

Chapter 2

Cubes and the Radon Transform

Let us now consider a more interesting example of a graph G , one whose eigenvalues have come up in a variety of applications. Let \mathbb{Z}_2 denote the cyclic group of order 2, with elements 0 and 1 and group operation being addition modulo 2. Thus $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, and $1 + 1 = 0$. Let \mathbb{Z}_2^n denote the direct product of \mathbb{Z}_2 with itself n times, so the elements of \mathbb{Z}_2^n are n -tuples (a_1, \dots, a_n) of 0's and 1's, under the operation of component-wise addition. Define a graph C_n , called the n -cube, as follows: the vertex set of C_n is given by $V(C_n) = \mathbb{Z}_2^n$, and two vertices u and v are connected by an edge if they differ in exactly one component. Equivalently, $u + v$ has exactly one nonzero component. If we regard \mathbb{Z}_2^n as consisting of *real* vectors, then these vectors form the set of vertices of an n -dimensional cube. Moreover, two vertices of the cube lie on an edge (in the usual geometric sense) if and only if they form an edge of C_n . This explains why C_n is called the n -cube. We also see that walks in C_n have a nice geometric interpretation—they are simply walks along the edges of an n -dimensional cube.

We want to determine explicitly the eigenvalues and eigenvectors of C_n . We will do this by a somewhat indirect but extremely useful and powerful technique, the finite Radon transform. Let \mathcal{V} denote the set of all functions $f: \mathbb{Z}_2^n \rightarrow \mathbb{R}$, where \mathbb{R} denotes the field of real numbers.¹ Note that \mathcal{V} is a vector space over \mathbb{R} of dimension 2^n [why?]. If $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$ are elements of \mathbb{Z}_2^n , then define their *dot product* by

$$u \cdot v = u_1 v_1 + \dots + u_n v_n, \quad (2.1)$$

where the computation is performed modulo 2. Thus we regard $u \cdot v$ as an element of \mathbb{Z}_2 . The expression $(-1)^{u \cdot v}$ is defined to be the *real number* $+1$ or -1 , depending on whether $u \cdot v = 0$ or 1 , respectively. Since for integers k the value of $(-1)^k$

¹For abelian groups other than \mathbb{Z}_2^n it is necessary to use complex numbers rather than real numbers. We could use complex numbers here, but there is no need to do so.

depends only on $k \pmod{2}$, it follows that we can treat u and v as integer vectors without affecting the value of $(-1)^{u \cdot v}$. Thus, for instance, formulas such as

$$(-1)^{u \cdot (v+w)} = (-1)^{u \cdot v + u \cdot w} = (-1)^{u \cdot v} (-1)^{u \cdot w}$$

are well defined and valid. From a more algebraic viewpoint, the map $\mathbb{Z} \rightarrow \{-1, 1\}$ sending n to $(-1)^n$ is a group homomorphism, where of course the product on $\{-1, 1\}$ is multiplication.

We now define two important bases of the vector space \mathcal{V} . There will be one basis element of each basis for each $u \in \mathbb{Z}_2^n$. The first basis, denoted B_1 , has elements f_u defined as follows:

$$f_u(v) = \delta_{uv}, \quad (2.2)$$

the Kronecker delta. It is easy to see that B_1 is a basis, since any $g \in \mathcal{V}$ satisfies

$$g = \sum_{u \in \mathbb{Z}_2^n} g(u) f_u \quad (2.3)$$

[why?]. Hence B_1 spans \mathcal{V} , so since $\#B_1 = \dim \mathcal{V} = 2^n$, it follows that B_1 is a basis. The second basis, denoted B_2 , has elements χ_u defined as follows:

$$\chi_u(v) = (-1)^{u \cdot v}.$$

In order to show that B_2 is a basis, we will use an inner product on \mathcal{V} (denoted $\langle \cdot, \cdot \rangle$) defined by

$$\langle f, g \rangle = \sum_{u \in \mathbb{Z}_2^n} f(u) g(u).$$

Note that this inner product is just the usual dot product with respect to the basis B_1 .

2.1 Lemma. *The set $B_2 = \{\chi_u : u \in \mathbb{Z}_2^n\}$ forms a basis for \mathcal{V} .*

Proof. Since $\#B_2 = \dim \mathcal{V} (= 2^n)$, it suffices to show that B_2 is linearly independent. In fact, we will show that the elements of B_2 are orthogonal.² We have

$$\begin{aligned} \langle \chi_u, \chi_v \rangle &= \sum_{w \in \mathbb{Z}_2^n} \chi_u(w) \chi_v(w) \\ &= \sum_{w \in \mathbb{Z}_2^n} (-1)^{(u+v) \cdot w}. \end{aligned}$$

²Recall from linear algebra that nonzero orthogonal vectors in a real vector space are linearly independent.

It is left as an easy exercise to the reader to show that for any $y \in \mathbb{Z}_2^n$, we have

$$\sum_{w \in \mathbb{Z}_2^n} (-1)^{y \cdot w} = \begin{cases} 2^n, & \text{if } y = \mathbf{0}, \\ 0, & \text{otherwise,} \end{cases}$$

where $\mathbf{0}$ denotes the identity element of \mathbb{Z}_2^n (the vector $(0, 0, \dots, 0)$). Thus $\langle \chi_u, \chi_v \rangle = 0$ if and only if $u + v = \mathbf{0}$, i.e., $u = v$, so the elements of B_2 are orthogonal (and nonzero). Hence they are linearly independent as desired. \square

We now come to the key definition of the Radon transform.

Given a subset Γ of \mathbb{Z}_2^n and a function $f \in \mathcal{V}$, define a new function $\Phi_\Gamma f \in \mathcal{V}$ by

$$\Phi_\Gamma f(v) = \sum_{w \in \Gamma} f(v + w).$$

The function $\Phi_\Gamma f$ is called the (*discrete or finite*) *Radon transform* of f (on the group \mathbb{Z}_2^n , with respect to the subset Γ).

We have defined a map $\Phi_\Gamma: \mathcal{V} \rightarrow \mathcal{V}$. It is easy to see that Φ_Γ is a linear transformation; we want to compute its eigenvalues and eigenvectors.

2.2 Theorem. *The eigenvectors of Φ_Γ are the functions χ_u , where $u \in \mathbb{Z}_2^n$. The eigenvalue λ_u corresponding to χ_u (i.e., $\Phi_\Gamma \chi_u = \lambda_u \chi_u$) is given by*

$$\lambda_u = \sum_{w \in \Gamma} (-1)^{u \cdot w}.$$

Proof. Let $v \in \mathbb{Z}_2^n$. Then

$$\begin{aligned} \Phi_\Gamma \chi_u(v) &= \sum_{w \in \Gamma} \chi_u(v + w) \\ &= \sum_{w \in \Gamma} (-1)^{u \cdot (v + w)} \\ &= \left(\sum_{w \in \Gamma} (-1)^{u \cdot w} \right) (-1)^{u \cdot v} \\ &= \left(\sum_{w \in \Gamma} (-1)^{u \cdot w} \right) \chi_u(v). \end{aligned}$$

Hence

$$\Phi_\Gamma \chi_u = \left(\sum_{w \in \Gamma} (-1)^{u \cdot w} \right) \chi_u,$$

as desired. \square

Note that because the χ_u 's form a basis for \mathcal{V} by Lemma 2.1, it follows that Theorem 2.2 yields a complete set of eigenvalues and eigenvectors for Φ_Γ . Note also that the eigenvectors χ_u of Φ_Γ are independent of Γ ; only the eigenvalues depend on Γ .

Now we come to the payoff. Let $\Delta = \{\delta_1, \dots, \delta_n\}$, where δ_i is the i th unit coordinate vector (i.e., δ_i has a 1 in position i and 0's elsewhere). Note that the j th coordinate of δ_i is just δ_{ij} (the Kronecker delta), explaining our notation δ_i . Let $[\Phi_\Delta]$ denote the matrix of the linear transformation $\Phi_\Delta: \mathcal{V} \rightarrow \mathcal{V}$ with respect to the basis B_1 of \mathcal{V} given by (2.2).

2.3 Lemma. *We have $[\Phi_\Delta] = A(C_n)$, the adjacency matrix of the n -cube.*

Proof. Let $v \in \mathbb{Z}_2^n$. We have

$$\begin{aligned} \Phi_\Delta f_u(v) &= \sum_{w \in \Delta} f_u(v + w) \\ &= \sum_{w \in \Delta} f_{u+w}(v), \end{aligned}$$

since $u = v + w$ if and only if $u + w = v$. There follows

$$\Phi_\Delta f_u = \sum_{w \in \Delta} f_{u+w}. \quad (2.4)$$

Equation (2.4) says that the (u, v) -entry of the matrix Φ_Δ is given by

$$(\Phi_\Delta)_{uv} = \begin{cases} 1, & \text{if } u + v \in \Delta, \\ 0, & \text{otherwise.} \end{cases}$$

Now $u + v \in \Delta$ if and only if u and v differ in exactly one coordinate. This is just the condition for uv to be an edge of C_n , so the proof follows. \square

2.4 Corollary. *The eigenvectors E_u ($u \in \mathbb{Z}_2^n$) of $A(C_n)$ (regarded as linear combinations of the vertices of C_n , i.e., of the elements of \mathbb{Z}_2^n) are given by*

$$E_u = \sum_{v \in \mathbb{Z}_2^n} (-1)^{u \cdot v} v. \quad (2.5)$$

The eigenvalue λ_u corresponding to the eigenvector E_u is given by

$$\lambda_u = n - 2\omega(u), \quad (2.6)$$

where $\omega(u)$ is the number of 1's in u . (The integer $\omega(u)$ is called the Hamming weight or simply the weight of u .) Hence $A(C_n)$ has $\binom{n}{i}$ eigenvalues equal to $n - 2i$, for each $0 \leq i \leq n$.

Proof. For any function $g \in \mathcal{V}$ we have by (2.3) that

$$g = \sum_v g(v) f_v.$$

Applying this equation to $g = \chi_u$ gives

$$\chi_u = \sum_v \chi_u(v) f_v = \sum_v (-1)^{u \cdot v} f_v. \quad (2.7)$$

Equation (2.7) expresses the eigenvector χ_u of Φ_Δ (or even Φ_Γ for any $\Gamma \subseteq \mathbb{Z}_2^n$) as a linear combination of the functions f_v . But Φ_Δ has the same matrix with respect to the basis of the f_v 's as $A(C_n)$ has with respect to the vertices v of C_n . Hence the expansion of the eigenvectors of Φ_Δ in terms of the f_v 's has the same coefficients as the expansion of the eigenvectors of $A(C_n)$ in terms of the v 's, so (2.5) follows.

According to Theorem 2.2 the eigenvalue λ_u corresponding to the eigenvector χ_u of Φ_Δ (or equivalently, the eigenvector E_u of $A(C_n)$) is given by

$$\lambda_u = \sum_{w \in \Delta} (-1)^{u \cdot w}. \quad (2.8)$$

Now $\Delta = \{\delta_1, \dots, \delta_n\}$ and $\delta_i \cdot u$ is 1 if u has a one in its i th coordinate and is 0 otherwise. Hence the sum in (2.8) has $n - \omega(u)$ terms equal to +1 and $\omega(u)$ terms equal to -1, so $\lambda_u = (n - \omega(u)) - \omega(u) = n - 2\omega(u)$, as claimed. \square

We have all the information needed to count walks in C_n .

2.5 Corollary. *Let $u, v \in \mathbb{Z}_2^n$, and suppose that $\omega(u + v) = k$ (i.e., u and v disagree in exactly k coordinates). Then the number of walks of length ℓ in C_n between u and v is given by*

$$(A^\ell)_{uv} = \frac{1}{2^n} \sum_{i=0}^n \sum_{j=0}^k (-1)^j \binom{k}{j} \binom{n-k}{i-j} (n-2i)^\ell, \quad (2.9)$$

where we set $\binom{n-k}{i-j} = 0$ if $j > i$. In particular,

$$(A^\ell)_{uu} = \frac{1}{2^n} \sum_{i=0}^n \binom{n}{i} (n-2i)^\ell. \quad (2.10)$$

Proof. Let E_u and λ_u be as in Corollary 2.4. In order to apply Corollary 1.2, we need the eigenvectors to be of *unit* length (where we regard the f_v 's as an orthonormal basis of \mathcal{V}). By (2.5), we have

$$|E_u|^2 = \sum_{v \in \mathbb{Z}_2^n} ((-1)^{u \cdot v})^2 = 2^n.$$

Hence we should replace E_u by $E'_u = \frac{1}{2^{n/2}} E_u$ to get an orthonormal basis. According to Corollary 1.2, we thus have

$$(A^\ell)_{uv} = \frac{1}{2^n} \sum_{w \in \mathbb{Z}_2^n} E_{uw} E_{vw} \lambda_w^\ell.$$

Now E_{uw} by definition is the coefficient of f_w in the expansion (2.5), i.e., $E_{uw} = (-1)^{u \cdot w}$ (and similarly for E_v), while $\lambda_w = n - 2\omega(w)$. Hence

$$(A^\ell)_{uv} = \frac{1}{2^n} \sum_{w \in \mathbb{Z}_2^n} (-1)^{(u+v) \cdot w} (n - 2\omega(w))^\ell. \quad (2.11)$$

The number of vectors w of Hamming weight i which have j 1's in common with $u + v$ is $\binom{k}{j} \binom{n-k}{i-j}$, since we can choose the j 1's in $u + v$ which agree with w in $\binom{k}{j}$ ways, while the remaining $i - j$ 1's of w can be inserted in the $n - k$ remaining positions in $\binom{n-k}{i-j}$ ways. Since $(u + v) \cdot w \equiv j \pmod{2}$, the sum (2.11) reduces to (2.9) as desired. Clearly setting $u = v$ in (2.9) yields (2.10), completing the proof. \square

It is possible to give a direct proof of (2.10) avoiding linear algebra, though we do not do so here. Thus by Corollary 1.3 and Lemma 1.7 (exactly as was done for K_n) we have another determination of the eigenvalues of C_n . With a little more work one can also obtain a direct proof of (2.9). Later in Example 9.12, however, we will use the eigenvalues of C_n to obtain a combinatorial result for which a nonalgebraic proof was found only recently and is by no means easy.

2.6 Example. Setting $k = 1$ in (2.9) yields

$$\begin{aligned} (A^\ell)_{uv} &= \frac{1}{2^n} \sum_{i=0}^n \left[\binom{n-1}{i} - \binom{n-1}{i-1} \right] (n-2i)^\ell \\ &= \frac{1}{2^n} \sum_{i=0}^{n-1} \binom{n-1}{i} \frac{(n-2i)^{\ell+1}}{n-i}. \end{aligned}$$

NOTE (for those familiar with the representation theory of finite groups). The functions $\chi_u: \mathbb{Z}_2^n \rightarrow \mathbb{R}$ are just the irreducible (complex) characters of the group \mathbb{Z}_2^n , and the orthogonality of the χ_u 's shown in the proof of Lemma 2.1 is the usual orthogonality relation for the irreducible characters of a finite group. The results of this chapter extend readily to any finite abelian group. Exercise 5 does the case \mathbb{Z}_n , the cyclic group of order n . For nonabelian finite groups the situation is much more complicated because not all irreducible representations have degree one (i.e., are homomorphisms $G \rightarrow \mathbb{C}^*$, the multiplicative group of \mathbb{C}), and there do not exist formulas as explicit as the ones for abelian groups.

We can give a little taste of the situation for arbitrary groups as follows. Let G be a finite group, and let $\mathbf{M}(G)$ be its multiplication table. Regard the entries of $\mathbf{M}(G)$ as *commuting* indeterminates, so that $\mathbf{M}(G)$ is simply a matrix with indeterminate entries. For instance, let $G = \mathbb{Z}_3$. Let the elements of G be a, b, c , where say a is the identity. Then

$$\mathbf{M}(G) = \begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix}.$$

We can compute that $\det \mathbf{M}(G) = (a+b+c)(a+\omega b+\omega^2 c)(a+\omega^2 b+\omega c)$, where $\omega = e^{2\pi i/3}$. In general, when G is abelian, Dedekind knew that $\det \mathbf{M}(G)$ factors into certain explicit linear factors over \mathbb{C} . Theorem 2.2 is equivalent to this statement for the group $G = \mathbb{Z}_2^n$ [why?]. Equation (12.5) gives the factorization for $G = \mathbb{Z}_n$. (For each $w \in G$ one needs to interchange the row indexed by the group element w with the row indexed by w^{-1} in order to convert $\mathbf{M}(\mathbb{Z}_n)$ to the circulant matrices of (12.5), but these operations only affect the sign of the determinant.) Dedekind asked Frobenius about the factorization of $\det \mathbf{M}(G)$, known as the *group determinant*, for nonabelian finite G . For instance, let $G = \mathfrak{S}_3$ (the symmetric group of all permutations of $1, 2, 3$), with elements (in cycle notation) $a = (1)(2)(3)$, $b = (1, 2)(3)$, $c = (1, 3)(2)$, $d = (1, 2, 3)$, $e = (1, 2, 3)$, and $f = (1, 3, 2)$. Then $\det \mathbf{M}(G) = f_1 f_2 f_3^2$, where

$$f_1 = a + b + c + d + e + f,$$

$$f_2 = -a + b + c + d - e - f,$$

$$f_3 = a^2 - b^2 - c^2 - d^2 + e^2 + f^2 - ae - af + bc + bd + cd - ef.$$

Frobenius showed that in general there is a set \mathcal{P} of irreducible homogeneous polynomials f , of some degree d_f , where $\#\mathcal{P}$ is the number of conjugacy classes of G , for which

$$\det \mathbf{M}(G) = \prod_{f \in \mathcal{P}} f^{d_f}.$$

Note that taking the degree of both sides gives $\#G = \sum_f d_f^2$. Frobenius' result was a highlight in his development of group representation theory. The numbers d_f are just the degrees of the irreducible (complex) representations of G . For the symmetric group \mathfrak{S}_n , these degrees are the numbers f^λ of Theorem 8.1, and Appendix 1 of Chap. 8 gives a bijective proof that $\sum_\lambda (f^\lambda)^2 = n!$.

Notes for Chap. 2

The Radon transform first arose in a continuous setting in the paper [90] of Radon and has been applied to such areas as computerized tomography. The finite version was first defined by Bolker [9]. For some further applications to combinatorics see

Kung [67]. For the Radon transform on the n -cube \mathbb{Z}_2^n , see Diaconis and Graham [28]. For the generalization to \mathbb{Z}_k^n , see DeDeo and Velasquez [27].

For an exposition of the development of group representation theory by Frobenius and other pioneers, see the survey articles of Hawkins [54–56].

Exercises for Chap. 2

1. (a) Start with n coins heads up. Choose a coin at random (each equally likely) and turn it over. Do this a total of ℓ times. What is the probability that all coins will have heads up? (Don't solve this from scratch; rather use some previous results.)
 (b) Same as (a), except now compute the probability that all coins have tails up.
 (c) Same as (a), but now we turn over two coins at a time.
2. (a) (difficult) (*) Let $C_{n,k}$ be the subgraph of the cube C_n spanned by all vertices of C_n with $k-1$ or k 1's (so the edges of $C_{n,k}$ consist of all edges of C_n that connect two vertices of $C_{n,k}$; there are a total of $k\binom{n}{k}$ edges). Show that the characteristic polynomial of $A = A(C_{n,k})$ is given by

$$\det(A - xI) = \pm x^{\binom{n}{k} - \binom{n}{k-1}} \prod_{i=1}^k (x^2 - i(n - 2k + i + 1))^{\binom{n}{k-i} - \binom{n}{k-i-1}},$$

where we set $\binom{n}{-1} = 0$.

- (b) Find the number of closed walks in $C_{n,k}$ of length ℓ beginning and ending with a fixed vertex v .
3. (unsolved and unrelated to the text) Let $n = 2k + 1$. Does the graph $C_{n,k+1}$ of Problem 2 above have a Hamiltonian cycle, i.e., a closed path that contains every vertex exactly once? A *closed path* in a graph G is a closed walk that does not repeat any vertices except at the last step.
4. Let G be the graph with vertex set \mathbb{Z}_2^n (the same as the n -cube) and with edge set defined as follows: $\{u, v\}$ is an edge of G if u and v differ in exactly *two* coordinates (i.e., if $\omega(u, v) = 2$). What are the eigenvalues of G ?
5. This problem is devoted to the graph Z_n with vertex set \mathbb{Z}_n (the cyclic group of order n , with elements $0, 1, \dots, n-1$ under the operation of addition modulo n) and edges consisting of all pairs $\{i, i+1\}$ (with $i+1$ computed in \mathbb{Z}_n , so $(n-1)+1 = 0$). The graph Z_n is called an n -cycle. We will develop properties of its adjacency matrix analogously to what was done for the n -cube C_n . It will be necessary to work over the complex numbers \mathbb{C} . Recall that there are exactly n complex numbers z (called n th roots of unity) satisfying $z^n = 1$. They are given by $\zeta^0 = 1, \zeta^1 = \zeta, \zeta^2, \dots, \zeta^{n-1}$, where $\zeta = e^{2\pi i/n}$.
 (a) Draw the graphs Z_3, Z_4 , and Z_5 .

- (b) Let \mathcal{V} be the complex vector space of all functions $f: \mathbb{Z}_n \rightarrow \mathbb{C}$. What is the dimension of \mathcal{V} ?
- (c) (*) If $k \in \mathbb{Z}$, then note that ζ^k depends only on the value of k modulo n . Hence if $u \in \mathbb{Z}_n$ then we can define ζ^u by regarding u as an ordinary integer, and the usual laws of exponents such as $\zeta^{u+v} = \zeta^u \zeta^v$ (where $u, v \in \mathbb{Z}_n$) still hold. For $u \in \mathbb{Z}_n$ define $\chi_u \in \mathcal{V}$ by $\chi_u(v) = \zeta^{uv}$. Let $B = \{\chi_u: u \in \mathbb{Z}_n\}$. Show that B is a basis for \mathcal{V} .
- (d) Given $\Gamma \subseteq \mathbb{Z}_n$ and $f \in \mathcal{V}$, define $\Phi_\Gamma f \in \mathcal{V}$ by

$$\Phi_\Gamma f(v) = \sum_{w \in \Gamma} f(v + w).$$

Show that the eigenvectors of Φ_Γ are the functions χ_u , with corresponding eigenvalue $\lambda_u = \sum_{w \in \Gamma} \zeta^{uw}$.

- (e) Let $\Delta = \{1, n-1\} \subseteq \mathbb{Z}_n$. Define $f_u \in \mathcal{V}$ by $f_u(v) = \delta_{uv}$. Let $F = \{f_u: u \in \mathbb{Z}_n\}$. It is clear that F is a basis for \mathcal{V} (just as for C_n). Show that the matrix $[\Phi_\Delta]$ of Φ_Δ with respect to the basis F is just $A(Z_n)$, the adjacency matrix of Z_n .
- (f) Show that the eigenvalues of $A(Z_n)$ are the numbers $2 \cos(\frac{2\pi j}{n})$, where $0 \leq j \leq n-1$. What are the corresponding eigenvectors?
- (g) How many closed walks in Z_n are of length ℓ and start at 0? Give the answers in the cases $n = 4$ and $n = 6$ without using trigonometric functions, complex exponentials, etc.
- (h) Let $Z_n^{(2)}$ be the graph with vertex set \mathbb{Z}_n and edges $\{i, j\}$ for $j - i = 1$ or $j - i = 2$. How many closed walks in $Z_n^{(2)}$ are of length ℓ and start at 0? Try to express your answer in terms of trigonometric functions and not involving complex numbers.
6. Let \tilde{C}_n be the graph obtained from the n -cube graph C_n by adding an edge between every vertex v and its antipode (the vertex which differs from v in all n coordinates). Find the number of closed walks in \tilde{C}_n of length ℓ which begin (and hence end) at the origin $\mathbf{0} = (0, 0, \dots, 0)$.



<http://www.springer.com/978-1-4614-6997-1>

Algebraic Combinatorics
Walks, Trees, Tableaux, and More
Stanley, R.
2013, XII, 223 p., Hardcover
ISBN: 978-1-4614-6997-1