish to pursue any topic more broadly.

There is some novelty in our approach.

- The graphs $X^{p,q}$ depend on two distinct, odd primes $p, q$. In the literature, it is commonly assumed that $p \equiv 1 \pmod 4$, for simplicity. We give a complete treatment of both the case $p \equiv 1 \pmod 4$ and the case $p \equiv 3 \pmod 4$.
- As in [42], [44], and [57], we give two constructions of the graphs $X^{p,q}$: one is based on quaternion algebras and produces connected graphs by construction; however, it gives little information about the number of vertices; the other describes the $X^{p,q}$ as Cayley graphs of $\mathrm{PGL}_2(q)$ or $\mathrm{PSL}_2(q)$, from which the number of vertices is obvious but connectedness is not. The isomorphism of both constructions, in the original paper [42] (and also in Proposition 3.4.1 in [57]), depends on fairly deep results of Malisěv [43] on the Hardy–Littlewood theory of quadratic forms. The proof in Theorem 7.4.3 of [41] appeals to Kneser's strong approximation theorem for algebraic groups over the adèles. In our approach here, we first give *a priori* estimates on the girth of the graphs obtained by the first method, showing that the girth cannot be too small. We then apply a result of Dickson [20], reproved in section 3.3, that up to two exceptions, proper subgroups of $\mathrm{PSL}_2(q)$ are metabelian, so that Cayley graphs of proper subgroups must have small girth. This is

enough to conclude that our Cayley graphs of $\mathrm{PGL}_2(q)$ or $\mathrm{PSL}_2(q)$ must be connected.

- The proof we give here that the $X^{p,q}$'s, with fixed $p$, form a family of expanders depends on a result going back to Frobenius [27], and is proved in section 3.5: any nontrivial representation of $\mathrm{PSL}_2(q)$ has degree at least $\frac{q-1}{2}$. As a consequence, the multiplicity of any nontrivial eigenvalue of $X^{p,q}$ is at least $\frac{q-1}{2}$. Using the fact that $\frac{q-1}{2}$ is fairly large compared to $q^3$, the approximate number of vertices, we deduce that there must be a spectral gap.

  The idea of trying to exploit this feature of the representations of $\mathrm{PSL}_2(q)$ was suggested by Bernstein and Kazhdan (see [8] and [58]). In Sarnak and Xue [59], this lower bound for the multiplicity is combined with some upper-bound counting arguments to rule out exceptional eigenvalues of quotients of the Lobachevski upper half-plane by congruence subgroups in co-compact arithmetic lattices in $\mathrm{SL}_2(\mathbb{R})$. Our proof of the spectral gap in these notes is based on similar ideas. This method has also been used recently by Gamburd [29] to establish a spectral gap property for certain families of infinite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Most of the exercices in this book were provided by Nicolas Louvet, who was the third author's teaching assistant: we heartily thank him for that. We also thank J. Dodziuk, F. Labourie, F. Ledrappier, and J.-P. Serre for useful comments, conversations, and correspondence.

The draft of this book was completed during a stay of the first author at the University of Roma La Sapienza and of the third author at IHES in the Fall of 1999. It was also at IHES that the book was typed, with remarkable efficiency, by Mrs Cécile Gourgues. We thank her for her beautiful job.

# Chapter 1

## Graph Theory

### 1.1. The Adjacency Matrix and Its Spectrum

We shall be concerned with graphs $X = (V, E)$, where $V$ is the set of vertices and $E$ is the set of edges. As stated in the Overview, we always assume our graphs to be undirected, and most often we will deal with finite graphs.

We let $V = \{v_1, v_2, \ldots\}$ be the set of vertices of $X$. Then the *adjacency matrix* of the graph $X$ is the matrix $A$ indexed by pairs of vertices $v_i, v_j \in V$. That is, $A = (A_{ij})$, where

$$A_{ij} = \text{number of edges joining } v_i \text{ to } v_j.$$

We say that $X$ is *simple* if there is at most one edge joining adjacent vertices; hence, $X$ is simple if and only if $A_{ij} \in \{0, 1\}$ for every $v_i, v_j \in V$.

Note that $A$ completely determines $X$ and that $A$ is symmetric because $X$ is undirected. Furthermore, $X$ has no loops if and only if $A_{ii} = 0$ for every $v_i \in V$.

**1.1.1. Definition.** Let $k \geq 2$ be an integer. We say that the graph $X$ is *$k$-regular* if for every $v_i \in V : \sum_{v_j \in V} A_{ij} = k$.

If $X$ has no loop, this amounts to saying that each vertex has exactly $k$ neighbors.

Assume that $X$ is a finite graph on $n$ vertices. Then $A$ is an $n$-by-$n$ symmetric matrix; hence, it has $n$ real eigenvalues, counting multiplicities, that we may list in decreasing order:

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

The *spectrum* of $X$ is the set of eigenvalues of $A$. Note that $\mu_0$ is a simple eigenvalue, or has multiplicity 1, if and only if $\mu_0 > \mu_1$.

For an arbitrary graph $X = (V, E)$, consider functions $f : V \to \mathbb{C}$ from the set of vertices of $X$ to the complex numbers, and define

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

The space $\ell^2(E)$ is defined analogously.

Clearly, if $V$ is finite, say $|V| = n$, then every function $f : V \to \mathbb{C}$ is in $\ell^2(V)$. We can think of each such function as a vector in $\mathbb{C}^n$ on which the adjacency matrix acts in the usual way:

$$Af = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ \vdots & \vdots & & \vdots \\ A_{i1} & A_{i2} & \dots & A_{in} \\ \vdots & \vdots & & \vdots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} f(v_1) \\ f(v_2) \\ \vdots \\ f(v_n) \end{pmatrix}$$

$$= \begin{pmatrix} A_{11}\, f(v_1) + A_{12}\, f(v_2) + \cdots + A_{1n}\, f(v_n) \\ \vdots \\ A_{i1}\, f(v_1) + A_{i2}\, f(v_2) + \cdots + A_{in}\, f(v_n) \\ \vdots \\ A_{n1}\, f(v_1) + A_{n2}\, f(v_2) + \cdots + A_{nn}\, f(v_n) \end{pmatrix}.$$

Hence, $(Af)(v_i) = \sum_{j=1}^{n} A_{ij}\, f(v_j)$. It is very convenient, both notationally and conceptually, to forget about the numbering of vertices and to index matrix entries of $A$ directly by pairs of vertices. So we shall represent $A$ by a matrix $(A_{xy})_{x,y \in V}$, and the previous formula becomes $(Af)(x) = \sum_{y \in V} A_{xy}\, f(y)$, for every $x \in V$.

**1.1.2. Proposition.** Let $X$ be a finite $k$-regular graph with $n$ vertices. Then

(a) $\mu_0 = k$;
(b) $|\mu_i| \leq k$ for $1 \leq i \leq n - 1$;
(c) $\mu_0$ has multiplicity 1, if and only if $X$ is connected.

*Proof.* We prove (a) and (b) simultaneously by noticing first that the constant function $f \equiv 1$ on $V$ is an eigenfunction of $A$ associated with the eigenvalue $k$. Next, we prove that, if $\mu$ is any eigenvalue, then $|\mu| \leq k$. Indeed, let $f$ be

a real-valued eigenfunction associated with $\mu$. Let $x \in V$ be such that

$$|f(x)| = \max_{y \in V} |f(y)|.$$

Replacing $f$ by $-f$ if necessary, we may assume $f(x) > 0$. Then

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

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

Cancelling out $f(x)$ gives the result.

To prove (c), assume first that $X$ is connected. Let $f$ be a real-valued eigenfunction associated with the eigenvalue $k$. We have to prove that $f$ is constant. As before, let $x \in V$ be a vertex such that $|f(x)| = \max_{y \in V} |f(y)|$. As $f(x) = \frac{(Af)(x)}{k} = \sum_{y \in V} \frac{A_{xy}}{k}\, f(y)$, we see that $f(x)$ is a convex combination of real numbers which are, in modulus, less than $|f(x)|$. This implies that $f(y) = f(x)$ for every $y \in V$, such that $A_{xy} \neq 0$, that is, for every $y$ adjacent to $x$. Then, by a similar argument, $f$ has the same value $f(x)$ on every vertex adjacent to such a $y$, and so on. Since $X$ is connected, $f$ must be constant.

We leave the proof of the converse as an exercise. □

Proposition 1.1.2(c) shows a first connection between spectral properties of the adjacency matrix and combinatorial properties of the graph. This is one of the themes of this chapter.

**1.1.3. Definition.** A graph $X = (V, E)$ is *bipartite*, or *bicolorable*, if there exists a partition of the vertices $V = V_+ \cup V_-$, such that, for any two vertices $x, y$ with $A_{xy} \neq 0$, if $x \in V_+$ (resp. $V_-$), then $y \in V_-$ (resp. $V_+$).

In other words, it is possible to paint the vertices with two colors in such a way that no two adjacent vertices have the same color. Bipartite graphs have very nice spectral properties characterized by the following:

**1.1.4. Proposition.** Let $X$ be a connected, $k$-regular graph on $n$ vertices. The following are equivalent:

(i) $X$ is bipartite;
(ii) the spectrum of $X$ is symmetric about 0;
(iii) $\mu_{n-1} = -k$.