On Bounded Weight Codes

Christine Bachoc Gérard Cohen Patrick Solé Aslan Tchamkerten

Abstract

The function $B(n,d,w,)$ the largest size of a binary code of length n, minimum distance d and minimum weight $\geq w$ is studied in comparison with the classical functions $A(n,d)$ and $A(n,d,w)$. The asymptotic growth rate $b(\delta,\omega)$ of $B(n,d,w)$ with respect to n and with fixed ratios $\delta = d/n$ and $\omega = w/n$ is shown to be equal to $a(\delta)$, the asymptotic exponential growth rate of $A(n,d)$, for $0 \leq w \leq 1/2$ and to $a(\delta,w)$ the asymptotic exponential growth rate of $A(n,d,w)$, for $1/2 \leq w \leq 1$. Sharp upper bounds on $B(n,d,w)$ are derived by the semidefinite programming (SDP) method.

Index Terms

constant weight codes, asynchronous communication, list decoding, semi definite programming

I. Introduction

Two classical functions in combinatorial coding theory are $A(n,d)$ and $A(n,d,w)$, the largest size of, respectively, a binary code of length n, minimum distance d, and of a binary code of length n, minimum distance d and constant weight w. A relaxation of the latter is the function $B(n,d,w)$ where the constant weight condition is replaced by minimum weight $\geq w$. Codes satisfying these constraints are called *heavy weight codes* in [7] where they were introduced to perform joint synchronization and error correction. See the introduction of [7] and the reference [8] for details and motivation. Another relaxation of interest is the function $L(n,d,w)$, where the constant weight condition is replaced by maximum weight $\leq w$. Corresponding codes might be called *light weight codes*. Complementation shows directly that $L(n,d,w) = B(n,d,n-w)$. This function occurs naturally in the proof of the Elias bound [14, Lemma 2.5.1]. It also occurs in the problem of list decoding when bounding the size of the list of closest codeword as a function of the decoding radius. Thus $L(n,d,w)$ is the largest size of a list of codewords at distance at most w from the received vector for a binary code of length n and distance d. This function is denoted by $A_2'(n,d,w)$ in [13], where [14, Lemma 2.5.1] is called the Johnson bound.

In the present paper we determine completely the asymptotic exponent of $B(n,d,w)$ as a function of those of $A(n,d)$ and $A(n,d,w)$. To achieve this goal we need to prove the asymptotic unimodality of $A(n,d,w)$, which was Conjecture 2 of [7]. We are indebted to Venkat Chandar for sketching a probabilistic proof of this conjecture. The proof given in section III is combinatorial. In section IV we apply the semidefinite programming method to derive upper bounds on $L(n,d,w)$. This allows us to improve the tables of finite values of $B(n,d,w)$ and also to give a non asymptotic improvement of the Elias/ Johnson Lemma.

The material is organized as follows. The next section 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 code construction techniques. A final section puts our results into perspective and collects some challenging open problems.

Christine Bachoc is with Math Dept, Bordeaux University, 33 Talence France. The last three authors are with Telecom ParisTech (Networks and Computer Science dept. for G. Cohen and Communications and Electronics dept. for P. Solé and A. Tchamkerten), 46 rue Barrault, 75634 Paris Cedex 13, 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

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

For reference we give the following analogue of the first half of the first Johnson bound [6, (3a)].

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 bounded weight code realizing $B(n,d,w)$, and consider the matrix whose rows are the codewords of C. The average weight W of a column is given by the total number of 1's in the matrix divided by n, i.e.,

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

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 code obtained after the above two procedures, we conclude that $W \leq |C'| \leq B(n,d,w-1)$. The result follows. ■

It is not clear if the analogue of the second half of the first Johnson bound, i.e. [6, (3a)], holds as well:

Question: Is it true that

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

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 by a series of tables derived from the preceding bounds. Some trivial entries are $B(n,d,n) = 1$ for all d and $B(n,d,n-1) = 1$ for $d \geq 3$, as well as $B(n,n,w) = 1$ for all w. We limited n and d to the values where the functions $A(n,d)$ and $A(n,d,w)$ are known exactly (for all w) in [5], [6]. Entries of the tables where $w > n$ are left blank.

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	1-2	
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- 3	1	1
10	6	6	6	6	6	5- 6	3- 6	1-3	1- 2
11	12	12	12	11-12	11-12	11- 12	6- 9	3- 6	1- 3
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

A. *The support of* $b(\delta, \omega)$

For fixed $\delta, \omega \in [0, 1]$, we denote by $b(\delta, \omega)$ the asymptotic exponent 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 the logarithm is to the base 2. 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.

The asymptotic Plotkin bound [14, Theorem 2.10.2], shows that $a(\delta) = 0$ for $\delta \in [1/2, 1]$. Hence, by (4) $b(\delta, \omega) = 0$ for all $\delta \in [1/2, 1]$ and all $\omega \in [0, 1]$. In fact, the support of $b(\delta, \omega)$ can be completely characterized.

Proposition 3: $b(\delta, \omega) > 0$ if and only if $\delta < 2\omega(1 - \omega)$.

Proof of Proposition 3: If $\delta < 2\omega(1 - \omega)$, then $a(\delta, \omega) > 0$ by the 'Gilbert lower bound' [17, p.160, right column, bottom]

$$a(\delta, \omega) \geq h(\omega) - \omega h(\delta/2\omega) - (1 - \omega) h(\delta/2(1 - \omega))\,.$$

Hence, $b(\delta, \omega) > 0$ by (1).

Now, restating a classical lemma of Elias [14, Lemma 2.5.1] yields

$$B(n, d, w) \leq \frac{nd}{nd - 2w(n - w)}$$

whenever $nd > 2w(n - w)$. Hence, by letting $d \simeq \delta n$ and $w \simeq \omega n$ with $\delta > 2\omega(1 - \omega)$, we get

$$\limsup_{n \to \infty} B(n, d, w) \leq \frac{\delta}{\delta - 2\omega(1 - \omega)}\,,$$

implying that $b(\delta, \omega) = 0$ whenever $\delta > 2\omega(1 - \omega)$. ■

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- 4
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

B. The easy half plane: $\omega \leq 1/2$

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

Proof of Theorem 2: The Elias-Bassalygo bound [17, equation (2.8)]

$$\frac{A(n,d)}{2^n} \leq \frac{A(n,d,w)}{\binom{n}{w}} \tag{5}$$

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 $w \leq n/2$. ■

C. Unimodality of $a(\delta, \omega)$

The following result is of interest in its own right.

Theorem 2: For any fixed $\delta \in [0, 1]$ we have that $a(\delta, \omega)$ is a nonincreasing function of $\omega \in [1/2, 1]$.

Proof: The scheme of the proof is as follows. Given two relative weights ω_1, ω_2 in the range $0 < \omega_1 < \omega_2 < 1/2$, we start from a constant weight code C_1 of parameters (n, d, w_1) such that $|C_1| = A(n, d, w_1)$ and construct, by translation by a vector t of weight w say, and expurgation a constant weight code C_2 of parameters (n, d, w_2) and same size as C_1 up to subexponential factors in n. Hence $a(\delta, \omega_2) \geq a(\delta, \omega_1)$. We assume that w_i grows like $\omega_i n$. Based on heuristics of independence we decide to choose a w such that

$$w_2 = w + w_1 - 2\lfloor w w_1/n \rfloor$$

or asymptotically on n

$$w \approx \frac{w_2 - w_1}{1 - 2\omega_1}.$$

Now we want to compute the proportion Π of suitable t (ie such that $t + C_1$ contains vectors of weight w_2) amongst all binary vectors of length n and weight w. Let x (resp y) denote the number of ones of t on (resp. outside) the support of an arbitrary $c \in C_1$. The bound on Π will turn out to be independent of c. We see that

$$\Pi \binom{n}{w} = \binom{w_1}{x} \binom{n - w_1}{y}$$

Surely $x + y = w$, the weight of t. Also for t to be suitable we need $y - x = w_2 - w_1$. Solving this system, we find that $x = \omega_1 w$ and $y = (1 - \omega_1)w$. We recall the standard estimates [15, Chap 10, Lemma 7] on the growth of binomial coefficients. For integers $m \leq n$ and $m \asymp \lambda n$ with $0 < \lambda < 1$, we have

$$\mu(\lambda) \le \binom{n}{m} 2^{-nh(\lambda)}\sqrt{n} \le M(\lambda),$$

where μ, M depend on λ but not on n. With these approximations we come up with the bound

$$\Pi \ge \kappa(\omega_1, \omega_2)/\sqrt{n},$$

where the quantity κ does not depend on n. To conclude we count the pairs (t, c). Counting c's first, we get $A(n, d, w_1)\Pi\binom{n}{w}$. Averaging over t we see that there is a translate with at least $A(n, d, w_1)\Pi$ vectors of weight w_2. These vectors form a constant weight code of parameters (n, d, w_2). Hence

$$A(n, d, w_2) \ge A(n, d, w_1)\Pi.$$

The result follows upon passing to the limit on n. ■

D. *The hard half plane* $\omega \ge 1/2$

Theorem 3: For any $\delta \in [0, 1]$ and $\omega \in (1/2, 1]$,

$$b(\delta, \omega) = a(\delta, \omega).$$

To prepare for the proof we require the following Lemma.

Lemma 1: For any $\delta \in [0, 1]$ and $\omega \in [0, 1]$

$$b(\delta, \omega) = \sup\{a(\delta, \rho),\ \omega \le \rho \le 1\}.$$

Proof of Lemma 1: We have

$$\begin{aligned}\max_{j\in\{w,w+1,\dots,n\}} A(n, d, j) &\le B(n, d, w)\\ &\le (n - w + 1) \max_{j\in\{w,w+1,\dots,n\}} A(n, d, j)\end{aligned}$$

by (1) for the first inequality and by (3) for the second inequality. The lemma then follows, after some algebra. ■

Proof of Theorem 3: The RHS of Lemma 1 is evaluated by the unimodality property, Theorem 2. ■

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

The semidefinite programming (SDP for short) 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 refer to [2] for a survey on 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, $L(n, d, w)$ is the independence number of a certain graph with vertex set H_n, thus is upper bounded by the 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 [18], under the name of block diagonalization of the Terwilliger algebra of the Hamming space, and in the framework of group representations in [20]. Numerical upper bounds for $L(n,d,w)$ obtained in this way are displayed in Tables IV, V, VI.

It is worth to point out the analogy between the case of codes in Hamming balls under consideration, and that of codes in spherical caps, studied in [4]. In the latter, the SDP method has lead to numerical bounds and also to explicit bounds of degree up to two. We propose in the remaining to follow the same line for Hamming balls. The bound of degree 1 obtained in this way is exactly the Elias/Johnson bound, while a new bound is obtained from degree 2 functions (Theorem 4.5).

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 $\mathrm{Aut}(H_n)$ 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 $u := wt(x)$, $v := wt(y)$ 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: $(x,y) \mapsto F(wt(x), wt(y), d(x,y)) \succeq 0$.

Theorem 4.1: 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 $F(x,y) := P(wt(x), wt(y), d(x,y))$. 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 (3) insures that $S_2\le 0$ and condition (4) 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 [18], and in [20] 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. 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 4.2: For all $P \in \mathbb{R}[u,v,t]$, symmetric in (u,v), $P \succeq 0$ if and only if

$$P(u,v,t) = \sum_{k=0}^{\lfloor n/2 \rfloor} \langle F_k, E_k(x,y)\rangle \tag{6}$$

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 (ie 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 $X = X_0 \cup \dots \cup X_n$, with $X_k = \{x \in H_n : wt(x) = k\}$, which leads to a decomposition of the functional space $\mathcal{C}(X) = \mathcal{C}(X_0) \perp \dots \perp \mathcal{C}(X_n)$ and then decompose each S_n-space $\mathcal{C}(X_k)$, following [12]. It is the method adopted in [20] 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 $\mathcal{C}(H_n) = P_0 \perp P_1 \perp \dots \perp P_n$ where $P_k = \oplus_{wt(w)=k} \mathbb{C}\chi_w$, $\chi_w(x) = (-1)^{w \cdot x}$, 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 $x \mapsto F(x,y) := P(wt(x), wt(y), d(x,y))$ belongs to $P_0 \perp \dots \perp P_k$ 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:

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

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

$$P_k = H_{0,k} \perp H_{1,k} \perp \dots \perp H_{k,k} \tag{7}$$

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

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

Since $u = wt(x)$, 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 4.3: 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 $wt(w) = 1$, 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 $wt(w') = wt(w) - 1$, 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 (7) 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:

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

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

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

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 4.4: 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 4.1 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

$$L(n,d,w) \leq \frac{d}{d-2w(1-w/n)}. \tag{8}$$

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 4.1, is equivalent to $F_0 - f_0 E_0 \succeq 0$. In order to fulfil 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 (8). 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

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

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	**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

This last value is positive if and only if

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

Alltogether we obtain:

Theorem 4.5: Assume $w \leq (n+1)/2$ and

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

Then

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

Example: with the above we obtain $b(n, n/2, n/2) \leq 2n-1$. 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 $b(n, n/2, n/2) = 2n-1$.

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

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

B. Tables

The tables IV, V and VI give upper bounds of $L(n,d,w)$ employing the SDP method. They improve on that of Section II and in some cases 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 [15]

The weight enumerator of the $RM(2,4)$ dual of the $RM(1,4)$ is computed by MacWilliams transform [15, 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

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

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

This shows by expurgation

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

The weight enumerator of the extended Golay code is

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

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 4: 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 $d \leq nh^{-1}(1/2)$,[1] we have

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

Proof: Pick a self dual code above the Gilbert bound [16]. 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

The following result sharpens, in certain cases, Proposition 4. We assume that the reader has some familiarity with the covering radius concept [10]. Define $R(n,d)$ the largest covering radius of a code achieving $A(n,d)$. Trivially $R(n,d) \geq \lfloor (d-1)/2 \rfloor$. A direct consequence of the sphere covering bound gives a sharper bound.

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

Proposition 5: 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 below the covering radius of C. This gives $B(n,d,w) \geq A(n,d)$. The reverse inequality is (4). ■

C. Concatenation

Consider a binary code of length n, size 2^m, minimum weight w, and distance d. If we concatenate this code with a code of length N, minimum weight W, and minimum distance D over $GF(2^m)$, we get a binary code of length $N2^m$, weight at least wW, and minimum distance dD. Hence

$$B(Nn, dD, wW) \geq B_{2^m}(N, D, W)\,.$$

where $B_q(\cdot,\cdot,\cdot)$ is the natural generalization of $B(\cdot,\cdot,\cdot)$ to an alphabet of size q.

Efficient decoding algorithms for concatenated codes can be found in [12].

VI. Perspective and open problems

In the present paper we have considered the notion of codes with weight bounded either from below (heavy weight codes) or from above (light weight codes). This led us to the definition of two combinatorial functions $B(n,d,w)$ and $L(n,d,w)$. The two problems are equivalent from the combinatorial standpoint, although the motivation is different.The asymptotic exponent attached to $B(n,d,w)$ is reduced to that of either $A(n,d)$ or $A(n,d,w)$, two very old and hard problems. On the other hand, for finite values of the parameters, it might be possible to find new exact values of $B(n,d,w)$ or $L(n,d,w)$ by special constructions. Investigating the new function $R(n,d)$, for instance, might be worth pursuing.

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

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] P. Delsarte, *Hahn polynomials, discrete harmonics and t-designs*, SIAM J. Appl. Math. **34**-1 (1978)

[12] 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.

[13] V. Guruswami, M; Sudan, Extensions to the Johnson bound, available from `http://www.cs.cmu.edu/ venkatg/pubs/pubs.html`

[14] W. Cary Huffman, Vera Pless *Fundamentals of error correcting codes*, Cambridge (2003).

[15] MacWilliams, F. J.; Sloane, N. J. A, *The theory of Error Correcting Codes*, North Holland (1977).

[16] MacWilliams, F. J.; Sloane, N. J. A.; Thompson, J. G. Good self dual codes exist. Discrete Math. 3 (1972), 153–162.

[17] 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.

[18] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Trans. Inform. Theory IT-51 (2005), 2859–2866.

[19] Tchamkerten, Aslan; Chandar, Venkat; Wornell, Gregory, Communication under strong asynchronism, IEEE Trans. Information Theory, IT-55 (2010), no. 10, 4508-4528.

[20] F. Vallentin, *Symmetry in semidefinite programs*, Linear Algebra and Appl. 430 (2009), 360-369.