Electronic Colloquium on Computational Complexity, Report No. 33 (2007)

Linear programming bounds for codes via a covering argument

Michael Navon* Alex Samorodnitsky†

Abstract

We recover the first linear programming bound of McEliece, Rodemich, Rumsey, and Welch for binary error-correcting codes and designs via a covering argument. It is possible to show, interpreting the following notions appropriately, that if a code has a large distance, then its dual has a small covering radius and, therefore, is large. This implies the original code to be small.

We also point out (in conjunction with further work) that this bound is a natural isoperimetric constant of the Hamming cube, related to its Faber-Krahn minima.

While our approach belongs to the general framework of Delsarte's linear programming method, its main technical ingredient is Fourier duality for the Hamming cube. In particular, we do not deal directly with Delsarte's linear program or orthogonal polynomial theory.

1 Introduction

This paper takes another look at the first linear programming bound on binary error correcting codes, or, alternatively, on optimal packing of Hamming balls in a Hamming cube.

The bound was originally proved by McEliece, Rodemich, Rumsey, and Welch [15], following Delsarte's linear programming approach [7]. Delsarte showed the distance distribution of a binary code to satisfy a family of linear constraints whose coefficients can be viewed as values of a certain family of orthogonal polynomials, i.e., the Krawchouk polynomials. This made it possible to construct a linear programming relaxation of the original combinatorial question, and to view the obtained linear program as an extremal problem in orthogonal polynomials. Good feasible solutions of the *dual program* were constructed in [15] using tools from the theory of orthogonal polynomials. These solutions lead to the bound, known as *the first linear programming bound* (or the first JPL bound). This bound is the best known upper bound on cardinality of a code with a given minimal distance, for a significant range of distances.

Delsarte's approach extends to a family of finite metric spaces, known as *commutative association schemes*. A Hamming cube is one example of an association scheme. Another relevant example is the Hamming sphere. In [15] good feasible solutions to Delsarte's linear program for the Hamming sphere are constructed. These lead to best known upper bounds on constant weight error correcting codes (ball packing in the Hamming sphere), and, combined

*School of Computer Science and Engineering, Hebrew University, Jerusalem, Israel.
†School of Computer Science and Engineering, Hebrew University, Jerusalem, Israel.

ISSN 1433-8092

with the Bassalygo-Elias inequality, to the best known upper bound on binary codes. This bound is known as the *second linear programming bound*.

We refer to [15, 11, 4, 14] for a detailed exposition of the notions discussed above, including error-correcting codes and their significance, packing in metric spaces, association schemes, Delsarte's linear program, and orthogonal polynomials.

The point of view presented in this paper is somewhat different. Our main tool is Fourier analysis on the group $\mathbb{F}_2^n$, or, equivalently, on the Hamming cube $\{0,1\}^n$. We follow the approach of Kalai and Linial [10] in which the characteristic function of a binary code is viewed as a real-valued function on the cube. A study of the Fourier transform of this function and its simple by-products makes it possible to recover Delsarte's linear program in a form which does not require treatment of Krawchouk polynomials.

Moreover, this viewpoint allows an easy access to new geometric information. Specifically, we establish a simple relation between the minimal distance (equivalently, packing radius) of a code and the *essential covering radius* of its dual. Recall that r is a covering radius of a subset C of $\{0,1\}^n$ if the union of Hamming balls of radius r centered at the points of C covers the whole space. Here we use a somewhat weaker notion, and require this union of balls to cover only a significant fraction of the space.

This observation, which we consider to be the main contribution of this paper, leads to a simple proof of the first linear programming bound. In particular, we do not need to deal directly with Delsarte's linear program or orthogonal polynomial theory.

We move to the principal definitions and to the statement of the main results.

A binary error-correcting code with block length n and minimal distance d is a subset of the n-dimensional Hamming cube in which the distance between any two distinct points is at least d. Let $A(n,d)$ be the maximal size of such a code. In this paper we are interested in the case in which the distance d is linear in the length n of the code, and we let the length n go to infinity. In this case $A(n,d)$ is known [11] to grow exponentially in n, and we consider the quantity

$$R(\delta) = \limsup_{n\to\infty} \frac{1}{n} \log_2 A(n, \lfloor \delta n \rfloor),$$

also known as *the asymptotic maximal rate of the code with relative distance δ* for $0 \le \delta \le \frac{1}{2}$.

Next, we need the notion of a *maximal eigenvalue* of a subset of the cube. We say that two elements x, y of $\{0,1\}^n$ are adjacent and write $x \sim y$ if the Hamming distance between x and y is 1. Let A be the adjacency matrix of the obtained graph. For $B \subseteq \{0,1\}^n$, set

$$\lambda_B = \max \left\{ \frac{\langle Af, f\rangle}{\langle f, f\rangle};\quad f:\ \{0,1\}^n \to \mathbb{R},\ \mathrm{supp}(f) \subseteq B \right\}$$

In other words, λ_B is the maximal eigenvalue of adjacency matrix of the subgraph of $\{0,1\}^n$ induced by the vertices of B.

Our main technical claim is

Proposition 1.1: *Let C be a code with block length n and minimal distance d. Let B be a subset of $\{0,1\}^n$ with $\lambda_B \ge n - 2d + 1$. Then*

$$|C| \le n|B|$$

A linear code C is a linear subspace of $\mathbb{F}_2^n$. The dual code $C^\perp$ is the orthogonal subspace, that is it contains all the vectors orthogonal to C over $\mathbb{F}_2$. Proposition 1.1 has an appealing geometric interpretation for linear codes.

Proposition 1.2: *Let C be a linear code with block length n and minimal distance d. Let B be a subset of $\{0,1\}^n$ with $\lambda_B \geq n - 2d + 1$. Then*

$$\Big| \bigcup_{z \in C^\perp} (z + B) \Big| \geq \frac{2^n}{n}$$

In other words, replacing every point in the dual code by a (shifted) copy of B, we will cover a large fraction of the space $\{0,1\}^n$. Proposition 1.1 for linear codes is an immediate corollary of (1) since $|C| \cdot |C^\perp| = 2^n$.

A code C' has *dual distance d* if Fourier transform of its characteristic function vanishes on points of Hamming weight $0 < |S| < d$. In particular, the dual distance of a linear code is easily seen to equal the minimal distance of its dual (cf. discussion in Subsection 2.1). Hence, the following claim generalizes Proposition 1.2.

Proposition 1.3: *Let C' be a code with block length n and dual distance d. Let B be a subset of $\{0,1\}^n$ with $\lambda_B \geq n - 2d + 1$. Then*

$$\Big| \bigcup_{z \in C'} (z + B) \Big| \geq \frac{2^n}{n} \tag{1}$$

Hamming balls are a good choice for the covering set B.

Lemma 1.4: *Let $B(r)$ be a Hamming ball of radius r. Then*

$$\lambda_{B(r)} \geq 2\sqrt{r(n-r)} - o(n)$$

Proposition 1.3 together with Lemma 1.4 lead to a relation between the dual distance of a code and its essential covering radius.

Corollary 1.5: *Let C' be a code with block length n and dual distance d. Then the essential covering radius of C' is at most*

$$r \leq \frac{n}{2} - \sqrt{d(n-d)} + o(n) \tag{2}$$

In particular, let C be a linear code with block length n and minimal distance d. Then the essential covering radius of the dual code $C^\perp$ is at most $r \leq \frac{n}{2} - \sqrt{d(n-d)} + o(n)$.

Proposition 1.1 together with Lemma 1.4 lead to an upper bound on the size of a code C with block length n and minimal distance d. They show that there exists a radius $r \leq \frac{n}{2} - \sqrt{d(n-d)} + o(n)$ such that

$$|C| \leq n|B(r)| \tag{3}$$

Corollary 1.5 gives a geometric explanation of this bound for a linear code C. The balls of radius r centered at the points of the dual code $C^{\perp}$ cover an $(1/n)$-fraction of the space. Therefore $|C^{\perp}| \cdot |B(r)| \geq 2^n/n$, and $|C| = 2^n/|C^{\perp}| \leq n|B(r)|$. This allows us to view the bound (3) as a *covering bound*.

For a general code the covering interpretation of (3) is more tenuous since, in particular, there is no natural notion of the dual code. However, the analytic reasoning leading to (3) can be viewed as a functional version of the covering argument above (see Subsection 2.3).

The cardinality of a Hamming ball of radius r is $2^{n(H(r/n)+o(1))}$ [12]. Substituting the value $r = \frac{n}{2} - \sqrt{d(n-d)} + o(n)$ on the right hand side of (3), we have

$$|C| \leq 2^{n\left(H\left(1/2-\sqrt{d/n(1-d/n)}\right)+o(1)\right)}$$

This bounds the asymptotic maximal rate of a code with relative distance δ,

$$R(\delta) \leq H\left(1/2 - \sqrt{\delta\,(1-\delta)}\right)$$

This is the first linear programming bound for error-correcting codes.

Finally, a code with dual distance d is a *design of strength* d [11] (or a $(d-1)$-*wise independent set* [1]). Proposition 1.3 together with Lemma 1.4 lead to the *first linear programming bound* for designs [15].

Summing up

Three notions of duality are relevant to this discussion. The first is linear programming duality as represented by the primal and dual linear programs of Delsarte. Recall that the primal linear program of Delsarte is a relaxation of the combinatorial question on cardinality of an optimal code. The linear programming bounds on codes are obtained by constructing good feasible solutions for the dual program.

The second notion is the Fourier duality, illustrated by the Kalai-Linial approach to the problem. Viewing the characteristic function of a code as a real-valued function on the cube, and studying the properties of this function and its Fourier transform lead to an equivalent version of Delsarte's linear program.

The third notion is the duality between packing and covering problems in hypergraphs [2]. The vertices of the pertinent hypergraph are the vertices of the cube and the edges are Hamming balls. The fractional packing and covering problems are dual linear programs. This induces a duality relation between their integer versions which are of interest here. Generally, covering is much easier than packing. For instance, integrality gap for covering is logarithmic at worst [13], while for packing it could be much larger [2]. In the context of coding theory, the asymptotics

of optimal packings are unknown, while the asymptotics of optimal coverings are easy to find [6].

The main observation of this paper is that, in our case, Fourier duality makes it possible to pass from a "hard' packing problem of finding the maximal cardinality of a code with a given minimal distance to an "easy" covering question of determining the minimal cardinality of a code with a given covering radius. We suggest that this point of view might explain the power of the resulting bound, namely the first linear programming bound for error-correcting codes.

We also point out that this bound is a natural isoperimetric constant of the Hamming cube, related to its *Faber-Krahn minima* ([8, 18], see the discussion below).

Related work

1. Our research was motivated by a recent result of Friedman and Tillich [8]. Using methods from algebraic graph theory the authors prove the first linear programming bound for linear binary codes. In particular, Proposition 1.1 for linear codes and Lemma 1.4 are proved in [8].[1] The appeal of [8] is in suggesting a way to work with Delsarte's linear inequalities without resorting to the language and tools of orthogonal polynomial theory.

2. Combining the approach of Friedman and Tillich with the Fourier-analytic view of Delsarte's linear program due to Kalai and Linial allowed us to extend this approach to general binary codes, with, we believe, a simpler proof. After completing our work on the conference version of this paper [16], we learned that Fourier analysis was used in a similar manner by Cohn and Elkies [5] to give a simpler proof of Levenshtein's bound on sphere packing in $\mathbb{R}^n$. In particular, [5] contains (somewhat implicitly) arguments analogous to our proofs of Proposition 1.1 and Lemma 1.4.

3. The relation between the dual distance of a code and its covering radius has been extensively investigated in the coding literature (see [19, 3] and the references there). The best known bounds are obtained via linear programming approach and are somewhat weaker than (2). This, of course, stands to reason, since covering radius of a code is, in general, larger that the essential covering radius. The best known upper bound on the covering radius r_c of a code with dual distance d is [19]

$$r_c \leq \frac{n}{2} - \sqrt{\frac{d}{2}\left(n - \frac{d}{2}\right)} + o(n)$$

   Better bounds are known for linear codes [3].

Extensions and ramifications

1. The approach of this paper extends to general commutative association schemes [17]. Given an association scheme with $k+1$ classes, it is possible to a formal "Fourier transform" on vectors in $\mathbb{R}^{k+1}$. This transform, contrary to a genuine Fourier transform, is

[1] We give a different proof of Lemma 1.4, based on an explicit construction of a function with a large Rayleigh ratio.

not self-dual. The solution is to define a pair of 'inverse transforms'. An appropriate pair of linear transformations is given by the transition matrices of the scheme. It is possible to define a convolution operation for each of these transforms, which is commutative and associative, and which is taken by the transform to a point-wise multiplication. This allows to recover the best known bounds for codes and designs in commutative association schemes via a Fourier-analytic proof similar to the proof of Proposition 1.1.

2. Friedman and Tillich [8] ask what are the optimal covering subsets of the Hamming cube, in the sense of Proposition 1.1. This question is answered in [18], by way of a modified logarithmic Sobolev inequality for the Hamming cube. If B is a Hamming ball and X is a subset of H with $|X| = |B|$, then $\lambda_X \leq (1 + o(1)) \cdot \lambda_B$. Hence Hamming balls are asymptotically optimal. In the terminology of [8], Hamming balls are the Faber-Krahn minimizers for the Hamming cube (up to a negligible error).

2 The proofs

2.1 Fourier analysis on $\mathbb{F}_2^n$

We refer to [9] for background in Fourier analysis on $\mathbb{F}_2^n$. Here we list several necessary definitions and simple facts.

$\mathbb{F}_2^n$ is a finite Abelian group, therefore its characters $\{W_S\}_{S \in \mathbb{F}_2^n}$ constitute a group (the *dual group* which is isomorphic to $\mathbb{F}_2^n$.) The character W_S is a function from $\mathbb{F}_2^n$ to $\{-1, 1\}$, defined as: $W_S(x) = (-1)^{\langle x, S \rangle}$. The characters $\{W_S\}_{S \in \mathbb{F}_2^n}$ form an orthonormal basis in the space of real-valued functions on $\mathbb{F}_2^n$, equipped with uniform probability distribution.

Write $\mathbb{E} f$ for $\frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)$. For $f : \mathbb{F}_2^n \to \mathbb{R}$, define $\widehat{f} : \mathbb{F}_2^n \to \mathbb{R}$ as $\widehat{f}(S) = \langle f, W_S \rangle \stackrel{\text{def}}{=} \mathbb{E}\left(f \cdot W_S\right)$. The function $\widehat{f}$ is the *Fourier Transform* of f. The Parseval identity states $\mathbb{E} fg = \langle f, g \rangle = \left\langle \widehat{f}, \widehat{g} \right\rangle \stackrel{\text{def}}{=} \sum \widehat{f}\widehat{g}$.

For $f, g : \mathbb{F}_2^n \to \mathbb{R}$, the *convolution* of f and g is defined by $(f * g)(x) = \mathbb{E}_y f(y) g(x + y)$. The convolution transforms to dot product: $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$. The convolution operator is commutative and associative.

Finally, we need to know Fourier transforms of some simple functions. The following facts are easily verifiable. Let $f = 1_C$ be the characteristic function of a linear code C. Then $\widehat{f} = \frac{|C|}{2^n} \cdot 1_{C^\perp}$. Let $L(x) = \begin{cases} 2^n & |x| = 1 \\ 0 & \text{otherwise} \end{cases}$. Then $\widehat{L}(S) = n - 2|S|$.

Note, for future use, that a code $C \subseteq \{0, 1\}^n$ has minimal distance d if and only if $\left(1_C * 1_C\right)(x) = 0$ for $0 < |x| < d$. For a linear code C this is equivalent to $1_C(x) = 0$ for $0 < |x| < d$. Observe also that for a function f on the cube holds $Af = f * L$.

2.2 The proof of Proposition 1.3

We start with a simple observation that a function supported on a small set has a large ratio between its second moment and the square of its first moment. Indeed, let a function F be

supported on a set U. Then, by the Cauchy-Schwarz inequality,

$$\mathbb{E}^2 F = \langle F, 1_U \rangle^2 \leq \mathbb{E}F^2 \cdot \mathbb{E}\left(1_U\right)^2 = \frac{|U|}{2^n} \cdot \mathbb{E}F^2 \tag{4}$$

Hence, to prove (1) it suffices to define a function F supported on $\bigcup_{z \in C'} (z + B)$ with $\frac{\mathbb{E}F^2}{\mathbb{E}^2 F} \leq n$. Consider the adjacency matrix of the subgraph of $\{0,1\}^n$ induced by the vertices of B. Let f_B be an eigenfunction of this matrix corresponding to its maximal eigenvalue λ_B. That is, f_B is supported on B and $\lambda_B = \frac{\langle Af_B, f_B \rangle}{\langle f_B, f_B \rangle}$. Since the matrix A is nonnegative, so is the function f_B, and we have $Af_B \geq \lambda_B f_B$. To see this, note that $Af_B = \lambda_B f_B$ on B and, since Af_B is nonnegative, the inequality holds outside B.

For typographic convenience we will write $\lambda = \lambda_B$ and $f = f_B$ from now on.

For a point z in the Hamming cube, let f_z be a shifted version of f, taking $f_z(x) = f(x+z)$. Define

$$F = \frac{1}{2^n} \sum_{z \in C'} f_z = 1_{C'} * f$$

This is a nonnegative function supported on $\bigcup_{z \in C'} (z + B)$. We estimate the inner product $\langle AF, F \rangle$ in two ways.

One one hand,

$$AF = F * L = (1_{C'} * f) * L = 1_{C'} * (f * L) = 1_{C'} * Af \geq \lambda \left(1_{C'} * f\right) = \lambda F$$

Therefore $\langle AF, F \rangle \geq \lambda_B \langle F, F \rangle = \lambda_B \, \mathbb{E}F^2$.

On the other hand, by Parseval's identity,

$$\langle AF, F \rangle = \left\langle \widehat{AF}, \widehat{F} \right\rangle = \left\langle \widehat{L} \cdot \widehat{F}, \widehat{F} \right\rangle = \left\langle (n - 2|S|)\widehat{F}, \widehat{F} \right\rangle = \sum_S (n - 2|S|)\widehat{F}^2(S)$$

Now, $\widehat{F}(S) = \widehat{1_{C'}}(S) \cdot \widehat{f}(S) = 0$, for $0 < |S| < d$. Hence,

$$\sum_S (n - 2|S|)\widehat{F}^2(S) = n\widehat{F}^2(0) + \sum_{|S| \geq d} (n - 2|S|)\widehat{F}^2(S) \leq n\widehat{F}^2(0) + (n - 2d) \sum_{|S| \geq d} \widehat{F}^2(S) \leq$$

$$n\widehat{F}^2(0) + (n - 2d) \sum_S \widehat{F}^2(S) = n\mathbb{E}^2 F + (n - 2d)\mathbb{E}F^2$$

Combining the two estimates on $\langle AF, F \rangle$ and recalling $\lambda \geq n - 2d + 1$, we get

$$n\mathbb{E}^2 F \geq (\lambda - (n - 2d))\, \mathbb{E}F^2 \geq \mathbb{E}F^2,$$

completing the proof. ∎

2.3 The proof of Proposition 1.1

The outline of the following proof is very similar to that of Proposition 1.2. We suggest that it is worthwhile to view this proof as a functional version of the preceding proof. In particular, in light of (4) and (5) below, it is useful to define the "essential support size" of a function g by $2^n \cdot \frac{\mathbb{E}^2 g}{\mathbb{E} g^2}$.

Let ϕ be a function on the Hamming cube such that $\widehat{\phi^2} = 1_C * 1_C$. In other words, $\widehat{\phi * \phi} = 1_C * 1_C$. Since the Fourier transform on the cube is an involution, up to normalization, we have $\phi * \phi = 2^n \, \widehat{1_C * 1_C} = 2^n \, \widehat{1_C}^2$. What is important is that

$$\phi * \phi \geq 0 \quad \text{and} \quad \frac{\mathbb{E}\phi^2}{\mathbb{E}^2 \phi} = \frac{(\phi * \phi)(0)}{\widehat{\phi * \phi}(0)} = |C|$$

That is, the essential support size of ϕ is $\frac{2^n}{|C|}$. Note that, for a linear code C, we can choose ϕ to be (a multiple of) $1_{C^\perp}$.

Take $F = \phi * f$. We will show that $\mathbb{E}F^2 \leq \; n\mathbb{E}^2 F$. It will take an easy additional step to deduce the desired inequality $|C| \leq n|B|$.

As before, we estimate the inner product $\langle AF, F \rangle$ in two ways. On one hand,

$$\langle AF, F \rangle = \langle (\phi * f) * L, \phi * f \rangle = \langle \phi * \phi * f, f * L \rangle = \langle \phi * \phi * f, Af \rangle \geq$$

$$\lambda \langle \phi * \phi * f, f \rangle = \lambda \langle \phi * f, \phi * f \rangle = \lambda \langle F, F \rangle = \lambda \, \mathbb{E}F^2$$

On the other hand, $\langle AF, F \rangle \leq n\mathbb{E}^2 F + (n - 2d)\mathbb{E}F^2$. The proof of this fact is exactly the same as in the proof of Proposition 1.2, and we omit it.

Combining the two estimates and the assumption $\lambda \geq n - 2d + 1$ implies $\mathbb{E}F^2 \leq n\mathbb{E}^2 F$.

Now, $\mathbb{E}^2 F = \mathbb{E}^2 (\phi * f) = \mathbb{E}^2 \phi \; \mathbb{E}^2 f$. On the other hand,

$$\mathbb{E}F^2 = \langle F, F \rangle = \langle \phi * f, \phi * f \rangle = \langle \phi * \phi, f * f \rangle \geq \frac{1}{2^n} (\phi * \phi)(0) \;\; (f * f)(0) = \frac{1}{2^n} \mathbb{E}\phi^2 \; \mathbb{E}f^2$$

The inequality follows from nonnegativity of $\phi * \phi$. Since f is supported on B, the calculation in (4) implies

$$|B| \geq 2^n \frac{\mathbb{E}^2 f}{\mathbb{E} f^2} \geq \frac{1}{n} \frac{\mathbb{E}\phi^2}{\mathbb{E}^2 \phi} = \frac{1}{n} |C|, \tag{5}$$

completing the proof. ∎

2.4 The proof of Lemma 1.4

We prove the lemma by constructing an explicit function f supported on $B = B(r)$ with $\frac{\langle Af, f \rangle}{\langle f, f \rangle} \geq \lambda = 2\sqrt{r(n-r)} - o(n)$. In fact, we will guarantee more, namely $f \geq 0$ and $Af \geq \lambda f$.

The Hamming ball B contains all the points x of the Hamming cube with Hamming weight $|x| \leq r$. The function f will be *symmetric*, namely its value at a point will depend only on the Hamming weight of the point. Such a function, of course, is fully defined by its values $f(0), ..., f(n)$ at Hamming weights $0...n$.

For a symmetric function g on $\{0,1\}^n$ holds $Ag(i) = ig(i-1) + (n-i)g(i+1)$. We start with a preliminary construction of a symmetric function g, setting $g(0) = 1$ and defining $g(i)$ for $1 \leq i \leq n$ so that the relation

$$\lambda g(i) = ig(i-1) + (n-i)g(i+1) \tag{6}$$

is satisfied for $i = 1, ..., n-1$. We will show below that there exists an integer $p \leq r$ and a real number λ such that the function g is nonnegative on the integers $i = 0, ..., p$ and nonpositive on $p+1$, and that $\lambda \geq 2\sqrt{r(n-r)} - o(n)$.

Given this, we define $f = g$ for $i = 0, ..., p$ and $f = 0$ otherwise. Clearly, f is nonnegative and supported on B. We claim $Af \geq \lambda f$. Indeed, by definition, $Af(i) = \lambda f(i)$, for $i \leq p-1$ and for $i > p+1$. It remains to check the two boundary values. For $i = p+1$, $Af(i) \geq 0 = \lambda f(i)$. For $i = p$,

$$Af(i) = pf(p-1) + (n-p)f(p+1) = pf(p-1) = pg(p-1) \geq$$

$$pg(p-1) + (n-p)g(p+1) = \lambda g(p) = \lambda f(p).$$

The inequality holds since $g(p+1) \leq 0$.

It remains to show $\lambda \geq 2\sqrt{r(n-r)} - o(n)$. We will show that there is a function $r(\lambda) = (1+o(n)) \cdot \frac{n-\sqrt{n^2-\lambda^2}}{2}$ such that $g = g_\lambda$ is negative at an integer point $p \leq r(\lambda)$. Writing λ as a function of r gives the relation we need, that is $\lambda \geq 2\sqrt{r(n-r)} - o(n)$.

Fix $\epsilon > 0$. Let $t = \frac{n-\sqrt{n^2-\lambda^2}}{2}$. We will assume that g is positive on the interval $[0, (1+\epsilon)t]$ and obtain a contradiction, for a sufficiently large n.

By the definition of g,

$$g(i+1) = \frac{\lambda g(i) - ig(i-1)}{n-i}.$$

Set $\theta(i) = \frac{f(i)}{f(i-1)}$. Since f is positive on $[0, (1+\epsilon)t]$, for any i in $[t, (1+\epsilon)t]$ holds $\theta(i+1) \geq \frac{i}{\lambda} \geq \frac{t}{\lambda}$. On the other hand, we claim that for any $i > (1+\epsilon/2)t$ holds $\theta(i+1) < \theta(i) \cdot (1-\delta)$, for a positive constant δ depending on ϵ. These two facts evidently cannot coexist, giving the desired contradiction.

Indeed, for any $i \geq 0$ holds $\theta(i+1) = \frac{\lambda}{n-i} - \frac{i}{(n-i)\theta(i)}$. We claim that for $i > (1+\epsilon/2)t$, and for any $x > 0$ holds

$$\frac{\lambda}{n-i} - \frac{i}{(n-i)x} < (1-\delta)x,$$

for some $\delta = \delta(\epsilon) > 0$. In fact, the discriminant of this quadratic inequality in x is easily seen to be negative, for a sufficiently small δ. ∎

3 Acknowledgements

We are grateful to Nati Linial for many useful discussions. We also thank Simon Litsyn and Madhu Sudan for valuable remarks.

References

[1] N. Alon, L. Babai, and A. Itai, *A fast and simple randomized parallel algorithm for the maximal independent set problem*, J. Algorithms, 7, vol. 4, 1986.

[2] R. Aharoni, P. Erdos, and N. Linial, *Optima of dual integer linear programs*, Combinatorica, 8 (1), 1988, 13-20.

[3] A. Ashkihmin, I. Honkala, T. Laihonen, and S. Litsyn, *On relations between covering radius and dual distance*, IEEE Trans. Inform. Theory, vol. IT-45, 1999, 1808-1816.

[4] E. Bannai and T. Ito, **Algebraic Combinatorics I: Association Schemes**, Benjamin/Cummings, 1984.

[5] H. Cohn, N. Elkies, *New upper bounds for sphere packings I*, Annals of Math., 157, 2003, pp. 689-714.

[6] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, **Covering Codes**, Elsevier, 1997.

[7] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep., Suppl., vol. 10, 1973.

[8] J. Friedman and J-P. Tillich, *Generalized Alon-Boppana Theorems and Error-Correcting Codes*, preprint, 2002.

[9] J. Kahn, G. Kalai, and N. Linial, *The influence of variables on boolean functions*, FOCS 1988, pp. 68-80.

[10] G. Kalai and N. Linial, personal communication.

[11] V. I. Levenshtein, *Universal bounds for codes and designs*, in Handbook of Coding Theory, V.S. Pless and W.C. Huffman Eds., Amsterdam, Elsevier, 1998.

[12] J.H. van Lint, **Introduction to Coding Theory**, Third edition. Springer-Verlag, Berlin, 1999.

[13] L. Lovasz, *On the ratio of optimal integral and fractional covers*, Disc. Math, 13, 1975, 383-390.

[14] J. MacWilliams and N. J. A. Sloane, **The Theory of Error Correcting Codes**, Amsterdam, North-Holland, 1977.

[15] R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch, *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities*, IEEE Trans. Inform. Theory, vol. IT-23, 1977, 157-166.

[16] M. Navon, A. Samorodnitsky, *On Delsarte's linear programming bounds for binary codes*, Proceedings of FOCS 46.

[17] A. Samorodnitsky, *The proof of the first JPL bound for association schemes via formal Fourier transform*, manuscript.

[18] A. Samorodnitsky, *An asymptotic Faber-Krahn inequality for the Hamming cube*, manuscript.

[19] A. Tietavainen, *Upper bound on the covering radius of a code as a function of its dual distance*, IEEE Trans. Inform. Theory, vol. IT-36, 1990, 1472-1474.

[20] G. Szegö, **Orthogonal Polynomials**, American Mathematical Society, 1939.

[21] V. A. Yudin, *Lower bounds for spherical designs*, Izvestiya. Mathematics 61:3, 1997, 673-683.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/