Spectral approach to linear programming bounds on binary codes

Alexander Barg
Dept. of ECE and Inst. for Systems Research
University of Maryland
College Park, MD 20742, USA
Email: abarg@umd.edu

Dmitry Nogin
IPPI RAN
Bol'shoj Karetnyj 19
Moscow 101447, Russia
Email: nogin@iitp.ru

***Abstract*— We give a new proof of the asymptotic upper bound on the size of binary codes obtained within the frame of Delsarte's linear programming method. The proof relies on the analysis of eigenvectors of some finite-dimensional operators related to Krawtchouk polynomials.**

I. Introduction

The problem of bounding the size of codes with a given minimum distance is one of the classical topics of coding theory. A powerful technique to bound M above as a function of d that is applicable in a large class of metric spaces is Delsarte's linear programming method [3]. In particular, the best known upper bounds on the size of codes in the examples mentioned above are obtained by using linear programming. We will be concerned with the case of large n. The best known asymptotic estimates of the size of binary codes and binary constant weight codes were obtained in McEliece, Rodemich, Rumsey, Welch [5] and are called the MRRW bounds. Our objective will be to give a new proof of these results that relies on the analysis of eigenvalues of some finite-dimensional operators related to orthogonal polynomials. Linear-algebraic ideas that we follow were introduced in a recent paper by Bachoc [1] in which a similar approach has been taken to establish an asymptotic bound for codes in the real Grassmann manifold.

II. Notation and preliminaries

Let C be a binary code of length n, size M and minimum distance $d = d(C)$. The maximum size of the code with a given value of d can be estimated by Delsarte's linear programming bound as follows. Let $\{\tilde{K}_k(x), k = 0, 1, \dots, n\}$ be the family of Krawtchouk polynomials orthogonal with respect to the inner product $\langle \tilde{K}_k, \tilde{K}_m \rangle = \sum_{i=0}^{n} \mu_H(i) \tilde{K}_k(i) \tilde{K}_m(i)$, where $\mu_H(i) = 2^{-n}\binom{n}{i}$, and normalized so that $\|\tilde{K}_k\|^2 = \langle \tilde{K}_k, \tilde{K}_k \rangle = 1$.

Theorem 2.1: [3] Let C be an (n, M, d) code. Let $F(x) = \sum_{i=0}^{t} F_i \tilde{K}_i(x)$ be a polynomial that satisfies

(a) $F_0 > 0, F_1, \dots, F_t \geq 0$;

(b) $F(j) \leq 0, j = d, d+1, \dots, n$.

Then $M \leq F(0)/F_0$.

This theorem is equivalent to a linear programming problem whose variables are the coefficients of the distance distribution of the code C. For this reason, estimates obtained from this theorem are called the Linear programming bounds.

The polynomials $\tilde{K}_k$ satisfy a three-term recurrence relation

$$(n-2x)\tilde{K}_k(x) = \sqrt{(n-k)(k+1)}\tilde{K}_{k+1}(x) + \sqrt{(n-k+1)k}\tilde{K}_{k-1}(x). \quad (1)$$

We also have (see [3])

$$\tilde{K}_i(x)\tilde{K}_j(x) = \sum_{k=0}^{n} p_{i,j}^k \tilde{K}_k(x), \quad (2)$$

where the numbers $p_{i,j}^k$ are nonnegative, and

$$\tilde{K}_k(0) = \sqrt{\binom{n}{k}}. \quad (3)$$

For a square symmetric matrix A we denote by $\lambda_{\max}(A)$ its maximum eigenvalue.

III. The method

Let V_k be the space of polynomials of degree $\leq k$ considered as a subspace of the space $V = L_2(d\mu_H)$, i.e., the space of functions on $\{1, 2, \dots, n\}$ with the inner product

$$\langle f, g \rangle = 2^{-n} \sum_i \binom{n}{i} f(i)g(i).$$

Below we use bold letters to denote operators acting on V and regular letters to denote their matrices in the basis $\{\tilde{K}_i\}$. Let $\mathbf{E}_k$ be the orthogonal projection from V to V_k. Consider the operator

$$\mathbf{S}_k = \mathbf{E}_k \circ (n-2x) : \ V_k \to V_k,$$

i.e., multiplication by $(n-2x)$ followed by projection on V_k. The argument that follows relies on the fact that this operator is self-adjoint with respect to the bilinear form $\langle \cdot, \cdot \rangle$. Indeed, both multiplication by a function and the orthogonal projection are self-adjoint operators. Therefore, the matrix S_k is symmetric. Its explicit form is shown on the next page.

A $p \times p$ matrix $A \geq 0$ is called irreducible if for any partition of the set of indices $\{1, 2, \dots, p\} = \{i_1, i_2, \dots i_s\} \cup \{j_1, j_2, \dots, j_t\}$ into two disjoint subsets with $s + t = p$, the matrix $(a_{i_\alpha, j_\beta})_{1 \leq \alpha \leq s, 1 \leq \beta \leq t}$ is nonzero (in other words,

$$S_k = \begin{bmatrix} 0 & \sqrt{n} & 0 & \dots & \dots & 0 \\ \sqrt{n} & 0 & \sqrt{2(n-1)} & \dots & \dots & 0 \\ 0 & \sqrt{2(n-1)} & 0 & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & 0 & \sqrt{(k-1)(n-k+2)} & 0 \\ \dots & \dots & \dots & \sqrt{(k-1)(n-k+2)} & 0 & \sqrt{k(n-k+1)} \\ 0 & 0 & \dots & 0 & \sqrt{k(n-k+1)} & 0 \end{bmatrix}.$$

a directed graph G with vertices $\{1, 2, \dots, p\}$ and edges (i, j) whenever $A_{ij} > 0$ is strongly connected). For instance, the matrix S_k is irreducible.

In the next lemma we collect the properties of irreducible matrices used below.

Lemma 3.1: Let $A \geq 0$ be a $p \times p$ irreducible symmetric matrix.

(a) Its largest eigenvalue $\lambda_{\max}(A)$ is positive and has multiplicity one. There exists a vector $y > 0$ such that $Ay = \lambda_{\max}(A)y$.

(b) $\lambda_{\max}(A) \leq \max_{1 \leq i \leq p} \sum_j A_{ij}$.

(c) For any $y \neq 0$, $\lambda_{\max}(A) \geq \frac{(Ay,y)}{(y,y)}$.

(d) If $0 \leq B \leq A$ for some matrix B, or if B is a principal minor of A, then $|\lambda_{\max}(B)| \leq \lambda_{\max}(A)$.

Here claims (a),(b),(d) form a part of the Perron-Frobenius theory, claim (c) is obvious and holds true for any square matrix.

Theorem 3.2: Let C be an (n, M, d) code. Then

$$M \leq \frac{4(n-k)}{n - \lambda_{\max}(S_k)} \binom{n}{k}$$

for all k such that $\lambda_{\max}(S_{k-1}) \geq n - 2d$.

Proof: Let $g = \sum_{i=1}^{k} g_i \tilde{K}_i \in V_k$. Consider the operator $\mathbf{T}_k : V_k \to V_k$ defined by

$$\mathbf{T}_k g = \mathbf{S}_k g - (n-k) g_k \tilde{K}_k \tag{4}$$

and let θ_k be its largest eigenvalue. Recall that T_k is the matrix of this operator in the basis $\{\tilde{K}_i\}$. (T_k is the same as S_k except that $(T_k)_{k+1,k+1} = -(n-k)$.) Let us "shift" the matrix T_k by a multiple of the identity matrix I to make all of its elements nonnegative. For instance, we have $T_k + (n-k)I \geq 0$. By the Perron-Frobenius theorem,

$$\lambda_{\max}(S_{k-1}) < \theta_k < \lambda_{\max}(S_k)$$

because the same inequalities hold for the largest eigenvalues of the shifted matrices. Moreover, the eigenvalue θ_k is of multiplicity one. Denote by $f \in V_k$ the eigenvector that corresponds to it. By (4) we have

$$(n - 2x)f = \theta_k f + (n-k) f_k \tilde{K}_k + f_k a_k \tilde{K}_{k+1},$$

so

$$f = \frac{(n-k)\tilde{K}_k + a_k \tilde{K}_{k+1}}{n - 2x - \theta_k} f_k.$$

Consider the polynomial $F = ((n-k)\tilde{K}_k + a_k \tilde{K}_{k+1})f$. By Lemma 3.1(a), f can be chosen to have positive coordinates. Therefore by (2), the coefficients of the expansion of F into the basis $\{\tilde{K}_i\}$ are nonnegative. Next, if $n - 2d \leq \lambda_{\max}(S_{k-1})$ then $F(x) \leq 0$ for $x \geq d$.

Since multiplication by f is a self-adjoint operator, we compute

$$\begin{aligned} F_0 &= \langle ((n-k)\tilde{K}_k + a_k \tilde{K}_{k+1}) f, 1 \rangle \\ &= \langle (n-k)\tilde{K}_k + a_k \tilde{K}_{k+1}, f \rangle \\ &= (n-k) f_k > 0, \end{aligned}$$

and

$$F(0) = \frac{\left((n-k)\sqrt{\binom{n}{k}} + a_k \sqrt{\binom{n}{n-k}} \right)^2}{n - \theta_k} f_k.$$

Substituting $a_k = \sqrt{(k+1)(n-k)}$ we find

$$F(0) = \frac{4(n-k)^2 f_k}{n - \theta_k} \binom{n}{k} < \frac{4(n-k)^2 f_k}{n - \lambda_{\max}(S_k)} \binom{n}{k}$$

provided that $\lambda_{\max}(S_k) < n$. The claimed estimate is obtained by using the polynomial F in Theorem 2.1. ∎

Remark 1. This result is close to the previously known estimates obtained within the frame of Delsarte's method. In particular, Levenshtein constructed a sequence of polynomials that are optimal in the Delsarte problem (with some qualifiers), see, e.g., [4]. The results of [4] imply that the above estimate does not improve the known bounds on M. The result of [5] is also of the form similar to Theorem 3.2.

Next we compute the asymptotic behavior of the largest eigenvalue.

Lemma 3.3: Let $k < n/2, \lambda_k = \lambda_{\max}(S_k)$. For all $s = 2, \dots, k+1$,

$$\lambda_k \geq \frac{2(s-1)}{s} \sqrt{(k-s+2)(n-k+s-1)}$$

$$\lambda_k \leq 2\sqrt{k(n-k+1)}.$$

In particular,

$$\lim_{n \to \infty,\ k/n \to \tau} \frac{\lambda_k}{n} = 2\sqrt{\tau(1-\tau)}.$$

Proof: By Lemma 3.1(b)

$$\lambda_k \leq \sqrt{(k-1)(n-k+2)} + \sqrt{k(n-k+1)},$$

hence the upper bound. On the other hand, take $y = (0^{k-s+1}1^s)^t$. Then by part (c) of the same lemma,

$$\lambda_k \geq \frac{2}{s}\sum_{p=0}^{s-1}\sqrt{(k-p)(n-k+p+1)}.$$

Since for $k \leq n/2$ the quantity $(k-p)(n-k+p+1)$ decreases as p grows, we can replace p with $s-2$ in every term under the sum. This implies the lower bound. Finally, taking $s \to \infty, s = o(n)$ we establish the limiting behavior of λ_k. ■

Theorem 3.2 and Lemma 3.3 together lead to the following asymptotic result (the asymptotic MRRW bound for binary codes [5]):

$$\frac{1}{n}\log M \leq h(1/2 - \sqrt{\delta(1-\delta)})(1+o(1)).$$

Indeed, let $\lim \frac{d}{n} = \delta$ and assume that $\delta \leq 1/2$. We need to choose k so that $n^{-1}\lambda_{\max}(S_{k-1}) \geq (1-2\delta)(1+o(1))$ as $n \to \infty$. In the limit, this amounts to taking τ that satisfies $2\sqrt{\tau(1-\tau)} \geq 1-2\delta$, or $\tau \geq 1/2 - \sqrt{\delta(1-\delta)}$. The result now follows by the Stirling approximation.

IV. Conclusion

In the full version of this paper [2] we state and prove the a general form of Theorem 3.2 above that applies to a broad class of polynomial metric spaces and consider the other main examples of interest to coding theory (constant weight codes, spherical codes). In this talk we have shown the working of the method for the most well-studied case of binary codes.

Acknowledgment

The research of the first author was supported in part by the NSF under grants CCR-0310961 and CCF-0515124. The research of the second author was supported in part by the NSF under grant CCR-0310961 and by RFFI under grant 02-01-22005.

References

[1] C. Bachoc, *Linear progamming bounds for codes in Grassmannian spaces*, preprint, 2005.

[2] A. Barg and D. Nogin, *Spectral approach to linear programming bounds of coding theory*, preprint, 2005, arxiv.org/cs.IT/0512025.

[3] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Repts Suppl. **10** (1973), 1–97.

[4] V. I. Levenshtein, *Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces*, IEEE Trans. Inform. Theory **41** (1995), no. 5, 1303–1321.

[5] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, *New upper bound on the rate of a code via the Delsarte-MacWilliams inequalities*, IEEE Trans. Inform. Theory **23** (1977), no. 2, 157–166.