Generalized Alon-Boppana Theorems and Error-Correcting Codes

Joel Friedman* Jean-Pierre Tillich†

May 27, 2002

Abstract

In this paper we describe several theorems that give lower bounds on the second eigenvalue of any quotient of a given size of a fixed graph, G. These theorems generalize Alon-Boppana type theorems, where G is a regular (infinite) tree.

When G is a hypercube, our theorems give minimum distance upper bounds on linear binary codes of a given size and information rate. Our bounds at best equal the current best bounds for codes, and only apply to linear codes. However, it is of interest to note that (1) one very simple Alon-Boppana argument yields non-trivial code bound, and (2) our Alon-Boppana argument that equals a current best bound for codes has some hope of improvement.

We also improve the bound in sharpest known Alon-Boppana theorem (i.e., when G is a regular tree).

1 Introduction

The goal of this paper is to draw a connection between the "Alon-Boppana" bound, in the theory of expanders or graph eigenvalues, and asymptotic upper bounds for the minimum distance of an error-correcting code of a given rate.

*Departments of Computer Science and Mathematics, University of British Columbia, Vancouver, BC V6T 1Z4 (V6T 1Z2 for Mathematics), CANADA. jf@cs.ubc.ca. Research supported in part by an NSERC grant.

†Inria Projet Codes, Domaine de Voluceau BP.105, 78153 FRANCE. jean-pierre.tillich@inria.fr Research supported in part by France Telecom.

Recall that the Alon-Boppana bound is a lower bound on the second eigenvalue of finite d-regular graphs. In its basic form it says that the second largest eigenvalue of a d-regular graph is greater than $2\sqrt{d-1}+o(1)$ as the number of vertices goes to infinity.

The connection with upper bounds on the minimum distance of a binary linear code is that the minimum distance of a binary linear code C can be expressed as a certain decreasing function of the second largest eigenvalue of a certain regular graph associated to C (this graph is generally called the *coset graph* of $C^\perp$; see Section 5). In other words any lower bound on the second eigenvalue of this graph translates into an upper bound on the minimum distance of the code. If we use the aforementioned Alon-Boppana directly then we only obtain a very weak upper bound on the minimum distance of the code.

However, when we know more about the geometry of the graph, such as for instance lower bounds on the number of cycles of a given length, then the Alon-Boppana lower bound can be strengthened considerably. We derive several lower bounds by different techniques. The first one is derived through lower bounds on the number of cycles of a given length, the second through comparison with Dirichlet eigenvalues. There is however a common underlying idea, namely the notion of a covering graph (see Section 3). In both cases, the relevant quantities (either the number of cycles or the Dirichlet eigenvalues) are bounded by the corresponding quantities of a cover graph. The crux of this approach is that the cover graph may have a simple structure (for instance, for the coset graph we may choose a Boolean hypercube), which enables us to estimate these quantities directly.

The second technique, when applied to the graph associated to the coset graph of a binary linear code, yields the first MRRW bound [MRRW77] in coding theory, which is the best known upper bound on the minimum distance for low rate codes. This bound was originally obtained with the "linear programming" approach. While our approach has elements in common with the classical "linear programming" approach, we believe our approach is easier to use and suggests more geometrically visualizable questions on the Boolean hypercube. This is because a simple "Alon-Boppana" argument easily gives an interesting coding bound (see Section 5), and we don't know of an analogous argument based on the linear programming approach. Also, in an attempt to improve the "first MRRW bound" (of [MRRW77], as explained in Section 2) there arises a geometric question about what is the correct analogue for the hypercube of the classical Faber-Krahn inequality for domains in $\mathbb{R}^n$ (see, e.g., [Fab23, Kra25, Cha84, Fri93]); if this analogue is "asymptotically different" (see Section 9), which is presently conceivable, then the first MRRW bound will be improved. We must admit, however, that at present we cannot improve but only duplicate the first MRRW bound with our methods; furthermore it is quite conceivable that any theorem obtained with our methods could be translated into a proof based only on the linear programming approach (it would be interesting to know if this were really true). But we reiterate that even if our approach is, in a sense, subsumed by the linear programming approach, the setting and geometric pictures suggested by our method seems to be easier to work with. Moreover, we also show how to obtain the linear programming bounds dealing only with the Hamming space through our approach, by changing slightly one of our Alon-Boppana bounds (see Section 9).

The consequences for the Alon-Boppana theorem in this paper is that we improve the best Alon-Boppana bound (of Friedman and Kahale, see [Fri93]) by a factor that depends on the graph's size. This is done by generalizing the known Alon-Boppana bound techniques to give coding bounds, and realizing that the first MRRW bound improves this bound, in a sense, by a factor of two (somewhere). It is not hard to see where this factor of two can be recovered (see Section 9).

2 A basic fact for obtaining Alon-Boppana bounds

Let us first introduce some general notation concerning eigenvalues of (adjacency matrices of) graphs. Let G be a graph with $|V_G| = n$ and adjacency matrix A_G. Recall that A_G is a $n \times n$ symmetric matrix, with entries a_{uv} indexed by the vertices of the graph, and $a_{uv} = 1$ iff u and v are adjacent in G, and $a_{uv} = 0$ otherwise. Since A_G is symmetric, it can be diagonalised in an orthonormal basis. Then we write

$$\lambda_1(G) \geq \lambda_2(G) \geq \cdots \geq \lambda_n(G)$$

for the eigenvalues of G's adjacency matrix (written with their multiplicity). We denote by $e_1, e_2, \ldots, e_n$ the corresponding (orthonormal) basis of eigenvectors. We write $\rho_i = \rho_i(G)$ for the i-th largest value that occurs among the $|\lambda_i|$; for example, the Perron-Frobenius theorem implies that $\rho_1 = \lambda_1$ and thus

$$\rho_2 = \rho_2(G) = \max(\lambda_2, -\lambda_n).$$

Estimating λ_2 is of interest in studying expansion; however, some techniques only estimate ρ_2 (and higher ρ_i).

Rayleigh principle gives us the following characterization of $\lambda_2(G)$ (it is a straightforward consequence of the fact that $e_1, e_2, \ldots, e_n$ is an orthornormal basis)

$$\lambda_2(G) = \max_{f \perp e_1} \frac{(A_G f, f)}{(f, f)} \tag{1}$$

If G is a regular graph, then e_1 can be chosen to be $\frac{1}{\sqrt{n}}\vec{1}$, where $\vec{1}$ is the all ones vector, and therefore by applying the previous equation we obtain

Fact 2.1 *If G is a regular graph, and $f \in \mathbb{R}^n$ is orthogonal to $\vec{1}$ then*

$$\lambda_2(G) \geq \frac{(A_G f, f)}{(f, f)} \tag{2}$$

This inequality is the key to obtain lower bounds on $\lambda_2(G)$: by choosing f appropriately we can relate $\lambda_2(G)$ to other quantities of the graph. Notice that we can also apply the Rayleigh principle to A_G^l (or even sometimes to a well chosen polynomial applied to A_G), this yields for $f \perp \vec{1}$ and any positive odd integer l:

$$\lambda_2(G)^l \geq \frac{(A_G^l f, f)}{(f, f)} \tag{3}$$

and in general for any positive integer l :

$$\rho_2(G)^l \geq \frac{(A_G^l f, f)}{(f, f)} \tag{4}$$

In what follows we are going to apply these simple facts to several different choices of f. For all these choices we are going to control the term $\frac{(A_G^l f,f)}{(f,f)}$ which appears on the righthand side through the notion of a cover graph.

3 Graphs and Covers

In this section we review the definition of graph covers. Until Section 10 we assume all graphs are *simple*, i.e. have no multiple edges or self-loops; this simplifies the discussion and notation. In Section 10 we give the definitions needed for general graphs; all theorems immediately carry over to general graphs.

By a *simple graph* we mean a graph with no multiple edges or self-loops; so we may think of a simple graph, G, as a pair (V_G, E_G) where E_G is a subset of the set of unordered pairs of V_G. Until Section 10 we understand a *graph* to mean a simple graph.

A *morphism* $\pi\colon H \to G$ of graphs is a map from V_H to V_G such that the natural map from E_H onto pairs in V_G has its image in E_G. π thus gives rise to a map from E_H to E_G which we also denote by π, assuming no confusion will arise.

A morphism $\pi\colon H \to G$ is called a *covering map* if for every edge $e = \{u, v\}$ of G and every $u' \in V_H$ with $\pi(u') = u$ there is a unique $v' \in \pi^{-1}(v)$ such that $\{u', v'\}$ is an edge in E_H. We also say that in this case H is a *cover* of G.

Example 3.1 Let G be any finite graph. Then G has a *universal cover*, $\pi\colon T \to G$, in that for any covering map $\nu\colon K \to G$ there is a covering map[1] $\mu\colon T \to K$ such that $\pi = \nu \circ \mu$. T is a tree. If G is d-regular, i.e. each row and column of A_G sums to d, then T is a d-regular tree (and any two d-regular trees are isomorphic).

Example 3.2 Let G be a connected Cayley graph on $(\mathbb{F}_2)^k$ of degree n, with generators $c_1, \ldots, c_n$. This is a graph where we connect any $x \in (\mathbb{F}_2)^k$ to $x + c_i$ for $i \in \{1, 2, \ldots, n\}$. Let $\mathbb{B}^n$ be the Boolean n-hypercube, i.e. the Cayley graph on $(\mathbb{F}_2)^n$ with generators $e_1, \ldots, e_n$ where e_i is the i-th standard basis vector, i.e., e_i is 0 on each coordinate except the i-th, where it is 1. Consider the map $\pi_{\mathrm{lin}}\colon (\mathbb{F}_2)^n \to (\mathbb{F}_2)^k$ which takes e_i (as above) to c_i and is extended by linearity. Then π_{lin} induces a covering map $\pi\colon \mathbb{B}^n \to G$.

4 Coding Theory

A *code* of *length* n is a subset $C \subset (\mathbb{F}_2)^n$, where $\mathbb{F}_2 = \{0, 1\}$ is the field with two elements. C is *linear* if it is a subspace of the vector space $(\mathbb{F}_2)^n$. We endow $(\mathbb{F}_2)^n$ with the Hamming distance, i.e. for $x, y \in (\mathbb{F}_2)^n$, $d(x, y)$ is the

[1]This covering map, μ, is uniquely defined if one works with "base-pointed graphs," i.e. graphs with a distiguished vertex.

number of coordinates on which x and y differ. The minimum distance of a code, C, is

$$d_{\min}(C) = \min\{d(x,y) \mid x, y \in C,\ x \neq y\},$$

and its *normalised minimum distance* is

$$\delta(C) = d_{\min}(C)/n.$$

The *information rate* of a code is

$$R(C) = \frac{\log_2 |C|}{n}.$$

If C is a linear code then this is just $(\dim C)/n$.

Let $\delta_{\max}$ be the function

$$\delta_{\max}(R) = \overline{\lim_{n\to\infty}} \max\{\delta(C) \mid R(C) \geq R,\ C \subset (\mathbb{F}_2)^n\}$$

and

$$R_{\max}(\delta) = \overline{\lim_{n\to\infty}} \max\{R(C) \mid \delta(C) \geq \delta,\ C \subset (\mathbb{F}_2)^n\}.$$

We are interested in estimating these functions.

To estimate $\delta_{\max}$ is essentially the same as to estimate $R_{\max}$, but a bit of care is required to make this precise.

Proposition 4.1 *Let $\delta_{\max}(\alpha) \leq f(\alpha)$ for a continuous, strictly decreasing function, f, defined on an open interval. Then (f^{-1} is defined on the image of f and) $R_{\max}(\delta) \leq f^{-1}(\delta)$.*

Proof This is an easy (but mildly annoying) technicality; see appendix B.

□

We now state some classical bounds.

Theorem 4.2 *$R_{\max}(\delta) \geq 1 - h(\delta)$, where*

$$h(\theta) = -\theta \log_2 \theta - (1-\theta)\log_2(1-\theta).$$

Proof See the asymptotic Gilbert-Varshamov bound in [vL99].

□

The best upper bound on $R_{\max}$ is given by the following

Theorem 4.3
$$R_{\max}(\delta) \leq \min_{u \in [0,1-2\delta]} b(u,\delta), \tag{5}$$
where
$$b(u,\delta) = 1 + g(u^2) - g(u^2 + 2\delta u + 2\delta)$$
with
$$g(x) = h\left(\frac{1}{2} - \frac{\sqrt{1-x}}{2}\right).$$
For $\delta \geq 0.273$ this bound is the same as
$$R_{\max}(\delta) \leq b(1-2\delta,\delta) = h\Big(1/2 - \sqrt{\delta(1-\delta)}\Big). \tag{6}$$

Proof See [MRRW77] (or [MS77] for the latter half of the theorem).

$\square$

The inequality (5) is known as the "second MRRW" bound; (6) is known as the "first MRRW" bound.

Corollary 4.4 *For small α we have*
$$\frac{1}{2} - \big(1+o(1)\big)\sqrt{\frac{\alpha}{2\log_2 e}} \leq \delta_{\max}(\alpha) \leq \frac{1}{2} - \big(1+o(1)\big)\sqrt{\frac{\alpha}{\log_2(1/\alpha)}}.$$

5 Codes and Eigenvalues

In this section we recall how a graph can be associated to a linear code in such a way that the eigenvalues of the graph are in relationship with the codeword weights.

Let $C \subset (\mathbb{F}_2)^n$ be a linear code with basis $r_1, \ldots, r_k$. We form the generator matrix, M, over $\mathbb{F}_2$, whose rows are the r_i's; so M is an $k \times n$ matrix. Its columns, $c_1, \ldots, c_n$, can each be viewed as an element of $(\mathbb{F}_2)^k$.

Let G be the Cayley graph on $(\mathbb{F}_2)^k$ with generators $c_1, \ldots, c_n$ [2]. Apparently G may depend on the choice of the basis $r_1, r_2, \ldots, r_k$. It turns out that

[2]We shall assume (until Section 10) that no c_i's vanish and the c_i's are all distinct; if not, then G will have self-loops and/or multiple edges, and we technically need Section 10 before we can apply our theory.

G only depends on C. This can be seen by bringing in the dual code $C^\perp$ of C, that is

$$C^\perp = \{x \in (\mathbb{F}_2)^n \mid x \cdot c = 0 \quad \forall c \in C\}.$$

Consider the graph with vertices the cosets $x + C^\perp$, and two cosets being linked by an edge iff they are at Hamming distance 1. We claim that the Cayley graph defined before and this new graph are isomorphic, the isomorphism being given by the map $\pi : x + C^\perp \to Mx$. Indeed, let two cosets $x+C^\perp$ and $y+C^\perp$ be linked by an edge. This means that there exists $c \in C^\perp$ and $i \in \{1, \ldots, n\}$ such that $x = y + c + e_i$ (where e_i is the i-th standard basis vector of ${\mathbb{F}_2}^n$, i.e., e_i is 0 on each coordinate except the i-th, where it is 1), this implies that $Mx = My + c_i$. On the other hand if $Mx = My + c_i$ then necessarily x and $y + e_i$ differ only by an element of $C^\perp$.

We say that this graph is the *coset graph* of $C^\perp$ or of the code[3], C. The following is a well-known folk theorem (see [DS91] and the reference there):

Theorem 5.1 *Let $\lambda_1 \geq \lambda_2 \geq \cdots$ be the eigenvalues of the adjacency matrix of the coset graph of $C^\perp$ arranged in non-increasing order. Then $\lambda_1 = n$ and $\lambda_2 = n - 2d_{min}(C)$. Moreover, the weights (i.e. distances to the zero code word) appearing in C are just the $(n - \lambda_i)/2$ as i ranges from 1 to 2^k.*

6 A Simple Generalized Alon-Boppana Theorem

In this section we give a very simple but rather weak generalized Alon-Boppana theorem and discuss its implications. Let G be a d-regular graph. We use the approach outlined in Section 2 to obtain a lower bound on $\lambda_2(G)$ and $\rho_2(G)$ and we choose $f = \chi_u - \chi_v$ where χ denotes the characteristic function in (4). Notice that

$$(A_G^l \chi_u, \chi_u) = N_l(u), \qquad (A_G^l \chi_v, \chi_v) = N_l(v),$$

where $N_l(v)$ denotes the number of walks of length l from v to itself. Moreover if u and v are at distance greater than $l \geq 0$, then

$$(A_G^l \chi_u, \chi_v) = (A_G^l \chi_v, \chi_u) = 0.$$

[3]This is the graph of cosets of the hypercube modulo $C^\perp$, or of $C^\perp$ cosets, but it is the graph of cosets one uses when working with C. Since we do not work with a code, C, and its dual, $C^\perp$, simultaneously (in this paper), no confusion will occur in referring to the graph as the coset graph of "the code."

Hence

$$(A_G^l f, f) = N_l(u) + N_l(v)$$

Let $N_l = N_l(G)$ denote the minimum of $N_l(v)$ ranging over all vertices v of the graph. Of course, $(f, f) = 2$, and so

$$\frac{(A_G^l f, f)}{(f, f)} \geq N_l(G).$$

By using (4) we now obtain

$$\rho(A_G) \geq \big(N_l\big)^{1/l};$$

The right-hand-side term can be estimated through a cover H of G for which the calculation of $N_l(H)$ might be much simpler. Indeed the following is clear.

Fact 6.1 *If $\pi\colon H \to G$ is a cover, then any H cycle about a vertex, v, gives rise to a unique G cycle about $\pi(v)$. Hence for any positive integer l we have*

$$N_l(G) \geq N_l(H).$$

In other words we have proved the following.

Theorem 6.2 *Let G be a d-regular graph that contains two vertices of distance $> l$ and H be a cover of G. Then*

$$\rho(A_G) \geq \big(N_l(H)\big)^{1/l};$$

furthermore, if l is odd then the above equation holds with ρ replaced by λ_2.

The last statement follows by using (3) instead of (4).

The above theorem is quite simple. Unfortunately, for some purposes, such as coding theory, we are interested in $\lambda_2(A_G)$ and the cover graph H (which can be chosen to be a boolean hypercube) will be bipartite (i.e. $N_l(H) = 0$ for l odd). So we prove the following variant of the above theorem.

Theorem 6.3 *Let $\pi\colon H \to G$ be a covering map. Let e_1, e_2 be two edges of distance $> l$ (i.e. the distance from any of e_1's endpoints to any of e_2's is greater than l). Then*

$$\rho(A_G) \geq \big(N_l(H) + N_{l-1}(H)\big)^{1/l};$$

furthermore, if l is odd then the above equation holds with ρ replaced by λ_2.

Proof Let $e_i = \{u_i, v_i\}$ and set

$$f = \chi_{u_1} + \chi_{v_1} - \chi_{u_2} - \chi_{v_2}.$$

We have that $(A^l \chi_{u_1}, \chi_{v_1})$ is at least $N_{l-1}(H)$, since any walk of length $l-1$ beginning and ending in u_1 yields a walk from u_1 to v_1 with one additional step. Similar reasoning to that in the previous theorem then yields:

$$(A^l f, f) \geq 4\big(N_l(H) + N_{l-1}(H)\big),$$

and, of course, $(f, f) = 4$. Similar reasoning as before now yields this theorem.

□

We state two corollaries of this simple theorem:

Corollary 6.4 *Fix d. Then for any d-regular graph, G, on n vertices, we have $\rho(G) \geq 2\sqrt{d-1} - o(1)$ as $n \to \infty$.*

This follows by taking H to be the universal cover of G (namely the infinite d-regular tree) and by noticing that any d-regular graph on n vertices has at least two vertices which are at distance $\lfloor \log_{d-1} n \rfloor$. The revelant computation can be found in [LPS88] for instance.

We get stronger bounds with regular graphs which admit a cover which has more closed walks than the d-regular infinite tree, and this is exactly what happens for the coset graph of a code of length n which admits the boolean hypercube as a cover (see Example 3.2)

Corollary 6.5 *Let C be a binary linear code of length n of rate $\leq R$. The normalised minimum distance of C, δ, satisfies $\delta \leq f(R)$, where f is a function that satisfies:*

$$f(R) = \frac{1}{2} - C\big(1 + o(1)\big)\sqrt{\frac{R}{\log_2 R}}$$

when R tends to 0, with $C = 1/\sqrt{4e}$.

The bound of [MRRW77] yields the same corollary but with $C = 1$. The calculation which lead to this theorem are in Appendix A.

7 Projecting out constants

In this section we introduce a technique that will strengthen essentially all of our Alon-Boppana theorems, including the ones in the previous section and the more refined theorems to come.

In the previous section we created functions, f, for which $(A^l f, f)$ could be bounded; the idea was to concentrate f at a few vertices. Since it is important that f be orthogonal to $\vec{1}$, the all ones vector, we took f to have as many positive values as negative values, taking the values of different sign to be far apart (a distance $> l$). However, we may alternatively take f to be all positive, provided that we then remove f's component in the direction of $\vec{1}$. This is the same as taking f to be concentrated and positive, subtracting the same (small) negative value at every other vertex.

The idea of choosing an arbitrary f and "projecting out the constant component" will be used repeatedly in this paper. Here is this technique applied to Theorem 6.2.

Theorem 7.1 *Let $\pi\colon H \to G$ be a covering map. Let G be a d-regular graph, and let l be a value such that*

$$N_l(H) \geq d^l/|V_G|.$$

Then

$$\rho(A_G) \geq \left(N_l(H) - \frac{d^l}{|V_G|} \right)^{1/l};$$

furthermore, if l is odd then the above equation holds with ρ replaced by λ_2.

Proof Fix any $v \in V_G$ and set $f = \chi_v$. Then $\widetilde{f} = f - \vec{1}/|V_G|$ is orthogonal to $\vec{1}$. We have

$$(A^l \widetilde{f}, \widetilde{f}) = (A^l f, f) - (A^l \vec{1}/|V_G|, \vec{1}/|V_G|) \geq N_l(H) - d^l/|V_G|,$$

and

$$(\widetilde{f}, \widetilde{f}) = (f, f) - (\vec{1}/|V_G|, \vec{1}/|V_G|) \leq 1.$$

The reasoning used at the end of Theorem 6.2 now applies here, and we conclude the theorem.

$\square$

We may also obtain the following variant of Theorem 6.3.

Theorem 7.2 *Let $\pi\colon H \to G$ be a covering map with G a d-regular graph, and let l be a value such that*

$$N_l(H) + N_{l-1}(H) \geq 2d^l/|V_G|.$$

Then

$$\rho(A_G) \geq \left(N_l(H) + N_{l-1}(H) - \frac{2d^l}{|V_G|} \right)^{1/l};$$

furthermore, if l is odd then the above equation holds with ρ replaced by λ_2.

Proof Fix any edge, $e = \{u, v\}$, and let $f = \chi_u + \chi_v$ and $\widetilde{f} = f - 2\vec{1}/|V_G|$. As before, $\widetilde{f}$ is orthogonal to $\vec{1}$, and we have

$$(A^l\widetilde{f}, \widetilde{f}) = (A^l f, f) - 4(A^l\vec{1}/|V_G|, \vec{1}/|V_G|) \geq 2N_l(H) + 2N_{l-1}(H) - 4d^l/|V_G|$$

and

$$(\widetilde{f}, \widetilde{f}) \leq 2.$$

We argue as before.

$\square$

Using this theorem we improve Corollary 6.5 by a factor of 2, as follows; see Appendix A for the proof.

Corollary 7.3 *In Corollary 6.5, we may take $C = 1/\sqrt{2e}$.*

8 Eigenfunction Pushing Techniques

Let us now apply (2) to functions of the form $\widetilde{f} = f - c\vec{1}$ (where c is chosen such that $\widetilde{f}$ is orthogonal to $\vec{1}$) where f is a function supported on a subset U of vertices of the graph (this means that f is equal to 0 outside of U). We easily obtain the following.

Proposition 8.1 *Let f be supported on a set, U. Let G be d-regular. Then*

$$\lambda_2(G) \geq \frac{(A_G f, f)}{(f, f)} - \frac{d|U|}{|V_G|}.$$

Proof Let $\widetilde{f} = f - c\vec{1}$ where $c = (f, \vec{1})/|V_G|$; then $\widetilde{f}$ is orthogonal to $\vec{1}$, and so

$$\lambda_2(G) \geq \frac{(A_G\widetilde{f}, \widetilde{f})}{(\widetilde{f}, \widetilde{f})}. \tag{7}$$

Since

$$(f, \vec{1})^2 = (f, \chi_U)^2 \leq (f, f)(\chi_U, \chi_U) = (f, f)|U|,$$

we have

$$(A_G\widetilde{f}, \widetilde{f}) = (A_G f, f) - dc^2|V_G| \leq (A_G f, f) - d(f, f)|U|/|V_G|.$$

Combining this with the fact that $(\widetilde{f}, \widetilde{f}) \leq (f, f)$ (since $\widetilde{f}$ is a projection of f onto the subspace orthogonal to $\vec{1}$) and with the inequality (7), finishes the proposition.

□

To optimize this inequality we have to find for a given subset of vertices U the function f which maximizes the ratio $\frac{(A_G f, f)}{(f,f)}$. This maximum is known as a Dirichlet eigenvalue. We define for a graph G and a subset of vertices $W \subset V_G$,

$$\lambda_{1,\mathrm{Dir}}(W) = \max_{f \in C_0(W)} \frac{(Af, f)}{(f, f)},$$

where we write $C_0(W)$ for those functions supported in W. It is easy to check that the maximum is attained for a non-negative function (this is a simple consequence of the Perron-Froebenius theorem, see also [Fri93]). The f achieving the above maximum is called the *first Dirichlet eigenfunction* of A; this f is known to satisfy $Af = \lambda f$ for $\lambda = \lambda_{1,\mathrm{Dir}}(W)$ (see [Fri93]).

Then it makes sense to find the subset W of a given size which maximizes this eigenvalue, this leads us to define for $a > 0$, $\mathrm{FK}_G(a)$, the *Faber-Krahn maximum of size a* as

$$\mathrm{FK}_G(a) = \max_{|W| \leq a} \lambda_{1,\mathrm{Dir}}(W);$$

the W achieving this maximum is the *Faber-Krahn maximizer of size a*.

The nice thing about this quantity is that it has a lower bound in terms of the Faber-Krahn maximum for the same size of a cover graph, that is

Theorem 8.2 *Let H be a cover of G. Then*

$$\mathrm{FK}_H(a) \leq \mathrm{FK}_G(a).$$

To prove this fact we need a lemma and a definition. For a covering map $\pi\colon H \to G$ and $f : V_H \to \mathbb{R}$, we define the *push forward*, $\pi_* f$, a function on V_G, whenever H is finite, via

$$(\pi_* f)(v) = \sum_{\pi(w)=v} f(w).$$

Lemma 8.3 *Let $f \in C(V_H)$ and let $\pi\colon H \to G$ be a covering map. Assume H is finite. If $f \geq 0$ everywhere, then also $\pi_* f \geq 0$. If $A_H f \geq \lambda f$ everywhere, for some real λ, then also $A_G \pi_* f \geq \lambda \pi_* f$. If f is supported in W, then $\pi_* f$ is supported in $\pi(W)$.*

Proof The first part (the non-negativity statement) is clear. The second part follows from the fact that π is a local isomorphism. The third part is also clear.

$\square$

We are ready now to prove Theorem 8.2.

Proof of Theorem 8.2 Let $\mathrm{FK}_H(a) = \lambda = \lambda_{1,\mathrm{Dir}}(W)$ be the minimizing eigenvalue with $|W| = a$, and let f be the corresponding eigenfunction. Then $\pi_* f$ satisfies $A_G(\pi_* f) \geq \lambda \pi_* f$ and $\pi_* f$ is non-negative and supported on $\pi(W)$, so

$$\lambda_{1,\mathrm{Dir}}\big(\pi(W)\big) \geq \frac{(A_G \pi_* f, \pi_* f)}{(\pi_* f, \pi_* f)} \geq \frac{(\lambda \pi_* f, \pi_* f)}{(\pi_* f, \pi_* f)} \geq \lambda.$$

Furthermore $\pi(W)$ is a set of size $\leq a$. Hence

$$\mathrm{FK}_G(a) \geq \lambda = \mathrm{FK}_H(a).$$

$\square$

Putting Proposition 8.1 and Theorem 8.2 together we obtain

Theorem 8.4 *Let G be a d-regular graph, and H be a cover of G. Then*

$$\lambda_2(A_G) \geq \mathrm{FK}_H(a) - \frac{da}{|V_G|}.$$

For an application to coding theory we observe:

Proposition 8.5 *Let H be the n-dimensional hypercube. Then for $\alpha \in (0,1)$ fixed we have* $\mathrm{FK}_H(2^{\alpha n}) \geq 2\sqrt{\gamma(1-\gamma)}n + o(n)$*, where* $\alpha = H_2(\gamma)$.

Proof We take a ball of size roughly $2^{\alpha n}$. For the details see appendix C.

$\square$

Notice that we could also give a simple bound of $\mathrm{FK}_H(2^{\alpha n}) \geq \alpha n$ by taking the characteristic function of a subcube of dimension αn.

A corollary is the first MRRW bound.

Corollary 8.6 *For any $\delta \in (0,1)$ we have*

$$R_{\max}(\delta) \leq h\Big(1/2 - \sqrt{\delta(1-\delta)}\Big).$$

Proof Fix an $\alpha \in (0,1)$ and a code C of information rate $\geq \alpha$ and a corresponding covering map $\pi\colon H \to G$ We apply Theorem 8.4 with $a = 2^{\alpha n}/\log n$. We conclude

$$\lambda_2(A_G) \geq 2\sqrt{\gamma(1-\gamma)} \; + o_n(1)$$

where $\alpha = h(\gamma)$. Hence

$$\delta \leq 1/2 - \sqrt{\gamma(1-\gamma)},$$

and so

$$\gamma \leq 1/2 - \sqrt{\delta(1-\delta)}$$

and the corollary follows.

$\square$

Remark 8.7 Notice that a (sub)cube of dimension αn has largest adjacency eigenvalue αn. This implies that $\mathrm{FK}_H(2^{\alpha n}) \geq \alpha n$. This gives the weak corollary that $\alpha_{\max}(\delta) \leq (1-\delta)/2$, which agrees asymptotically with the Plotkin and Griesmer bounds of coding theory (see [vL99]).

Remark 8.8 The approach which was used in this section borrows some ideas from [Nil91, Fri93]. Assume that G has a cover graph H. If f_H is a non-negative "approximate eigenfunction" on H, we can try to form "versions" of it, f_G, on a quotient, G, with similar properties. In this section we have formed our version on G by "summing over fibres" (this was the push forward function defined above); this is a similar technique to that used by Nilli (see [Nil91]), later refined by Friedman and Kahale (see [Fri93])[4]. Our improvement on this technique was obtained by "projecting out the constants," meaning that we project out the $\vec{1}$ component from f_G rather than setting up f_G (or f_H) with a matching non-positive component to make it orthogonal to $\vec{1}$ (as done by Nilli, Friedman, and Kahale).

9 A Stronger Alon-Boppana Bound

9.1 A Simple Improvement

In this subsection we give an example of a more general generalized Alon-Boppana bound. Namely, the following theorem and corollary strengthen Proposition 8.1.

Theorem 9.1 *Let G be a d-regular graph and let p be any real-valued function defined on the eigenvalues of A_G. Then*

$$(f,f)\max_{i\geq 2} p(\lambda_i) \geq \bigl(p(A_G)f,f\bigr) - p(d)(f,\vec{1})^2/|V_G|,$$

The theorem follows immediately from the spectral decomposition on A_G as applied to f.

Corollary 9.2 *If in addition to the hypothesis in the above theorem we have f is supported in U, then*

$$(f,f)\max_{i\geq 2} p(\lambda_i) \geq \bigl(p(A_G)f,f\bigr) - p(d)(f,f)|U|/|V_G|.$$

The special case $p(x) = x$ was the bound used in the previous section. When G has a cover which is distance regular, then there is a very natural choice of polynomials in the corollary which enables to have some control on

[4] Actually, the previous technique (of Nilli, Friedman, and Kahale) takes radial functions on G given by the radial function on H that gives the first Dirichlet eigenfunction of a ball in H of a given radius. The technique used here "pushed down" the eigenfunction on H to G by summing over the fibres, i.e. for each vertex, $v \in V_G$ we sum the eigenfunction over $\pi^{-1}(v)$. This may be better suited in certain situations, e.g. when the graphs are not regular.

the term $\big(p(A_G)f, f\big)$ when $f = \chi_v$ for any vertex v of G. Indeed, let H be a distance regular cover of G. Let D denote the diameter of H. Then there are $D + 1$ polynomials $P_0, P_1, P_2, \dots, P_D$ (see [BCN89]) such that $P_i(A_H)$ is the adjacency matrix of the graph with the same vertices as H and two vertices are joined by an edge iff they are at distance i in H. In such a setting for any $Q = \sum_{i=0}^{D} \beta_i P_i$ where the β_i's are nonnegative we have that $\big(Q(A_G)\chi_v, \chi_v\big) \geq \big(Q(A_H)\chi_v, \chi_v\big)$. Notice now that $\big(Q(A_H)\chi_v, \chi_v\big) = \beta_0$ and therefore

$$\big(Q(A_G)\chi_v, \chi_v\big) \geq \beta_0. \tag{8}$$

The coset graphs associated to a binary linear code of length n that we consider in this article have a common cover which is distance regular namely the boolean cube $\mathbb{B}^n$. An application of the aforementioned remark leads to the Delsarte linear programming bound in coding theory as explained in the following subsection.

9.2 Connections with the Delsarte Approach

Let us first quickly review the linear programming approach for obtaining upper bounds on the minimum distance of a code (see [MS77, vL99] for more details). For a code $C \in (\mathbb{F}_2)^n$, we consider the *distance distribution* of the code, i.e. the B_i's for $i = 0, \dots, n$, where B_i denotes the average number of codewords of distance i to a fixed codeword, that is $B_i \stackrel{\text{def}}{=} \frac{1}{|C|} \left|\{(x, y); x \in C, y \in C, d(x, y) = i\}\right|$. The linear programming bound is based on the inequality

$$\sum_{i=0}^{n} B_i K_k(i) \geq 0$$

for $k \in \{0, 1, \dots, n\}$, where K_k is a Krawtchouk polynomial of degree k :

$$K_k(x) \stackrel{\text{def}}{=} \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j},$$

with $\binom{x}{j} \stackrel{\text{def}}{=} \frac{x(x-1)\dots(x-j+1)}{j!}$. This yields linear inequalities which should be satisfied by the B_i's. By maximizing the sum of the B_i's (which is equal to the size of the code) which satisfy these inequalities we obtain a linear programming problem for which an upper bound can be found by duality. This duality result can be written as (see [vL99] Theorem 5.3.5)

Theorem 9.3 *Let $\beta(x) = 1 + \sum_{k=1}^{n} \beta_k K_k(x)$ be any polynomial with $\beta_k \geq 0$ ($1 \leq k \leq n$) such that $\beta(j) \leq 0$ for $j = d, d+1, \ldots, n$ then any code of minimum distance $\geq d$ and length n has cardinality at most $\beta(0)$.*

Finding interesting choices for β turns out to be a nontrivial task, however the first MRRW bound can be obtained by a direct application of this theorem by choosing β appropriately (see [vL99]).

We now claim that this theorem is a simple consequence of Corollary 9.2, provided we restrict to linear codes. Indeed, if we let $P_k \stackrel{\text{def}}{=} K_k((n-x)/2)$, then $P_k(A_{\mathbb{B}^n})$ is nothing but the adjacency matrix of the graph with vertices belonging to ${\mathbb{F}_2}^n$ and two vertices being adjacent iff they are at Hamming distance k. This follows immediately from classical results about the Hamming association scheme (see for instance Chapter 21 in [MS77]). Therefore by using the remark which follows Corollary 9.2 for any polynomial $Q(x) = 1 + \sum_{k=1}^{n} \beta_k P_k(x) = 1 + \sum_{k=1}^{n} \beta_k K_k((n-x)/2)$ with $\beta_k \geq 0$ we have that for any vertex of the coset graph G of a binary linear code of length n :

$$\big(Q(A_G)\chi_v, \chi_v\big) \geq 1. \tag{9}$$

Notice now that by Theorem 5.1 $P_k(\lambda_i) = K_k(j)$ for some integer $j \in [d_{\min}(C), n]$ for any eigenvalue of the adjacency matrix of G different from n. Therefore $Q(\lambda_i) = 1 + \sum_{k=1}^{n} \beta_k K_k(j)$. This implies that

$$(\chi_v, \chi_v) \max\{Q(\lambda_i) | 2 \leq i \leq |V_G|\} \leq 0 \tag{10}$$

if Q has been chosen such that $1 + \sum_{k=1}^{n} \beta_k K_k(j) \leq 0$ for any integer $j \in [d_{\min}(C), n]$ (since this implies that $Q(\lambda_i) \leq 0$ for $i \in \{2, \ldots, |V_G|\}$). We eventually obtain by using Corollary 9.2 with $f = \chi_v$ and by putting inequalities (10) and (9) together that

$$0 \geq 1 - \frac{1 + \sum_{k=1}^{n} \beta_k P_k(0)}{|C|}$$

since $Q(n) = 1 + \sum_{k=1}^{n} \beta_k P_k(0)$ by Theorem 5.1 and $|V_G| = |C|$. This proves Theorem 9.3.

10 General Graph Theory

In this section we review some basic terminology and notions needed to generalize covering theory to graphs with multiple edges and/or self-loops.

10.1 Directed Graphs

By a *directed graph* we mean a pair of sets, $G = (V_G, E_G)$, with an identification of E_G as a multi-set of $V_G \times V_G$. In other words, G comes with an *incidence map* $i_G \colon E_G \to V_G \times V_G$. We write i, E, V for i_G, E_G, V_G if no confusion can result. If $i(e) = (u, v)$ we say that e is of *type* (u, v) or that e *orginates* in u and *terminates* in v or that e's *tail* is u and e's *head* is v; in any case we will write $e \sim (u, v)$; if no multiple edges occur, i.e. if i is injective, then we may unambiguously write $e = (u, v)$.

A *walk* is an alternating sequence of vertices and edges such that when $\ldots, v, e, \ldots$ occurs in the sequence, e's tail is v, and similarly with the order of v, e reversed (with "head" replacing "tail"). The *adjacency matrix*, A_G, of a graph, G, is the square matrix indexed on V_G whose u, v-th entry counts how many edges have type u, v. For a positive integer, k, the u, v-th entry of $(A_G)^k$ counts how many directed walks there are from u to v of length k. All this makes sense if V_G or E_G is infinite, although the entries of A_G or $(A_G)^k$ may not be finite.

A morphism $\pi \colon H \to G$ of directed graphs is a collection of maps $\pi_V \colon V_H \to V_G$ and $\pi_E \colon E_H \to E_G$ that commutes with the incidence relations (i.e., $i_G \circ \pi_E = (\pi_V \times \pi_V) \circ i_H$). We often drop the subscripts from π_V, π_E if no confusion can result.

For a morphism of directed graphs, $\pi \colon H \to G$, it is possible to give a number of equivalent definitions for π to be a *covering map*; all definitions amout to π being a local isomorphism in some sense. One definition is that for every vertex, $v \in V_G$, $w \in \pi^{-1}(v)$, and every edge $e \in E_G$ with tail v, there is exactly one $f \in \pi^{-1}(e)$ whose tail is w, and similarly with "head" replacing "tail." Another possibility is to define the *geometric realization* of a graph (as in [Fri93]); then a covering map is a covering map in the topological sense.

10.2 Graphs

By an *undirected graph* or simply a *graph* we mean a directed graph, G, with an involution[5] ι on E_G that reverses heads and tails; in other words, G's edges are paired, $e \sim (u, v)$ with an edge $\iota(e) \sim (v, u)$, where e may be paired with

[5]For ι to be an involution means that $\iota \circ \iota$ is the identity.

itself[6] if $u = v$.

A morphism of graphs is one of the underlying directed graphs that commutes with the ι's. A covering maps, adjacency matrices, and walks in graphs are just the same of the underlying directed graphs.

It is now simple to see that all the theorems of this paper could as well have been stated for graphs that may have self-loops or multiple edges.

11 Concluding Remarks

One of the most exciting questions to us is to find the Faber-Krahn maximizer and maximum of the hypercube. One can find examples[7] of very small or large balls that are *not* the Faber-Krahn minimizers.

Question 11.1 Given $\gamma \in (0, 1/2)$ is

$$\varliminf_{n\to\infty} \mathrm{FK}_{\mathbb{B}^n}\left(2^{H_2(\gamma)}\right)/n = 2\sqrt{\gamma(1-\gamma)},$$

i.e. are balls asymptotically maximizers for the hypercube?

If the answer is no, then according to the method of Corollary 8.6, we have an improvement to the first MRRW bound.

A Calculations for Coding Theory

In this section we derive some simple combinatorial bounds needed in our discussion of coding theory bounds.

Throughout this section we write $f(n) \approx g(n)$ if $\left(\log f(n)\right)/\left(\log g(n)\right) \to 1$ as $n \to \infty$ (for example, $n \approx 2n$ but $n \not\approx n^2$).

[6] This gives rise to "half-loops," which are edges paired with themselves, and "whole-loops" in the languauge of [Fri93]. For example, a whole-loop contributes 2 to an entry on the diagonal of the adjacency matrix, whereas a half-loop contributes 1.

[7] For example, in the 3-hypercube, the 2-dimensional subcube has eigenvalue 2, which is greater than that of a ball of the same size, namely $\sqrt{3}$. Similarly for the 3-dimensional ball in the 7-hypercube. Also the $n/2 - \sqrt{n}$ radius ball has eigenvalue $n - 4$ (since $n/2 - \sqrt{n}$ is the first zero of the second Krawtchouk polynomial), and the $(n-4)$ dimensional subcube is smaller; so by monotonicity (see [Fri93]) the ball here can also be beaten.

Lemma A.1 *If $\rho \in (0, 1/2]$ is fixed, and if any integer $n > 0$ we set $r = r(n) = \lfloor \rho n \rfloor$, then*

$$|B_r| \approx \binom{n}{r} \approx 2^{nh(\rho)},$$

where $|B_r|$ is the size of the ball of radius r in the n-hypercube, and where

$$h(\theta) = -\theta \log_2 \theta - (1-\theta)\log_2(1-\theta).$$

Proof This is a very standard application of Stirling's formula; see, for example, [vL99].

□

Lemma A.2 *Let $\alpha \in (0, 1)$ be fixed. For any integer $n > 0$ set k to be the even integer equal either to $\lfloor \alpha n \rfloor$ or to $\lfloor \alpha n \rfloor + 1$. Then*

$$N_k(\mathbb{B}^n) \approx 2^{h(\beta_0)n-n} n^k (1-2\beta_0)^k,$$

where β_0 is the unique solution in $(0, 1/2)$ to the following equation

$$(1-2\beta_0)\log(\beta_0^{-1}-1) = 2\alpha. \tag{11}$$

Proof Since $A_{\mathbb{B}^n}$ has eigenvalues $n - 2i$ with multiplicity $\binom{n}{i}$, we have

$$N_k(\mathbb{B}^n) = \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}|n-2i|^k.$$

It follows that setting $B_i = \binom{n}{i}(n-2i)^k$, we see that

$$\frac{N_k(\mathbb{B}^n)}{n+1} \le \max_{i=0,\dots,n/2} \frac{B_i}{2^n} \le N_k(\mathbb{B}^n).$$

To find the i maximizing B_i, we write

$$\frac{B_{i+1}}{B_i} = \left(\frac{n-i}{i+1}\right)\left(\frac{n-2(i+1)}{n-2i}\right)^k = \left(\frac{n-i}{i+1}\right)e^{k\log_e\left(1-2/(n-2i)\right)}.$$

Set $\beta = \beta_n = i_0/n$ where i_0 is the (an) $i \le n/2$ maximizing B_i. Since $B_{i_0+1} < B_{i_0}$ we have

$$\left(\frac{1-\beta}{\beta} + O(n^{-1})\right)e^{\frac{-2\alpha}{1-2\beta}+O(n^{-1})} < 1.$$

Hence

$$\frac{1-\beta}{\beta} < e^{\frac{2\alpha}{1-2\beta}} + O(n^{-1}).$$

Similarly $B_{i_0-1} < B_{i_0}$, and the reverse inequality holds. Taking logarithms we conclude that

$$\log(\beta^{-1}-1)(1-2\beta) = 2\alpha,$$

where β is the lim sup and lim inf of β_n. But differentiation shows that

$$f(\beta) = \log(\beta^{-1}-1)(1-2\beta)$$

has $f'(\beta) = -2\log(\beta^{-1}-1) - (1-2\beta)/(\beta-\beta^2)$ which is < 0 for $\beta \in (0, 1/2)$. It follows that there is a unique $\beta_0 \in (0, 1/2)$ that satisfies equation (11), and this β_0 is the limit of β_n.

□

Corollary A.3 *For α, n, k as above we have*

$$N_k(\mathbb{B}^n) \approx n^k \left(\frac{\alpha + \omega(\alpha)}{e}\right)^{k/2},$$

where $\omega(\alpha)$ is a function of α with $\omega(\alpha) = O(\alpha^{3/2})$ as $\alpha \to 0$.

Proof For $\beta = 1/2 - \epsilon$ with ϵ small we have

$$\log(\beta^{-1}-1)(1-2\beta) = \log\left(\frac{1/2+\epsilon}{1/2-\epsilon}\right)2\epsilon = 2\epsilon\log\big(1+4\epsilon+O(\epsilon^2)\big) = 8\epsilon^2 + O(\epsilon^3).$$

Hence for α small we have

$$2\alpha = 8\epsilon^2 + O(\epsilon^3) \quad \text{or} \quad \sqrt{\alpha/4} = \epsilon + O(\epsilon^2) = \epsilon + O(\alpha).$$

Differentiation shows that

$$h'(x) = \log_2(x^{-1}-1), \quad h''(x) = \frac{-\log_2 e}{x - x^2}.$$

So $h'(1/2) = 0$ and $h''(1/2) = -4\log_2 e$, and

$$h(1/2-\epsilon) = 1 - 2(\log_2 e)\epsilon^2 + O(\epsilon^3).$$

It follows that

$$2^{-n}2^{nh(\beta)}(n-2\beta)^k \approx 2^{-n(2\log_2 e)\epsilon^2+O(n\epsilon^3)}n^k(1-2\epsilon)^k$$

$$\approx e^{-2n(\alpha/4+O(\alpha^{3/2}))}n^{\alpha n}\left(2\sqrt{\alpha/4}+O(\alpha)\right)^{\alpha n}$$

$$\approx e^{-\alpha n/2}e^{O(\alpha^{3/2}n}\Big(n\sqrt{\alpha}\Big)^{\alpha n}\Big(1+\big(\sqrt{\alpha}\big)\Big)^{\alpha n} \approx n^k(\alpha/e)^{k/2}\Big(1+O\big(\sqrt{\alpha}\big)\Big)^{k/2},$$

and the proposition is finished.

$\square$

Proof of Corollary 6.5: Let G be the coset graph of $C^{\perp}$. Consider the largest odd integer, k, for which

$$\sum_{i=0}^{k+2}\binom{n}{i} \geq 2^{\alpha n}. \tag{12}$$

It follows that there are two points in G of distance $\geq k+3$, and hence two edges of distance $\geq k+1$. By Theorem 6.3, we have

$$\lambda_2(A_G) \geq \big(N_{k-1}(\mathbb{B}^n)\big)^{1/k}.$$

But by equation (12) and Lemma A.1 we have

$$2^{nh(k/n)+O(1)} \approx 2^{\alpha n},$$

and thus

$$k/n = h^{-1}(\alpha) + o_n(1)$$

(where $o_n(1)$ denotes a function that tends to zero as $n \to \infty$). Since $h^{-1}(\alpha) = \alpha/\log_2(1/\alpha) + O(\alpha)$ for α small, Corollary A.3 then implies that

$$\lambda_2/n \geq \sqrt{\frac{\alpha}{e\log_2(1/\alpha)}} + \omega(\alpha) + o_n(1),$$

where $\omega(\alpha) = O\big(\sqrt{\alpha}\big)$. Now we use the fact that the minimum distance is $(n-\lambda_2)/2$.

$\square$

Proof of Corollary 7.3: Let k be as in the previous proof, except that k is the largest odd integer such that

$$N_{k+1}(\mathbb{B}^n) \geq n^k/|V_G|.$$

Then taking k-th roots and dividing by n yields that $k = n\gamma + o(n)$ where

$$\sqrt{\gamma/e} + \omega(\gamma) = 2^{-\alpha/\gamma}$$

where $\omega(\gamma) = O(\gamma)$ for γ small. Hence

$$\gamma = \frac{2\alpha}{\log_2(1/\alpha)} + O(\alpha),$$

for α small. Now we follow as in the proceeding proof, except that here $\gamma = k/n$ is, to first order, twice what it was in the previous proof; this factor of two changes the C from $1/\sqrt{4e}$ to $1/\sqrt{2e}$ here.

$\square$

B A Calculus Proposition

In this section we prove Proposition 4.1.

Let f be defined at α_0, and set $\delta_0 = f(\alpha_0)$. It suffices to show that $\alpha_{\max}(\delta_0) \leq \alpha_0$.

For any $\epsilon > 0$ near 0, fix an $\eta > 0$. If

$$\alpha_{\max}\bigl(f(\alpha_0 + \epsilon) + \eta\bigr) > \alpha_0 + \epsilon, \tag{13}$$

then there are codes C_i of length $n_i \to \infty$ as $i \to \infty$ such that $\delta_{C_i} \geq f(\alpha_0 + \epsilon) + \eta$ and

$$\overline{\lim_{i\to\infty}}\, \alpha_{C_i} > \alpha_0 + \epsilon.$$

By passing to a subsequence we can assume that $\alpha_{C_i} > \alpha_0 + \epsilon$ for all i. But then δ_{max} exceeds f (by at least η) at the value $\alpha_0 + \epsilon$, which is impossible. So inequality (13) is impossible, meaning that

$$\alpha_{\max}\bigl(f(\alpha_0 + \epsilon) + \eta\bigr) \leq \alpha_0 + \epsilon.$$

Now let $\eta = \eta(\epsilon) = \delta_0 - f(\alpha_0 + \epsilon)$ and let $\epsilon \to 0$. We conclude $\alpha_{\max}(\delta_0) \leq \alpha_0$, and we are done.

C The First Eigenvalue of a Ball and Related Calculations

In this appendix we prove Proposition 8.5.

Since the size of the ball of radius $n\gamma$ in $\mathbb{B}^n$ is $\approx 2^{nh(\gamma)}$, we need only show that the ball of radius $n\gamma$ has first eigenvalue at least

$$2n\sqrt{\gamma(1-\gamma)} + o(n).$$

Let 0 denote the origin in $(\mathbb{F}_2)^n$, which is a vertex of $\mathbb{B}^n$; the *weight*, $|v|$, of a vertex, v, of $\mathbb{B}^n$ is its distance from 0, or the number of nonzero coordinates it has. Consider those functions, f, on $\mathbb{B}^n$ that depend only on the weight of the vertex. For such an f, let f_{nrm}, the *normalization of* f, be the function on $[0..n]$ such that

$$f_{\mathrm{nrm}}(i) = f(v) \Bigg/ \sqrt{\binom{n}{i}} \qquad \text{for any } v \text{ with } |v| = i.$$

Then it is easy (and completely standard) to see that

$$(A_G f)_{\mathrm{nrm}}(i) = \sqrt{i(n-i+1)}\, f_{\mathrm{nrm}}(i-1) + \sqrt{(i+1)(n-i)}\, f_{\mathrm{nrm}}(i+1),$$

for all i (the coefficient of the right-hand-side vanishes for f_{nrm} at the values -1 and $n+1$). So under normalization the operator A_G becomes a symmetric tridiagonal operator $\widetilde{A}$ whose $i-1, i$ entry is $\sqrt{i(n-i+1)}$. It follows that if $i \in [\gamma n - \omega(n), \gamma n]$, where $\omega(n)$ is any function that is $o(n)$, then the $i-1, i$ entry is

$$n\sqrt{\gamma(1-\gamma)} + o(n).$$

Hence, by monotonicity (see, e.g., [Fri93]), the first Dirichlet eigenvalue of the ball of radius $n\gamma$ is at least that of the path of length $\omega(n)+1$ times

$$n\sqrt{\gamma(1-\gamma)} + o(n).$$

But this path's eigenvalue is well-known to be $2\cos(\pi/\omega(n))$, giving us a lower bound on the ball's eigenvalue of

$$2n\sqrt{\gamma(1-\gamma)} + o(n),$$

provided that $\omega(n)$ grows faster than $\sqrt{n}$ (e.g., we may take $\omega(n) = n^{3/4}$).

$\square$

References

[BCN89] A.E. Brouwer, A.M. Cohen, and A. Neumaier. *Distance regular graphs*. Springer Verlag, Berlin, 1989.

[Cha84] Isaac Chavel. *Eigenvalues in Riemannian geometry*. Academic Press Inc., Orlando, Fla., 1984. Including a chapter by Burton Randol, With an appendix by Jozef Dodziuk.

[DS91] Charles Delorme and Patrick Solé. Diameter, covering index, covering radius and eigenvalues. *European J. Combin.*, 12(2):95–108, 1991.

[Fab23] C. Faber. Beweiss, dass unter allen homogenen Membrane von gleicher Spannung die Kreisförmige den tiefsten Grundton gibt. *Sitzungsber.–Bayer. Akad. Wiss., Math.-Phys. Munich*, pages 169–172, 1923.

[Fri93] Joel Friedman. Some geometric aspects of graphs and their eigenfunctions. *Duke Math. J.*, 69(3):487–525, 1993.

[Kra25] E. Krahn. Über eine von Rayleigh formulierte Minimaleigenschaft des Kreises. *Math. Ann.*, 94:97–100, 1925.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[MRRW77] Robert J. McEliece, Eugene R. Rodemich, Howard Rumsey, Jr., and Lloyd R. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Trans. Information Theory*, IT-23(2):157–166, 1977.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.*, volume I,II. North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[Nil91] A. Nilli. On the second eigenvalue of a graph. *Discrete Math.*, 91(2):207–210, 1991.

[vL99] J. H. van Lint. *Introduction to coding theory*. Springer-Verlag, Berlin, third edition, 1999.