On Bounded Weight Codes

Christine Bachoc Venkat Chandar Gérard Cohen Patrick Solé Aslan Tchamkerten

Abstract

The maximum size of a binary code is studied as a function of its length n, minimum distance d, and *minimum* codeword weight w. This function $B(n, d, w)$ is first characterized in terms of its exponential growth rate in the limit $n \to \infty$ for fixed $\delta = d/n$ and $\omega = w/n$. The exponential growth rate of $B(n, d, w)$ is shown to be equal to the exponential growth rate of $A(n, d)$ for $0 \leq \omega \leq 1/2$, and equal to the exponential growth rate of $A(n, d, w)$ for $1/2 < \omega \leq 1$. Second, analytic and numerical upper bounds on $B(n, d, w)$ are derived using the semidefinite programming (SDP) method. These bounds yield a non-asymptotic improvement of the second Johnson bound and are tight for certain values of the parameters.

Index Terms

Constant weight codes, Johnson bounds, semidefinite programming

I. Introduction

Two classical functions in combinatorial coding theory are $A(n, d)$, the largest size of a binary code of length n and minimum distance d, and $A(n, d, w)$, the largest size of a binary code of length n, minimum distance d, and constant weight w. A closely related function is $B(n, d, w)$, obtained from $A(n, d, w)$ by relaxing the weight constraint to only require that the weight of each codeword is at least w. Codes satisfying a minimum weight constraint are called *heavy weight codes* in [7], where they are motivated by certain asynchronous communication problems. The other relaxation where codewords are required to have weight at most w defines the function $L(n, d, w)$. Complementation immediately shows that $L(n, d, w) = B(n, d, n - w)$. The function L naturally occurs in the proof of the Elias bound [15, Lemma 2.5.1]. It also occurs in the problem of list decoding when bounding the size of the list as a function of the decoding radius w. In this problem, $L(n, d, w)$ represents the largest size of a list of codewords at distance at most w from the received vector, given a binary code of length n and minimum distance d. This function is denoted by $A_2'(n, d, w)$ in [14], where the Elias Lemma [15, Lemma 2.5.1] is referred to as the Johnson bound, and is used to prove upper bounds on the list size.

In the present paper we first characterize the asymptotic exponent of $B(n, d, w)$ as a function of those of $A(n, d)$ and $A(n, d, w)$ (Theorem 1). This result is based on the asymptotic unimodality of $A(n, d, w)$, which was conjectured in [7, Conjecture 2]. Note that, the non asymptotic analogue of this result (posed as a research problem in [16, p.674]) is *false* as $A(15, 6, 6) < A(15, 6, 7)$ [19].

Second, we provide upper bounds on $L(n, d, w)$ obtained by the semidefinite programming method. From these bounds, we derive a non asymptotic improvement of the Elias/Johnson Lemma in a certain range of n, d, and w (Theorem 3) as well as numerical tables.

The material is organized as follows. Section II contains elementary bounds and some tables of $B(n, d, w)$ derived therefrom. Section III contains the asymptotic results. Section IV is dedicated to the SDP method. Section V explores three heavy weight codes construction techniques. In Section VI we provide some concluding remarks.

C. Bachoc is with the University of Bordeaux (France), V. Chandar is with MIT Lincoln Laboratory (USA), and G. Cohen , P. Solé, and and A. Tchamkerten are with Telecom ParisTech (France). A. Tchamkerten is partly supported by an Excellence Chair grant from the French National Research Agency (ANR, ACE project). Part of this work appeared at ISIT 2010.

II. Elementary bounds

In this section we establish a few basic relations between $B(n,d,w)$ and $A(n,d,w)$.

Note first that $B(n,d,w)$ is increasing in n, and decreasing in d and w. Further, by definition of $B(n,d,w)$, we have

$$B(n,d,w) \geq A(n,d,j) \quad \text{for } j \geq w\,. \tag{1}$$

By taking weight classes sufficiently far apart so that they do not overlap, we get

$$B(n,d,w) \geq \sum_{h=0}^{\lfloor \frac{n-w}{d} \rfloor} A(n,d,w+hd) \tag{2}$$

where $\lfloor x \rfloor$ denotes the largest integer not exceeding x.

Since any code is a disjoint union of constant weight codes, we have

$$B(n,d,w) \leq \sum_{j=w}^{n} A(n,d,j)\,. \tag{3}$$

Removing the weight constraint can only improve the size, hence

$$B(n,d,w) \leq A(n,d) = B(n,d,0)\,. \tag{4}$$

The following result is analogous to the first half of the first Johnson bound [6, $(3a)$]:[1]

Proposition 1: For $w \leq n$ we have

$$B(n,d,w) \leq \frac{n}{w} B(n-1,d,w-1)\,.$$

Proof: Let C be a code realizing $B(n,d,w)$, and consider the matrix whose rows are its codewords. Since the average weight of a column, which we denote by W, is given by the total number of 1's in the matrix divided by n, we get

$$W \geq \frac{wB(n,d,w)}{n}\,. \tag{5}$$

Now, say column l has weight at least W (one such column clearly exists). Pick the subcode of C given by the codewords of C that have a 1 in the l-th position. Modify this subcode by deleting the l-th component of each codeword. If we denote by C' the resulting code, we conclude that $W \leq |C'| \leq B(n-1,d,w-1)$. Using this together with (5) yields the desired result. ■

Finally, the following Gilbert type lower bound is immediate:

Proposition 2: For all $n \geq 1$, $d \leq n$, and $w \leq n$

$$B(n,d,w) \geq \frac{\sum_{i=w}^{n} \binom{n}{i}}{\sum_{i=0}^{d-1} \binom{n}{i}}\,.$$

We conclude this section with tables derived from the preceding bounds. Some trivial entries are $B(n,d,w) = 1$ whenever $d > \min\{2w, 2(n-w)\}$. We limited n and d to the values where $A(n,d)$ and $A(n,d,w)$ are known exactly (for all w) in [5], [6]. Entries of the tables where $w > n$ are left blank.

[1] Whether or not the analogous of the second half of the first Johnson bound, i.e. [6, $(3b)$], holds as well remains an open question. Specifically, it is unclear at this point whether the inequality

$$B(n,d,w) \leq \frac{n}{n-w} B(n-1,d,w)$$

is valid.

TABLE I: $B(n,4,w)$

n	$A(n,4)$	$w=2$	$w=3$	$w=4$	$w=5$	$w=6$	$w=7$	$w=8$	$w=9$
6	4	4	3-4	3 -4	1	1			
7	8	8	7-8	7-8	3-5	1	1		
8	16	16	15 -16	15-16	8-10	4 -6	1	1	
9	20	20	19-20	19-20	18-20	12-18	4-6	1	
10	40	40	39- 40	39-40	36-40	30-40	13-20	5-7	1

TABLE II: $B(n,6,w)$

n	$A(n,6)$	$w=2$	$w=3$	$w=4$	$w=5$	$w=6$	$w=7$	$w=8$	$w=9$
9	4	4	4	3- 4	3- 4	3-4	1	1	1
10	6	6	6	6	6	5- 6	3- 6	1	1
11	12	12	12	11-12	11-12	11- 12	6- 9	3- 6	1
12	24	24	24	23- 24	23-24	23-24	12- 24	9-16	4- 7
13	32	32	32	31-32	31- 32	31- 32	26-32	18-32	13- 20

III. Asymptotics

For fixed $\delta, \omega \in [0,1]$, we denote by $b(\delta,\omega)$ the exponential growth rate of $B(n,d,w)$ with respect to n with $d = d(n) = \lfloor \delta n \rfloor$ and $w = w(n) = \lfloor \omega n \rfloor$, i.e.

$$b(\delta,\omega) = \limsup_{n\to\infty} \left(\frac{1}{n} \log B(n, d(n), w(n)) \right)$$

where logarithms are taken to the base 2 throughout the paper. The asymptotic exponents of $A(n,d,w)$ and $A(n,d)$ are defined similarly and are denoted by $a(\delta,\omega)$ and $a(\delta)$, respectively.

Proposition 3: For any $\delta \in [0,1]$ and $\omega \in [0,1/2]$, we have $b(\delta,\omega) = a(\delta)$.

Proof: The Elias-Bassalygo bound [18, equation (2.8)]

$$\frac{A(n,d)}{2^n} \leq \frac{A(n,d,w)}{\binom{n}{w}} \tag{6}$$

together with the trivial inequality $A(n,d,w) \leq A(n,d)$ shows that the asymptotic exponents of $A(n,d)$ and $A(n,d,n/2)$ are the same. The result then follows by combining the bounds (1) and (4) to obtain

$$A(n,d,n/2) \leq B(n,d,w) \leq A(n,d)$$

for $w \leq n/2$. ■

The next result provides the main ingredient for proving that $b(\delta,\omega) = a(\delta,\omega)$ when $\omega \in (1/2,1]$.

Theorem 1: For fixed $\delta \in [0,1]$, $a(\delta,\omega)$ is unimodal in ω with a maximum at $\omega = 1/2$.

Corollary 1: For any $\delta \in [0,1]$ and $\omega \in (1/2,1]$, we have $b(\delta,\omega) = a(\delta,\omega)$.

Proof of Corollary 1: We have

$$\max_{j\in\{w,w+1,\ldots,n\}} A(n,d,j) \leq B(n,d,w) \leq (n-w+1) \max_{j\in\{w,w+1,\ldots,n\}} A(n,d,j) \tag{7}$$

by (1) for the first inequality and by (3) for the second inequality. Letting $w = \lfloor \omega n \rfloor$ and $d = \lfloor \delta n \rfloor$ we get

$$\max_{j\in\{w,w+1,\ldots,n\}} A(n,d,j) = \max_{\rho\in[\omega,1]} A(n,d,\lfloor \rho n \rfloor)\,, \tag{8}$$

TABLE III: $B(n, 8, w)$

n	$A(n,8)$	$w=2$	$w=3$	$w=4$	$w=5$	$w=6$	$w=7$	$w=8$	$w=9$
12	4	4	4	4	4	4	3- 4	3- 4	1
13	4	4	4	4	4	4	4	3-4	3-4
14	8	8	8	8	8	8	8	7- 8	4- 8
15	16	16	16	16	15-16	15-16	15-16	15-16	10- 16

and therefore from (7) we have

$$b(\delta, \omega) = \sup_{\omega \leq \rho \leq 1} a(\delta, \rho)$$

for any $\delta \in [0, 1]$ and $\omega \in [0, 1]$. Assuming that $1/2 < \omega \leq 1$, the theorem then follows from Theorem 1. ■

Proof of Theorem 1:: We establish that $a(\delta, \cdot)$ is non-decreasing over $[0, 1/2]$. This, by complementation, shows that $a(\delta, \cdot)$ is non-increasing over $[1/2, 1]$, proving the claim.

Fix $\delta \in [0, 1]$ and let ω_1, ω_2 be such that $0 \leq \omega_1 < \omega_2 \leq 1/2$. Throughout the proof we disregard discrepancies due to the rounding of non-integer quantities as they play no role asymptotically. Thus, for instance, we shall always treat $\omega_1 n$ as if it is an integer.

We show that, from a given constant weight code C_1 with parameters $(n, d = \delta n, w_1 = \omega_1 n)$ such that $|C_1| = A(n, d, w_1)$, it is possible to construct a constant weight code C_2 with parameters $(n, d, w_2 = \omega_2 n)$, of size at least equal to $|C_1|$ multiplied by $1/(n+1)^2$. This shows that $a(\delta, \omega_2) \geq a(\delta, \omega_1)$. The code C_2 is obtained from C_1 via translation.

For a given fixed codeword $\mathbf{c} \in C_1$, let us construct a length n binary vector $\mathbf{t}$ of weight

$$w = \omega n = \frac{\omega_2 - \omega_1}{1 - 2\omega_1} n$$

as follows. Consider first the positions of $\mathbf{t}$ that form the support of $\mathbf{c}$ (w_1 of them). Pick $\omega_1 w$ of these positions arbitrarily and assign them 1's. Similarly, assign 1's to an arbitrary selection of the $(1 - \omega_1)w$ positions that lie outside the support of $\mathbf{c}$. The remaining positions of $\mathbf{t}$ are filled with 0's. Note that, by of our choice of w, the vector $\mathbf{c}' = \mathbf{t} \oplus \mathbf{c}$ (component wise modulo 2 sum of $\mathbf{t}$ and $\mathbf{c}$) has weight w_2.

Now observe that, because the selections made to construct $\mathbf{t}$ are arbitrary, for any given $\mathbf{c} \in C_1$ there are

$$\binom{\omega_1 n}{\omega_1 \omega n} \binom{(1 - \omega_1) n}{(1 - \omega_1) \omega n}$$

ways of choosing $\mathbf{t}$ for which $\mathbf{c}'$ has weight w_2. Therefore, if we now pick $\mathbf{t}$ randomly and uniformly among all possible sequences of weight w, the probability that this sequence translates a given $\mathbf{c} \in C_1$ to a sequence of weight w_2 is given by

$$p = \frac{\binom{\omega_1 n}{\omega_1 \omega n} \binom{(1-\omega_1) n}{(1-\omega_1) \omega n}}{\binom{n}{\omega n}} \,.$$

This implies that a vector $\mathbf{t}$ that is randomly and uniformly chosen among all possible sequences of weight w translates on average

$$pA(n, d, w_1)$$

codewords from C_1 into codewords of weight w_2 (and minimum distance d). Therefore,

$$A(n, d, w_2) \geq pA(n, d, w_1) \,.$$

Finally, using the following standard bounds on binomial coefficients[2]

$$\frac{1}{(n+1)}2^{nh(k/n)} \leq \binom{n}{k} \leq 2^{nh(k/n)} \quad k \leq n\,,$$

(see, e.g.,[11, Example 11.1.3, p.353]) shows that

$$p \geq \frac{1}{(n+1)^2}\,.$$

Therefore we obtain

$$A(n,d,w_2) \geq \frac{1}{(n+1)^2}A(n,d,w_1)\,,$$

from which the theorem follows. ■

IV. Upper bounds on $L(n,d,w)$ from semidefinite programming

The semidefinite programming method is a far reaching generalization of Delsarte linear programming method to obtain bounds for extremal problems in coding theory. In the present situation, we aim at upper bounding $L(n,d,w)$, which is the maximal number of elements of a code contained in the ball $B(w)$ centered at the all-zero word with radius w of the binary Hamming space $H_n = \{0,1\}^n$. We obtain numerical bounds for small values of the parameters (n,d,w), which improve the elementary bounds for $B(n,d,n-w) = L(n,d,w)$ given in Section II. We also obtain a new bound, which is an explicit function of (n,d,w), and improves on the Elias/Johnson bound for some values of these parameters.

The numerical bounds are obtained by a straightforward application of the SDP method. We refer to [2] for a survey of this method and its applications to the binary Hamming space, including the case of codes in balls. See also [3] for a survey on the more general subject of symmetry reduction of semidefinite programs, with applications to coding theory. In a few words, $L(n,d,w)$ can be interpreted as the independence number of a certain graph with vertex set H_n, thus is upper bounded by the so-called *Lovász theta number* ϑ of this graph (or rather by its strengthening ϑ'), which is the optimal value of a certain semidefinite program. This SDP has exponential size, but can be reduced to polynomial size by the action of the symmetry group of the graph, which is the symmetry group of $B(w)$, i.e. the group S_n of permutations of the n coordinates.

Let us recall that a function $F : H_n^2 \mapsto \mathbb{R}$ is said to be *positive definite* (or positive semidefinite) if the matrix $(F(x,y))$ indexed by H_n is positive semidefinite. This property is denoted $F \succeq 0$. In the symmetrization process discussed above, a description of the S_n-invariant positive definite functions on H_n is required. This description is in fact provided in [20], under the name of block diagonalization of the Terwilliger algebra of the Hamming space, and in the framework of group representations in [22]. Numerical upper bounds for $L(n,d,w)$ obtained in this way are displayed in Tables IV, V, VI.

For the announced explicit bound, we use a slightly different (and self contained) formulation of the SDP bound, which is given in Theorem 2. We shall recover the Elias/Johnson bound as a special case, and obtain a new bound in Theorem 3. There, we follow the same line for Hamming balls as the one followed for spherical caps in [4]. In the latter, the SDP method has lead to numerical bounds and also to explicit bounds of degree up to two.

A. Improving the Johnson bound

We start with a more handy restatement of the SDP bound, which is essentially the dual form of the SDP defining the theta number ϑ'. The notations are as follows: the space of functions on H_n is denoted $\mathcal{C}(H_n) = \{f : H_n \mapsto \mathbb{C}\}$ and is endowed with the standard inner product $\langle f_1, f_2\rangle = \frac{1}{2^n}\sum_{x\in H_n} f_1(x)\overline{f_2(x)}$. We shall consider the decomposition of this space under the action of the full automorphism group

[2] $h(p)$ denotes the binary entropy $-p\log p - (1-p)\log(1-p)$.

$\mathrm{Aut}(H_n)$ of the Hamming space and under the action of the symmetric group S_n. Since the irreducible components are indeed real, we can restrict to the real valued functions.

The orbit of $(x,y) \in H_n^2$ under the action of S_n is determined uniquely by the values of $u := \mathrm{wt}(x)$, $v := \mathrm{wt}(y)$ and $t := d(x,y)$. Thus the elements of $F \in \mathcal{C}(H_n^2)$ which are S_n-invariant, i.e. which satisfy $F(gx,gy) = F(x,y)$ for all $g \in S_n$, $(x,y) \in H_n^2$, are of the form $F = F(u,v,t)$. With this notation, $F \succeq 0$ stands for: $(x,y) \mapsto F(\mathrm{wt}(x), \mathrm{wt}(y), d(x,y)) \succeq 0$.

Theorem 2: Let

$$\Omega(n,d,w) := \{(u,v,t) \in \mathbb{N}^3 : \ 0 \le u,v \le w, \ d \le t \le n,$$
$$t \le u+v, \ u+v-t \equiv 0 \mod 2\}.$$

Let $P(u,v,t) \in \mathbb{R}[u,v,t]$ be a polynomial symmetric in (u,v). If P satisfies the following conditions:

1) $P - f_0 \succeq 0$ for some $f_0 > 0$
2) $P(u,v,t) \le 0$ for all $(u,v,t) \in \Omega(n,d,w)$,
3) $P(u,u,0) \le 1$ for all $u \in \{0,\dots,w\}$,

then

$$L(n,d,w) \le \frac{1}{f_0}.$$

Proof: For $(x,y) \in H_n^2$, let $F(x,y) := P(\mathrm{wt}(x), \mathrm{wt}(y), d(x,y))$. We consider for a code $C \subset B(w)$ with minimal distance at least equal to d, the sum

$$S := \sum_{(x,y)\in C^2} F(x,y).$$

From property (1) of P, we have $S \ge f_0|C|^2$. On the other hand, $S = S_1 + S_2$ where S_1 is the sum over pairs $(x,y) \in C^2$ with $x = y$ and S_2 is the sum over the non equal pairs $(x,y) \in C^2$, $x \ne y$. Condition 2) on P insures that $S_2 \le 0$ and condition 3) on P that $S_1 \le |C|$. Altogether we obtain $|C| \le 1/f_0$. ∎

In order to apply the above theorem with specific polynomials $P(u,v,t)$, we need an explicit description of those who are positive definite. Such a description is indeed obtained in [20], and in [22] in terms of orthogonal polynomials (Hahn polynomials to be precise). As we shall see, for our purpose, we need a slightly different expression.

A general method is explained in [1], [2], [3], involving group representation. The space $\mathcal{C}(H_n)$ can be decomposed into the direct sum of S_n-irreducible subspaces. The sum of those subspaces which are isomorphic to a given irreducible representation of S_n is called an isotypic subspace. We recall that certain matrices $E_k(x,y)$ are associated to the isotypic components $\mathcal{I}_k$ of $\mathcal{C}(H_n)$ under the action of S_n. Here $k \in [0..\lfloor n/2 \rfloor]$, $\mathcal{I}_k$ corresponds to the irreducible representation $[n-k,k]$ of the symmetric group S_n, and has multiplicity $n-2k+1$. Moreover, $E_k(x,y)$ is S_n-invariant thus can be expressed in terms of (u,v,t), namely $E_k(x,y) := Y_k(u,v,t)$. Then we have the following characterization (we use the standard notation $\langle A,B\rangle = \mathrm{Trace}(AB^*)$ for matrices):

Proposition 4: For all $P \in \mathbb{R}[u,v,t]$, symmetric in (u,v), $P \succeq 0$ if and only if

$$P(u,v,t) = \sum_{k=0}^{\lfloor n/2 \rfloor} \langle F_k, E_k(x,y)\rangle \tag{9}$$

where for $k \in [0..\lfloor n/2 \rfloor]$, $F_k \in \mathbb{R}^{m_k \times m_k}$, $m_k = n-2k+1$, and $F_k \succeq 0$. More precisely, $E_k(x,y)$ is computed from a decomposition of $\mathcal{I}_k$ into irreducible subspaces $\mathcal{I}_k = R_{k,1} \oplus \dots R_{k,m_k}$. If for all i, $(e_{k,i,1},\dots,e_{k,i,h_k})$ is an orthonormal basis of $R_{k,i}$ in which the action of S_n is expressed by the same matrices (i.e., not depending on i), then

$$E_{k,i,j}(x,y) = \sum_{s=1}^{h_k} e_{k,i,s}(x) e_{k,j,s}(y).$$

The decomposition of $\mathcal{I}_k$ with irreducible submodules is not unique but changes $E_k(x,y)$ to $AE_k(x,y)A^*$ for an invertible matrix A, see [1, Lemma 4.2]. Note that such a change does not affect the above characterization of P being positive definite since $\langle F_k, AE_k(x,y)A^*\rangle = \langle A^*F_kA, E_k(x,y)\rangle$ and $F_k \succeq 0$ if and only if $A^*F_kA \succeq 0$.

There are essentially two strategies to obtain such a decomposition. One can start from the decomposition of $X = H_n$ into orbits under the action of S_n, namely $X = X_0 \cup \cdots \cup X_n$, with $X_k = \{x \in H_n : \mathrm{wt}(x) = k\}$, which leads to a decomposition of the functional space $\mathcal{C}(X) = \mathcal{C}(X_0) \perp \cdots \perp \mathcal{C}(X_n)$ and then decompose each S_n-space $\mathcal{C}(X_k)$, following [12]. It is the method adopted in [22] where the corresponding matrices $E_k(x,y)$ are obtained in terms of Hahn polynomials. Another approach starts from the decomposition of $\mathcal{C}(H_n)$ under the full $\mathrm{Aut}(H_n)$, namely $\mathcal{C}(H_n) = P_0 \perp P_1 \perp \cdots \perp P_n$ where $P_k = \oplus_{\mathrm{wt}(w)=k}\mathbb{C}\chi_w$, $\chi_w(x) = (-1)^{w\cdot x}$, then decomposes each P_k under the action of the subgroup S_n. Because we want to work with polynomials in (u,v,t) of low degree, this last decomposition is better suited. Indeed, if $P \in \mathbb{R}[u,v,t]$, then $x \mapsto F(x,y) := P(\mathrm{wt}(x), \mathrm{wt}(y), d(x,y))$ belongs to $P_0 \perp \cdots \perp P_k$ if and only if the total degree of P in the variables (u,t) is at most equal to k.

An isomorphism of S_n-modules between $\mathcal{C}(X_k)$ and P_k is given by ϕ_k:

$$\begin{aligned}\phi_k : \mathcal{C}(X_k) &\to P_k\\ f &\mapsto \phi_k(f) := \sum_{\mathrm{wt}(w)=k} f(w)\chi_w.\end{aligned}$$

so we have exactly the same picture for the decomposition of $\mathcal{C}(H_n)$ when P_k replaces $\mathcal{C}(X_k)$, namely the irreducible decomposition of P_k under the action of S_n that is for $0 \le k \le \lfloor \frac{n}{2} \rfloor$, we have

$$P_k = H_{0,k} \perp H_{1,k} \perp \cdots \perp H_{k,k} \tag{10}$$

and the isotypic components of $\mathcal{C}(H_n)$, i.e.

$$\mathcal{I}_k = H_{k,k} \perp H_{k,k+1} \perp \cdots \perp H_{k,n-k} \simeq H_{k,k}^{n-2k+1}.$$

Since $u = \mathrm{wt}(x)$, as a function of x, is invariant under S_n, and is of degree 1, the isotypic subspace $\mathcal{I}_k$ can also be decomposed as:

$$\mathcal{I}_k = \oplus_{i=0}^{n-2k} u^i H_{k,k}$$

Moreover, starting from an orthonormal basis $(e_{k,s})$ of $H_{k,k}$, we obtain an orthonormal basis $(u^i e_{k,s})$ of $u^i H_{k,k}$ in which the action of S_n is expressed by the same matrices, thus we can use it to compute the corresponding matrix $E_k(x,y)$ the coefficients of which will be equal to:

$$E_{k,i,j}(x,y) = u^i v^j \sum_{s=1}^{h_k} e_{k,s}(x)e_{k,s}(y).$$

In other words, it is enough to compute $Z_k(x,y) := \sum_{s=1}^{h_k} e_{k,s}(x)e_{k,s}(y)$, which is the zonal function associated to $H_{k,k}$, in terms of (u,v,t). We obtain:

Proposition 5: We have the following expressions for Z_k, up to a positive multiplicative constant:

- $Z_0 = 1$
- $Z_1 = -t + u + v - 2uv/n$
- $Z_2 = t^2 + (2/(n-2))(n - nu - nv + 2uv)t + (1/(n-1)(n-2))(4u^2v^2 - 4n(u^2v + uv^2) + (n+2)(n-1)(u^2+v^2) + 2n(n+1)uv - 2n(n-1)(u+v))$

Proof: We take the following notations: if $\mathrm{wt}(w) = 1$, and $w_i = 1$, we let $\chi_i := \chi_w$. Let

$$\begin{cases} U := n - 2u = \sum_{i=1}^n \chi_i(x),\\ V := n - 2v = \sum_{i=1}^n \chi_i(y),\\ T := n - 2t = \sum_{i=1}^n \chi_i(x)\chi_i(y).\end{cases}$$

Following [12], and the isomorphism ϕ_k defined above, $H_{k,k} = \ker(d)$ where $d : P_k \to P_{k-1}$ is defined by: $d\chi_w = \sum \chi_{w'}$ where the sum is over the words w' of weight $\mathrm{wt}(w') = \mathrm{wt}(w) - 1$, and of support contained in the support of w. We set $d = d_x$ to specify the variable under consideration and $d = d_x + d_y$ when applied to a function $F(x, y)$ on H_n^2. Then, Z_k is uniquely determined up to a multiplicative constant by the properties:

1) $Z_k \in \mathbb{R}[U, V, T]$, is symmetric in (U, V),
2) $x \mapsto Z_k(x, y)$ belongs to P_k,
3) $dZ_k = 0$.

According to the decomposition (10) with pairwise non isomorphic irreducible subspaces, the space of functions satisfying conditions (1) and (2) below is of dimension $1+k$. In the variable x, U and T belong to P_1, and it is easy to check that $U^2 - n$, $UT - V$, $T^2 - n$, belong to P_2. Thus a basis for the space of functions satisfying (1) and (2) is given by:

$$\begin{cases} k = 0 : \quad \{1\} \\ k = 1 : \quad \{UV, T\} \\ k = 2 : \quad \{(U^2 - n)(V^2 - n), \\ UVT - U^2 - V^2 + n, T^2 - n\} \end{cases}$$

The assertion $Z_0 = 1$ is then trivial. In order to compute Z_1 and Z_2, we need formulas for the image under d of the monomials in (U, V, T). We compute the following:

$$\begin{cases} d_x 1 = d1 = 0, \\ d_x U = n \quad \text{thus} \quad d(UV) = n(U + V), \\ d_x T = V \quad \text{thus} \quad dT = U + V. \end{cases}$$

With the above we obtain that Z_1 is proportional to $T - \frac{1}{n}UV$. Similarly we obtain:

$$\begin{cases} d(U^2 + V^2) = 2(n - 1)(U + V), \\ d(U^2V^2) = 2(n - 1)(U^2V + UV^2), \\ d(UVT) = (U^2V + UV^2) + (n - 2)(U + V)T, \\ d(T^2) = -2(U + V) + 2(U + V)T. \end{cases}$$

and Z_2 turns to be proportional to

$$\begin{aligned} T^2 - n - \frac{2}{n-2}(UVT - U^2 - V^2 + n) \\ + \frac{1}{(n-1)(n-2)}(U^2 - n)(V^2 - n). \end{aligned}$$

From the identity $Z_k(x, x) = \sum e_{k,s}(x)^2$, we have that $Z_k(U, U, 0) \geq 0$ which determines the sign of the multiplicative factor. We obtain the announced formulas. ■

Remark: The method used to calculate the polynomials Z_k for $0 \leq k \leq 2$ outlines an algorithmic way to compute Z_k for general k. It would be more satisfactory to have an expression of these polynomials in terms of orthogonal polynomials.

Now we apply Theorem 2 in order to obtain upper bounds for $L(n, d, w)$. We start with a polynomial $P(u, v, t)$ of degree one and recover Elias bound: Let

$$\begin{aligned} P(u, v, t) :=& Z_1(u, v, t) + d - 2w(1 - w/n) \\ =& d - t + (u + v - 2uv/n) - 2w(1 - w/n). \end{aligned}$$

With $f_0 := d-2w(1-w/n)$, we have $P - f_0 \succeq 0$. If $w \leq n/2$, the maximum over $[0,w]^2$ of $u+v-2uv/n$ equals $2w(1-w/n)$, and is attained for $u=v=w$. Thus $P(u,v,t) \leq 0$ for $(u,v,t) \in \Omega(n,d,w)$, and $P(u,u,0) \leq d$. Thus we obtain that if $w \leq n/2$ and $d > 2w(1-w/n)$, then

$$L(n,d,w) \leq \frac{d}{d-2w(1-w/n)}. \tag{11}$$

It is unclear in general how to design a good polynomial P of degree k. A possible strategy is to start from a polynomial $L(t)$ optimizing the bound for $A(n,d)$ and disturb it with a polynomial $p(u,v)$, i.e. take $P = L(t) + p(u,v)$. Since $L(t) \succeq 0$, condition (1) of Theorem 2, is equivalent to $F_0 - f_0 E_0 \succeq 0$. In order to fulfill condition (2), it is enough to have $p(u,v) \leq 0$ for $[u,v] \in [0,w]^2$ so one can take $p(u,v) = (u+v-2w)s(u,v)$ or $p(u,v) = (u(u-w)+v(v-w))s(u,v)$ where $s(u,v)$ is a sum of squares. For the degree 1, if one follows this line and takes $P = (d-t) + \lambda(u+v-2w)$ with $\lambda > 0$, one finds that the optimal choice of λ is $\lambda = 1-2w/n$ and obtains again the Elias bound (11). For the degree 2, we consider accordingly a polynomial P of the form

$$P = (t-d)(t-n) + \lambda(u(u-w)+v(v-w)),$$

with $\lambda \geq 0$. The matrix $F_0(\lambda)$ associated to P is equal to

$$F_0(\lambda) = \begin{pmatrix} nd & -n-d-\lambda w & 1+\lambda \\ & 4n/(n-1)+2d/n & -4/(n-1) \\ & & 4/(n(n-1)) \end{pmatrix}.$$

Let $f_0(\lambda) := \det(F_0(\lambda)$. The lower left 2×2 corner of $F_0(\lambda)$ is positive semidefinite so the matrix $F_0(\lambda) - f_0 E_0$ is positive semidefinite if and only if its determinant is non negative, which amounts to the condition

$$f_0 \leq \frac{n^2(n-1)}{8d} f_0(\lambda).$$

On the other hand

$$P(u,u,0) = dn + 2\lambda u(u-w) \leq dn$$

so we obtain the bound $8d^2/((n-1)f_0(\lambda))$. It remains to find the maximum of $f_0(\lambda)$, which is a polynomial of degree 2 in λ:

$$\begin{aligned} \frac{n(n-1)}{2} f_0(\lambda) &= -((n-1)d + 2(n-w)^2)\lambda^2 \\ &+ d(2n+2-4w)\lambda + d(2d-(n-1)). \end{aligned}$$

The maximum is attained for $\lambda_0 = d(n+1-2w)/((n-1)d+2(n-w)^2)$, $\lambda_0 \geq 0$ if $w \leq (n+1)/2$, and is equal to

$$\frac{4d\big(d^2 + \frac{2(n-w)(n+1-2w)}{n-1} d - (n-w)^2\big)}{n((n-1)d+2(n-w)^2)}.$$

This last value is positive if and only if

$$d > \frac{(n-w)}{(n-1)}\big(\sqrt{2(n-w)(n-1)} - (n+1-w)\big).$$

Altogether we obtain:

Theorem 3: Assume $w \leq (n+1)/2$ and

$$d > \frac{(n-w)}{(n-1)}\big(\sqrt{2(n-w)(n-1)} - (n+1-w)\big).$$

TABLE IV: $d = 4$

$n \backslash w$	4	5	6	7	8	9	10	11	12	13		$A(n,4) \leq$
10	31	37										40
11	42^*	67										72
12	56^*	100	138									144
13	72^*	144^*	221	248								256
14	92^*	201^*	340	411	486	503						512
15	114^*	274^*	508	750	849	989	1002					1024
16	$\mathbf{141}^*$	365^*	736	1184	1571	1767	1984	2012				2048
17	171	477	1039	1813	2602	2981						3276
18	205	613	1437	2703	4183	5041	6007	6324				6552
19	243	776	1947	3933	6541	9174	10532	12249	12641			13104
20	286	970	2594	5600	9976	14966	19390	21965	24834	25388		26168

Then

$$L(n,d,w) \leq \frac{2d\left(d + \frac{2(n-w)^2}{n-1}\right)}{d^2 + \frac{2(n-w)(n+1-2w)}{n-1}d - (n-w)^2}.$$

Example: with the above we obtain $L(n, n/2, n/2) \leq 2n - 1$. It is an almost sharp bound in view of $A(n, n/2, n/2) = 2n - 2$ for values of n for which an Hadamard matrix of order n exists [6, Theorem 10]. Note that adding the all zero codeword to such an Hadamard code yields $L(n, n/2, n/2) = 2n - 1$.

Example: For $d = 2w(1 - w/n)$ the degree 1 bound does not apply. The degree 2 gives a bound if $w > n/2 - \sqrt{n^2/(2(n+1))}$ which equals

$$\frac{2w(n^2 - w)}{\frac{n^2}{2} - (n+1)\left(w - \frac{n}{2}\right)^2}.$$

B. Tables

The tables IV, V and VI give upper bounds of $L(n,d,w)$ employing the SDP method. They *always* improve on the bound (4) (Cf right most column) and sometimes on (3) when the latter is stronger than the former. This situation is indicated by a star exponent.

In some cases they allow us to derive *exact* values of $L(n,d,w)$ by using the expurgation technique of the next section. These cases are indicated by bold face numbers. To do that we collect the weight enumerators of some special binary codes in the notation of [16].

The weight enumerator of the $RM(2,4)$ dual of the $RM(1,4)$ is computed by MacWilliams transform [16, Ch. 5, Th. 1] as

$$x^{16} + y^{16} + 140(x^{12}y^4 + x^4y^{12}) + 448(x^{10}y^6 + x^6y^{10})$$
$$+870x^8y^8.$$

This shows by expurgation that

$$L(16,4,4) = 141.$$

The weight enumerator of the Nordstrom Robinson code is

$$x^{16} + y^{16} + 112(x^{10}y^6 + x^6y^{10}) + 30x^8y^8.$$

This shows by expurgation

$$L(16,6,6) = 113,\ L(16,6,10) = 255.$$

The weight enumerator of the extended Golay code is

$$x^{24} + y^{24} + 759(x^{16}y^8 + x^8y^{16}) + 2576x^{12}y^{12}.$$

TABLE V: $d = 6$

$n\backslash w$	6	7	8	9	10	11		$A(n,6) \leq$
14	51	56	63					64
15	74	96	113	127				128
16	**113**	157	207	228	**255**	255		256
17	159	250	318					340
18	205	409	481	563	677			680
19	259	554	752	913	1107			1280
20	324	739	1200	1519	1835	2096		2372

TABLE VI: $d = 8$

$n\backslash w$	8	9	10	11	12	13	14	15	16		$A(n,8) \leq$
18	67										72
19	100	123	137								142
20	154	222	253								256
21	245	359	465								512
22	349	598	759	870	967	990	1023				1024
23	**507**	831	1112	1541	1800	1843	1936	2047	**2048**		2048
24	**760**	1161	1641	2419	**3336**	3439	3711	3933	**4095**		4096

Shortening we obtained the dual of the perfect Golay code.

$$x^{23} + 506x^{15}y^8 + 1288x^{11}y^{12} + 253x^7y^{16}.$$

This shows by expurgation

$$L(24, 8, 8) = 760,\ L(24, 8, 12) = 3336,\ L(24, 8, 16) = 4095,$$

and

$$L(23, 8, 8) = 507,\ L(23, 8, 16) = 2048.$$

V. Constructions

Three well studied code construction techniques are expurgation, translation, and concatenation. In the context of heavy weight codes, the first is perhaps mostly of theoretical interest as a good decoding algorithm needs not, in general, provide a good decoding algorithm for a subcode. In contrast, the other two techniques also provide practical decoding algorithms.

A. Expurgation

The following result shows that, for $w \leq d$, $B(n, d, w)$ and $A(n, d)$ are essentially the same (recall that $B(n, d, w) \leq A(n, d)$).

Proposition 6: For $1 \leq w \leq d \leq n$, we have

$$B(n, d, w) \geq A(n, d) - 1.$$

Proof: Let C be a code achieving $A(n, d)$. By first translating this code so that to include the all-zero codeword, then by removing the all-zero codeword, we get a new code of size $A(n, d) - 1$, with minimum distance and weight both at least equal to d. The proposition follows. ■

Theorem 4: For all large enough and even n, all $w \leq n/2$, and all $d \leq nh^{-1}(1/2)$,[3] we have

$$B(n, d, w) \geq 2^{(n-2)/2}.$$

[3] $h^{-1}(\cdot)$ denotes the inverse function of the binary entropy over the range $[0, 1/2]$.

Proof: Pick a self dual code above the Gilbert bound [17]. This code being binary self-dual, contains the all-one codeword, and is therefore self-complementary. Hence, half of its codewords at least have weight at least $n/2$. ■

B. Translation

We assume that the reader has some familiarity with the covering radius concept [10]. Recall that the covering radius of a code is the smallest integer t such that Hamming balls of radius t centered on the codewords cover the ambient space. Define $R(n,d)$ as the largest covering radius of a code achieving $A(n,d)$. Since the covering radius exceeds $\lfloor (d-1)/2 \rfloor$, we get $R(n,d) \geq \lfloor (d-1)/2 \rfloor$ with equality iff the code that achieves $R(n,d)$ is perfect. A sharper bound on $R(n,d)$ for non perfect codes is obtained as a direct consequence of the sphere covering bound

$$2^n \leq A(n,d) \sum_{i=0}^{R(n,d)} \binom{n}{i}.$$

The motivation for taking “largest” rather than “smallest” in the definition of $R(n,d)$ is to have the best upper bound on w in the next Proposition, which sharpens, in certain cases, Proposition 6.

Proposition 7: Fix two integers $n \geq 1$ and $d \geq 1$. If $w \leq R(n,d)$ then

$$B(n,d,w) = A(n,d).$$

Proof: Pick a code C realizing $A(n,d)$. There exists a translate of C of weight w as long as w is less than or equal to the covering radius of C. This gives $B(n,d,w) \geq A(n,d)$. The reverse inequality is (4). ■

C. Concatenation

Consider an heavy weight code of length n, size q, minimum weight w, and distance d. If we concatenate this code with a code of length N, size M, and minimum distance D over $GF(q)$, we get a binary code of length Nn, weight at least wN, size M and minimum distance dD. Hence, provided $B(n,d,w) \geq q$, we see that

$$B(Nn, dD, wN) \geq A_q(N,D)\,.$$

where $A_q(N,D)$ denotes the largest size of a code of length N and minimum distance D, over $GF(q)$. Efficient decoding algorithms for concatenated codes can be found in [13].

VI. Concluding remarks

We investigated $B(n,d,w)$, defined as the largest number of codewords of weight at least w and minimum distance d. The asymptotic exponent of $B(n,d,w)$ is reduced to those of $A(n,d)$ or $A(n,d,w)$, depending on w. For finite values of the parameters, we obtained bounds on $B(n,d,w)$ partly using the SDP method. As future research, it might be possible to find new exact values of $B(n,d,w)$ by special constructions. In this direction, one possibility is to investigate $R(n,d)$ defined in Section V.

Acknowledgement

We thank Navin Karshyap for pointing out [19].

REFERENCES

[1] C. Bachoc, *Semidefinite programming, harmonic analysis and coding theory*, arXiv:0909.4767.
[2] C. Bachoc, *Applications of semidefinite programming to coding theory*, ITW 2010, Dublin.
[3] C. Bachoc, D. C. Gijswijt, A. Schrijver, F. Vallentin, *Invariant semidefinite programs* arXiv:1007.2905 .
[4] C. Bachoc, F. Vallentin, *Semidefinite programming, multivariate orthogonal polynomials and codes in spherical caps*, Europ. J. Comb. 30 (2009), 625-637.
[5] Best, M. R.; Brouwer, A. E.; MacWilliams, F. Jessie; Odlyzko, Andrew M.; Sloane, Neil J. A. Bounds for binary codes of length less than 25. IEEE Trans. Information Theory IT-24 (1978), no. 1, 81–93.
[6] Brouwer, A. E.; Shearer, James B.; Sloane, N. J. A.; Smith, Warren D. A new table of constant weight codes. IEEE Trans. Inform. Theory IT-36 (1990), no. 6, 1334–1380.
[7] G. Cohen, P. Solé, A. Tchamkerten, Heavy weight codes, ISIT 2010.
[8] Chandar, Venkat; Tchamkerten, Aslan; Wornell, Gregory, Training-based schemes are suboptimal for high rate asynchronous communication, Information Theory Workshop (ITW),Taormina, Italy, October 2009.
[9] Brouwer, A. E., Cohen, A. M.; Neumaier, A. *Distance-regular graphs.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) , 18. Springer-Verlag, Berlin, 1989.
[10] G.Cohen, I.Honkala, S.Litsyn, A.Lobstein, *Covering Codes*, Elsevier, 1997.
[11] T.Cover and J. Thomas, *Information Theory*, Wiley, 2006.
[12] P. Delsarte, *Hahn polynomials, discrete harmonics and t-designs*, SIAM J. Appl. Math. **34**-1 (1978)
[13] Dumer, Ilya I., Concatenated codes and their multilevel generalizations in *Handbook of coding theory*, Vol. II, V. Pless and W.C Huffman, eds, 1911–1988, North-Holland, Amsterdam, 1998.
[14] V. Guruswami, M; Sudan, Extensions to the Johnson bound, available from `http://www.cs.cmu.edu/ venkatg/pubs/pubs.html`
[15] W. Cary Huffman, Vera Pless *Fundamentals of error correcting codes*, Cambridge (2003).
[16] MacWilliams, F. J.; Sloane, N. J. A, *The theory of Error Correcting Codes*, North Holland (1977).
[17] MacWilliams, F. J.; Sloane, N. J. A.; Thompson, J. G. Good self dual codes exist. Discrete Math. 3 (1972), 153–162.
[18] McEliece, Robert J.; Rodemich, Eugene R.; Rumsey, Howard, Jr.; Welch, Lloyd R. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. IEEE Trans. Information Theory IT-23 (1977), no. 2, 157–166.
[19] Patric R. J. Östergård, Classification of binary constant weight codes, IEEE Trans. Inform. Theory, to appear.
[20] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Trans. Inform. Theory IT-51 (2005), 2859–2866.
[21] Tchamkerten, Aslan; Chandar, Venkat; Wornell, Gregory, Communication under strong asynchronism, IEEE Trans. Information Theory, IT-55 (2010), no. 10, 4508-4528.
[22] F. Vallentin, *Symmetry in semidefinite programs*, Linear Algebra and Appl. 430 (2009), 360-369.