Preface

For now, think of a graph $\Gamma = (V, E)$ as a pair of sets: V is a finite set of points, called vertices, and E is a finite set of pairs of vertices, called edges.

If the edges of Γ are labeled

$$E = \{e_1, e_2, \ldots, e_m\},$$

the vertices of Γ are labeled

$$V = \{v_1, v_2, \ldots, v_n\},$$

let

$$C^0(\Gamma, \mathbb{C}) = \{f \mid f : V \to \mathbb{C}\},$$

and let

$$C^1(\Gamma, \mathbb{C}) = \{f \mid f : E \to \mathbb{C}\},$$

where $\mathbb{C}$ denotes the field of complex numbers. We can identify $C^0(\Gamma, \mathbb{C})$ with the vector space $\mathbb{C}^n$ via the map $f \mapsto (f(v_1), f(v_2), \ldots, f(v_n))$. We can identify $C^1(\Gamma, \mathbb{C})$ with the vector space $\mathbb{C}^m$ via the map $f \mapsto (f(e_1), f(e_2), \ldots, f(e_m))$.

The goal this book is to illustrate and explore connections between graph theory and diverse fields of mathematics such as

- calculus on manifolds,
- group theory,
- algebraic curves,
- Fourier analysis,
- cryptography,

and other areas of combinatorics.

For an excellent (and free!) introduction to more basic discrete mathematics, also using SageMath, see the book by Doerr and Lavasseur [DL17].

Graph theory and calculus

How can these be similar? One deals with a finite set of vertices and edges, the other deals with functions on the (infinite) real line.

You are all familiar with the usual definition of the derivative of a function $f : \mathbb{R} \to \mathbb{R}$ (where $\mathbb{R}$ denotes the real numbers):

$$f'(a) = \lim_{\varepsilon \to 0} \frac{f(a+\varepsilon) - f(a)}{\varepsilon}, \qquad a \in \mathbb{R}.$$

We want to replace this by either a function $f : V \to \mathbb{R}$, or a function $g : E \to \mathbb{R}$, and find an analogous definition. Before proceeding, we need to assume that the graph is "oriented". That is, we assume that each edge $e \in E$ has a "head" $h(e)$ and a "tail" $t(e)$. Roughly speaking, for any pair of neighboring vertices (i.e., two vertices which are connected by an edge), there is a well-defined direction to travel from one to the other. If the vertices of a graph is the set $V = \{0, 1, \ldots, n-1\}$ then the default orientation of an edge $e = (u, v)$ is defined by $h(e) = \max\{u, v\}$, $t(e) = \min\{u, v\}$.

One way to proceed is to define, for $f : V \to \mathbb{R}$, the derivative by

$$f'(e) = f(h(e)) - f(t(e)).$$

In this case and for the usual definition from calculus, we look at a difference of values of f at nearby points.

If $f \in C^0(\Gamma, \mathbb{C})$ is identified with the column vector

$$\vec{f} = \begin{pmatrix} f(v_1) \\ f(v_2) \\ \vdots \\ f(v_n) \end{pmatrix},$$

then the derivative map $f \to f'$ may be regarded as an $m \times n$ matrix, M. Indeed, the entries of this matrix are

$$M_{i,j} = \begin{cases} 1, & \text{if } v_j = h(e_i), \\ -1, & \text{if } v_j = t(e_i), \\ 0, & \text{otherwise.} \end{cases}$$

(By the way, this matrix is the transpose of the incidence matrix, and will be studied in more detail in later chapters.)

Another way to proceed is to define, for $g \in C^1(\Gamma, \mathbb{C})$, the derivative by

$$g'(v) = \sum_{e \in E, h(e)=v} g(e) - \sum_{e \in E, t(e)=v} g(e).$$

If we think of two edges as "nearby" if they share a vertex then this definition also is a difference of values of the function at nearby points.

If the edges and vertices are labeled as before, and if $g \in C^1(\Gamma, \mathbb{C})$ is identified with the column vector

$$\vec{g} = \begin{pmatrix} g(e_1) \\ g(e_2) \\ \vdots \\ g(e_m) \end{pmatrix},$$

then the derivative map $g \to g'$ may be regarded as an $n \times m$ matrix, B. Indeed, the entries of this matrix are

$$B_{i,j} = \begin{cases} 1, & \text{if } v_i = h(e_j), \\ -1, & \text{if } v_i = t(e_j), \\ 0, & \text{otherwise.} \end{cases}$$

Notice that $M_{i,j} = B_{j,i}$. In other words, one is the transpose matrix of the other, $B = M^t$. The two definitions which seemed so different are in fact in some sense dual to one another.

In §3.3 we introduce the notion of a graph morphism $\phi : \Gamma_2 \to \Gamma_1$ between connected graphs Γ_2 and Γ_1, whose distinguishing property is that it must behave well with respect to the corresponding incidence matrices B_2 and B_1. For example, in §3.3.3 we show that $B_2^t \Phi_V = \Phi_E B_1^t$, where Φ_V is a matrix describing the vertex map of ϕ, with rows indexed by vertices of Γ_2 and columns indexed by vertices of Γ_1, and Φ_E is a matrix describing the edge map of ϕ, with rows indexed by edges of Γ_2 and columns indexed by edges of Γ_1.

Graph theory and groups

There are several well-known constructions of graphs arising from a finite group G. These so-called Cayley graphs are named for Arthur Cayley[1]. It's not hard to show that the Cayley graph of a permutation group and a set of generators is connected.

[1] Cayley, 1821–1895, worked for 14 years as a lawyer before his election to the Sadleirian Professorship at Cambridge University.

Let X be a finite set, let $S = \{g_1, g_2, \ldots, g_n\}$ be a set of permutations of X, and let G be the permutation group generated by them:

$$G = \langle g_1, g_2, \ldots, g_n \rangle \subset S_X,$$

where S_X denotes the symmetric group on X. If S is, in addition, a *symmetric* generating set (meaning that it is closed under inverses) then we define the *Cayley graph* of G with respect to S to be the graph

$$\Gamma = Cay(G, S) = (V, E),$$

whose vertices V are the elements of G and whose edges are determined by the following condition: if x and y are vertices in $V = G$ then there is an edge $e = (x, y)$ from x to y in Γ if and only if $y = g_i x$, for some $i = 1, 2, \ldots, n$.

Cayley graphs encode group-theoretic information about G, as the following example shows.

Example. The Cayley graph of the Rubik's cube group. Let

$$G = \langle R, L, U, D, F, B \rangle \subset S_{54}$$

be the group of the $3 \times 3 \times 3$ Rubik's Cube generated by the quarter-turn moves, where S_{54} is the symmetric group on the 54 facets of the cube, and R denotes the move which rotates the Right face of the cube a quarter-turn counterclockwise (and similarly for Left, Up, Down, Front, Back).

Let

$$S = \{R, L, U, D, F, B, R^{-1}, L^{-1}, U^{-1}, D^{-1}, F^{-1}, B^{-1}\}.$$

The associated Cayley graph $\Gamma_{QT} = Cay(G, S)$ is called the Cayley graph of the cube in the quarter-turn metric. Each position of the cube corresponds to a unique element of the group G (i.e., the move you had to make to get to that position), hence to a unique vertex of the Cayley graph. Note each vertex of this graph has degree 12.

Let

$$S = \{R, L, U, D, F, B, R^2, L^2, U^2, D^2, F^2, B^2, R^{-1}, L^{-1}, U^{-1}, D^{-1}, F^{-1}, B^{-1}\}.$$

The associated Cayley graph $\Gamma_{FT} = Cay(G, S)$ is called the *Cayley graph of the cube in the faceturn metric.*

Moreover, a solution of the Rubik's cube is simply a path in the graph from the vertex associated to the present position of the cube to the vertex associated to the identity element. The number of moves in the shortest possible solution is simply the distance from the vertex associated to the present position of the cube to the vertex associated to the identity element. The

diameter of the Cayley graph of G is the number of moves in the best possible solution in the worst possible case.

Thanks to years of hard work, led by computer scientist Tomas Rokicki, the diameter of Γ_{QT} is now known to be 26, and the diameter of Γ_{FT} is now known to be 20 [J15].

Graph theory and algebraic curves

There are a number of analogies between graphs and algebraic curves over a finite field. Each has a notion of a genus, there are harmonic mappings between graphs and between curves, each has a Picard group, each has a zeta function, and so on. Several sections in this book explore this connection, for example, §1.2.2, §1.2.3, and Chapter 3.

Let X be a smooth projective curve over an algebraically closed field F. Let $F(X)$ denote the function field of X (the field of rational functions on X) and $F(X)^\times = F(X) - \{0\}$ its group of units. If D is any divisor on X (i.e., a formal sum of points in X) then the *Riemann–Roch space* $L(D)$ is a finite dimensional F-vector space given by

$$L(D) = \{f \in F(X)^\times \mid div(f) + D \geq 0\} \cup \{0\},$$

where $div(f)$ denotes the (principal) divisor of the function f.

The Riemann–Roch space $L(D)$ may be regarded as a vector space of rational functions with prescribed zeroes and allowed poles on X. Let $\ell(D) = \dim(L(D))$ denote its dimension. We recall the *Riemann–Roch theorem*,

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g,$$

where K denotes a canonical divisor, $\deg(D)$ the degree of D, and g the genus of X.

There is an analogous Riemann–Roch theorem for graphs as well. The graph-theoretic analog is described in Chapter 3, "Graphs as Manifolds," below.

A finite graph has a Jacobian group, analogous to the Jacobian (abelian) variety of an algebraic curve (see §4.6). The Jacobian group, also called the critical group, has cardinality equal to the number of spanning trees of the graph (see Proposition 4.9.15 and Corollary 4.9.16).

In algebraic geometry, one studies nice maps between varieties that induce maps on certain structures on the varieties. What is the graph-theoretic analog of a nice map between algebraic curves? This is a harmonic morphism of graphs (see §3.3.2), which induces a surjective pushforward map and an injective pullback map of the corresponding Jacobian groups (see §4.8).

What is the graph-theoretic analog of the zeta function (see [La70]) of an algebraic curve over a finite field? One analog is the Duursma zeta function of a graph discussed in §1.2.3 below.

Graph theory and Fourier transforms

The theory of Fourier series is a part of a branch of mathematics called harmonic analysis. Given a manifold X with a Laplacian operator $\Delta = \Delta_X$, harmonic analysis, roughly speaking, seeks to express the functions on X as expansions in terms of the eigenfunctions of Δ, then to derive consequences from this "Fourier series." Can this general motif carry over to graph theory? In Chapter 2, we discuss some connections between the spectrum of the Laplacian $Q = Q_\Gamma$ of the graph and the graph Γ itself. In the simple case of circulant graphs, we even show (see §2.4) that functions on the graph can be expressed as expansions in terms of the eigenfunctions of the Laplacian.

Historically, Fourier series were discovered by J. Fourier, a French mathematical physicist[2].

To have a Fourier series, you must be given two things: (1) a period $P = 2L$, and (2) a suitably behaved function $f(x)$ defined on an interval of length $2L$, say $-L < x < L$. The Fourier series of $f(x)$ with period $2L$ is

$$FS(f)(x) = \sum_{n=-\infty}^{\infty} a_n \exp\left(\frac{n\pi xi}{L}\right),$$

where a_n is given by the integral formula[3],

$$a_n = \frac{1}{2L}\int_{-L}^{L} f(x)\exp\left(\frac{-n\pi xi}{L}\right) dx. \tag{1}$$

The Fourier operator $f \mapsto FS(f)$ has eigenvectors $\exp(\frac{n\pi xi}{L})$.

Graph-theoretic Fourier series

For the cycle graph on n vertices, Γ_n, the eigenvalues of the adjacency matrix are $\lambda_k = 2\cos(2\pi k/n)$, for $0 \le k \le n-1$, with eigenvectors $v_k = (\exp(\pi jki/n))_{j\in\{0,\dots,n-1\}}$. These λ's are not all distinct but the multiplicities can be described as follows.

- (n even) The only eigenvalues of Γ_n which occur with multiplicity 1 are 2 and -2. The eigenvalues $2\cos(2\pi k/n)$, for $1 \le k \le \frac{n-2}{2}$, all occur with multiplicity 2.

[2] Physics was not Fourier's only profession. Indeed, Napoleon selected Fourier to be his scientific advisor during France's invasion of Egypt in the late 1700s, where he oversaw some large construction projects, such as highways and bridges. During this time, Fourier developed the theory of trigonometric series (now called Fourier series) to solve the heat equation.

[3] These formulas were not known to Fourier. To compute the Fourier coefficients he used sometimes ingenious roundabout methods involving large systems of equations.

• (n odd) The only eigenvalue of Γ_n which occurs with multiplicity 1 is 2. The eigenvalues $2\cos(2\pi k/n)$, for $1 \le k \le \frac{n-1}{2}$, all occur with multiplicity 2.

For example, the graph Γ_8 has eigenvalues (counted according to their multiplicity) 2, $\sqrt{2}$, $\sqrt{2}$, 0, 0, $-\sqrt{2}$, $-\sqrt{2}$, -2.

We identify the vertices V of a cycle graph Γ having n vertices with the abelian group of integers mod n, $\mathbb{Z}/n\mathbb{Z}$. If $\mathbb{C}$ denotes the field of complex numbers, let

$$C^0(\Gamma, \mathbb{C}) = \{f \mid f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}\}.$$

This is a complex vector space which we can identify with the vector space $\mathbb{C}^n$ via the map $f \mapsto (f(0), f(1), \ldots, f(n-1))$.

Let $\zeta = \zeta_n = e^{2\pi i/n}$ denote an n^{th} root of unity in $\mathbb{C}$. Recall, for $g \in C^0(\Gamma, \mathbb{C})$, the *discrete Fourier transform* of g is the function $\mathcal{F}_n g \in C^0(\Gamma, \mathbb{C})$ (also written $g^\wedge$) defined by

$$(\mathcal{F}_n g)(\lambda) = g^\wedge(\lambda) = \sum_{\ell \in \mathbb{Z}/n\mathbb{Z}} g(\ell)\zeta^{\ell\lambda},\ \lambda \in \mathbb{Z}/n\mathbb{Z}.$$

If $G \in C^0(\Gamma, \mathbb{C})$, the *inverse discrete Fourier transform* of G is the function $(\mathcal{F}_n^{-1} G) \in C^0(\Gamma, \mathbb{C})$ (also written $G^\vee$) defined by

$$(\mathcal{F}_n^{-1} G)(\ell) = G^\vee(\ell) = \frac{1}{n} \sum_{\lambda \in \mathbb{Z}/n\mathbb{Z}} G(\lambda)\zeta^{-\ell\lambda},\ \ell \in \mathbb{Z}/n\mathbb{Z}.$$

Using this, any function in $C^0(\Gamma, \mathbb{C})$ has an expansion in terms of the eigenvectors of the Laplacian.

Graph theory and cryptography

In Chapter 6, we explore a fascinating connection between graph theory, combinatorics, and cryptography.

Let $GF(p)$ be the prime field of characteristic p and let $d > 1$. A function $GF(2)^d \to GF(2)$ is a *Boolean function* on d variables. A function $GF(p)^d \to GF(p)$ is a *p-ary function* on d variables. Let

$$supp(f) = \{v \in V \mid f(v) \neq 0\}$$

denote the *support* of f, where $V = GF(p)^d$.

The set of invertible $n \times n$ matrices having coefficients in the field $GF(p)$ is denoted $GL(n, p)$. This set is a group under matrix multiplication. The group $GL(d, p)$ acts on the set of p-ary functions $f : GF(p)^d \to GF(p)$ by

$$g : f \mapsto f^g,$$

where

$$f^g(x) = f(gx), \quad x \in GF(p)^d.$$

It preserves the subspaces of (a) affine functions, (b) even functions, and (c) functions for which $f(0) = 0$.

Let p be a prime. A *general feedback shift register* is a map

$$C : GF(p)^d \to GF(p),$$

which, given initial values $x_0, \ldots, x_{d-1}$, gives rise to a sequence $x_0, \ldots, x_n, \ldots$, where $x_n = C(x_{n-d}, \ldots, x_{n-1})$ for $n \geq d$. When C is a linear function, iterating the map C generates a *linear feedback shift register* (LFSR). These are pseudorandom sequences in $GF(p)$ with long periods. Unfortunately, while LFSRs have some good pseudorandomness properties, they are not very secure. Here is one way to fix this. Consider a periodic sequence of period P,

$$x = x_0, \ldots, x_n, \ldots,$$

for example, a LFSR. Given $F : GF(p)^d \to GF(p)$, construct a filtered sequence by setting

$$y_i = F(x_{i-d}, \ldots, x_{i-1}),$$

for $i \geq d$, and $y_i = x_i$ for $0 \leq i \leq d-1$. For suitably chosen F, these can be used to build secure stream ciphers.

What kind of function f makes a good filter function? A very nonlinear one. How to measure nonlinearity? One way is with a finite field analog of the Fourier transform. The *Walsh–Hadamard transform* of a $GF(p)$-valued function f is a complex-valued function on $V = GF(p)^d$ that can be defined as

$$W_f(u) = \sum_{x \in V} \zeta^{f(x) - \langle u, x \rangle},$$

where $\zeta = e^{2\pi i/p}$.

The Walsh transform of an affine function is a "spike" (supported at a single vector).

We call f *bent* if

$$|W_f(u)| = p^{n/2},$$

for all $u \in V$. In some sense, bent functions are maximally nonlinear. Bent functions are good filter functions (F above).

There is an interesting connection between bent functions and combinatorial structures called difference sets. The Dillon correspondence states that a function $f : GF(2)^d \to GF(2)$ is bent if and only if $f^{-1}(1)$ is an elementary Hadamard difference set of $GF(2)^n$.

There is also an interesting connection between bent functions and graph theory. The Bernasconi–Codenotti–VanderKam correspondence states that a function $f : GF(2)^d \to GF(2)$ is bent if and only if the Cayley graph of f is a strongly regular graph having parameters $(2^d, k, \lambda, \lambda)$ for some λ, where $k = |supp(f)|$. (In fact, the values of λ are known more explicitly.)

Is there a weighted analog, for $p > 2$, of the Dillon and Bernasconi–Codenotti–VanderKam correspondences? Questions of this sort are studied further in Chapter 6.

Graph theory and error-correcting codes

There are several well-known constructions of error-correcting codes that arise from a graph. Roughly speaking, an error-correcting code is a subset $C \subset GF(q)^n$ (where $GF(q)$ is a finite field having q elements), for which different elements are distinct enough that a small number of errors can be corrected by a suitable decoding algorithm.

For example, there is the binary code which is generated by the rows of the incidence matrix of a graph. There are also error-correcting codes over a finite field $GF(q)$ arising from cycles or cocycles of a graph. And there are expander codes constructed from specially constructed Cayley graphs.

Constructions in the other direction, graphs from codes, are less well known, but here's an example. Let $C \subset GF(2)^n$ denote an error-correcting code with (full rank) $k \times n$ generator matrix G. Let $f_i : GF(2)^n \to GF(2)$ denote the function supported on the i-th row of G, let

$$f = f_1 + \ldots + f_k,$$

and let Γ be the Cayley graph of f. In other words, the vertices of Γ are the vectors in $GF(2)^n$, and $e = (v, w) \in GF(2)^n \times GF(2)^n$ is an edge if and only if $f(v - w) \neq 0$. The code C corresponds in a natural way to the connected component of Γ containing the 0-vector. This is a k-regular, distance-regular graph.

There is a similar construction where we replace the rows of G by the columns of G, but we must assume that the columns don't contain the 0-vector. See §6.15 below for more details.

Note on using Sage: Some Sage commands used in this book use modules written for this book and uploaded to the github site for this book (https://github.com/springer-math/adventures-in-graph-theory).

http://www.springer.com/978-3-319-68381-2

Adventures in Graph Theory

Joyner, D.; Melles, C.G.
2017, XXVI, 327 p. 80 illus., 56 illus. in color., Hardcover
ISBN: 978-3-319-68381-2
A product of Birkhäuser Basel