DIMACS Technical Report 98-53
December 1998

New upper bounds on generalized weights

by

A.Ashikhmin
Los Alamos National Laboratory
Group CIC-3
Mail Stop P990
Los Alamos, NM 87545
alexei@c3serve.c3.lanl.gov.

A. Barg [1]
Bell Labs, Lucent Technologies
600 Mountain avenue 2C-375
Murray Hill, NJ 07974-0636
abarg@research.bell-labs.com

S. Litsyn [2]
Department of Electrical Engineering–Systems
Tel Aviv University
Ramat Aviv 69978
Israel
litsyn@eng.tau.ac.il.

[1]Permanent Member
[2]Research done while visiting DIMACS

DIMACS is a partnership of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, Bellcore and NEC Research Institute.

DIMACS is an NSF Science and Technology Center, funded under contract STC–91–19999; and also receives support from the New Jersey Commission on Science and Technology.

ABSTRACT

We derive new asymptotic upper bounds on the generalized weights of a binary linear code of a given size. We also prove some asymptotic results on the distance distribution of binary codes.

1 Introduction

Let C be a linear binary code of length n and rate $R(C) = \log_2 |C|/n$. The *support* of a subset $\mathcal{C} \subset C$ is defined as

$$\mathsf{supp}\,\mathcal{C} = \bigcup_{\mathbf{c}\in\mathcal{C}} \mathsf{supp}\,(\mathbf{c}),$$

where $\mathsf{supp}\,(\mathbf{c}) = \big\{e \in \{1, 2, \dots, n\} \,:\, c_e = 1\big\}$.

Definition 1 *Let*

$$d_r(C) = \min |\mathsf{supp}\,\mathcal{C}|,$$

where the minimum is taken over all linear subcodes $\mathcal{C}$ of C of dimension r. The number $d_r(C)$ is called the rth (generalized) weight of C.

Generalized weights were first studied in [9], [11]. They received much publicity in the 90-ies following the appearance of [19]. Knowing generalized weights is of importance in the analysis of cryptographic resistance of codes in the wire-tap channel, estimation of trellis complexity, design of codes for the switching multiple-access channel, etc. A summary of a large part of known results related to calculating generalized weights of specific codes, geometric connections, and bounds was given in [17].

The subject of this paper is the following problem: given the parameters $[n, k]$, establish the maximal possible value of the rth weight of an $[n, k]$ linear code. Here $r \geqslant 2$ is a given constant. A number of bounds on $d_r = d_r(n, k)$ are known in the literature. Analogs of the Gilbert-Varshamov, Singleton, and Griesmer bounds were proved in [19]. Another lower bound was given in [8]. Upper bounds analogous to the classical Plotkin, Hamming, and Bassalygo-Elias bounds were proved in [5],[6]. A generalization of Definition 1 to the case of unrestricted codes and lower and upper bounds on generalized weights were given in [4]. A particular case of codes over rings was studied in [1]. A detailed summary of recent studies is given in [17].

In this paper we are primarily interested in the asymptotic upper bounds on d_r. More formally, we shall study bounds on the function

$$\delta_r(R) = \limsup_{n\to\infty} \frac{d_r(C)}{n}$$

where the limit is calculated over all sequences of codes C of growing length n and rate at least R. We shall also be interested in the behavior of the inverse function

$$R_r(\delta) = \limsup_{n\to\infty} R(C),$$

where the limit is calculated over all sequences of codes C of growing length n and relative r-th weight $d_r(C)/n$ at least δ.

Let us quote the best known bounds on $\delta_r(R)$ and $R_r(\delta)$. Below

$$H_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x)$$

is the entropy function and $H_q^{-1}(\cdot)$ is its inverse. Thus $H_q : [0,1] \to [0,1]$ and $H_q^{-1} : [0,1] \to [0, \frac{q-1}{q}]$. Further, let $\lambda_q(R) = H_q^{-1}(1-R)$. If $q=2$, we omit the subscript and write simply $H(\cdot), H^{-1}(\cdot), \lambda(\cdot)$. A lower existence bound (the "Gilbert-Varshamov" bound) follows from a result in [19]. It is the best known asymptotic lower bound on δ_r and R_r.

Theorem 2 [19] *For* $0 \leqslant R \leqslant 1$, $0 \leqslant \delta \leqslant \frac{2^r-1}{2^r}$,

$$\begin{aligned} \delta_r(R) &\geqslant \delta_r^{gv}(R) = \lambda_{2^r}(R), &(1)\\ R_r(\delta) &\geqslant R_r^{gv}(\delta) = 1 - H_{2^r}(\delta). &(2) \end{aligned}$$

Other proofs of this theorem are given in [7], [8], [17]. The following bound (the "Elias," or "Bassalygo-Elias," bound) was proved in [5] for $r=2$ and in [6] for the general case.

Theorem 3 [5], [6] *For* $0 \leqslant R \leqslant 1$, $0 \leqslant \delta \leqslant \frac{2^r-1}{2^r}$,

$$\begin{aligned} \delta_r(R) &\leqslant \delta_r^{el}(R) = 1 - \lambda(R)^{r+1} - (1-\lambda(R))^{r+1}, &(3)\\ R_r(\delta) &\leqslant R_r^{el}(\delta) = 1 - H(\rho), &(4) \end{aligned}$$

where ρ *is the smallest root of*

$$x^{r+1} + (1-x)^{r+1} = 1 - \delta.$$

This bound can be improved in a certain range of rates; see [18]. In particular, the following theorem holds true.

Theorem 4 [18] *For* $0 \leqslant R \leqslant 1$,

$$\delta_r(R) \leqslant \min_{1 \leqslant s \leqslant r-1} \left(\delta_s^{up}(R) + (1 - \delta_s^{up}(R)) \delta_{r-s}^{up} \Big(\frac{R}{1 - \delta_s^{up}(R)} \Big) \right), \tag{5}$$

where $\delta_s^{up}(R)$ *and* $\delta_{r-s}^{up}(R)$ *are any asymptotic upper bounds on* $\delta_s(R)$ *and* $\delta_{r-s}(R)$, *respectively.*

Then taking $r=2$, one can put $s=1$ and use the McEliece-Rodemich-Rumsey-Welch bound [14], which we quote in the following theorem.

Theorem 5 [14] *For* $0 \leqslant R \leqslant 1$, $0 \leqslant \delta \leqslant 1/2$,

$$\delta_1(R) \leqslant \delta_1^{lp}(R) = \min_{\substack{0 \leqslant \beta \leqslant \alpha \leqslant 1/2 \\ H(\alpha) - H(\beta) = 1 - R}} 2 \frac{\alpha(1-\alpha) - \beta(1-\beta)}{1 + 2\sqrt{\beta(1-\beta)}} \tag{6}$$

$$R_1(\delta) \leqslant R_1^{lp}(\delta) = \min_{0 \leqslant \alpha \leqslant 1/2} 1 - H(\alpha) + H\left(\frac{1}{2} \left(1 - \sqrt{1 - (\sqrt{4\alpha(1-\alpha) - \delta(2-\delta)} - \delta)^2} \right) \right) \tag{7}$$

Then we obtain the following upper bound [18]:

$$\delta_2(R) \leqslant \delta_2^{vl}(R) = \delta_1^{lp}(R) + (1 - \delta_1^{lp}(R))\delta_1^{lp}\left(\frac{R}{1 - \delta_1^{lp}(R)}\right) \tag{8}$$

Bound $\delta_2^{vl}(R)$ is better than the Elias bound (3)

$$\delta_2^{el}(R) = 3\lambda(R)(1 - \lambda(R)), \tag{9}$$

for code rates $R \in (0, 0.52]$. For larger R one can use recursion (5), relying on the upper bounds on $\delta_s(R)$, $s < r$, already obtained. This improves the Elias bound for (low) code rates in a certain range.

The main results of this paper are two bounds on the size of binary codes with given generalized weights. The first bound (see Proposition 17) improves both (9) and (8) for all $R \in (0, 1)$. The second bound (Theorem 20) holds for any r and improves the Elias bound (3). The principal technical tool of obtaining the new bound is an application of Delsarte's linear programming method to deriving lower bounds on code invariants, found recently in [13], [2]. In particular, in [13] it is proved that in every code of rate $R > 0$ and sufficiently large length n, there necessarily exists an exponentially large component of the weight distribution. This theorem, made more precise in Section 3, is then used together with bounds on the size of constant weight codes [12], [15] (see Section 2) to prove the existence of two codewords of the same weight having a support of size bounded from above. This provides a new bound on $\delta_2(R)$. Note that a similar line of thought was adopted in [10] for estimating the 2nd weight of binary BCH codes. Once we have a new upper bound on $\delta_2(R)$, we can proceed using (5) as described above and improve upper bounds on $\delta_r(R), r \geqslant 3$. For the second result, we use the lower bound on the weight enumerator in a certain averaging argument.

En route we prove some asymptotic results on the distance distribution of binary codes that meet the MRRW bound (6)-(7) (assuming that such exist), which appear to be of independent interest. This is the subject of Section 3.

Remark. Research Problem 4.2 in [17] suggests to generalize the asymptotic upper bound (6)-(7) on $\delta_1(R)$ to the case $r \geqslant 2$. A few attempts known in the literature [3], [16] did not lead to a successful result. It would seem that our Theorem 15 is a reasonable generalization for the case $r = 2$.

2 Bounds on constant weight codes

We need asymptotic upper bounds on the minimum distance of constant weight codes of a given size. Let C be a binary constant weight code of length n and weight αn, rate $R(C)$, and distance $d(C) = d(Rn, \alpha n)$. As above, let

$$\begin{aligned}\delta(R, \alpha) &= \limsup_{n\to\infty} \frac{d(Rn, \alpha n)}{n},\\ R(\delta, \alpha) &= \limsup_{n\to\infty} R(C).\end{aligned}$$

We start with the linear programming bound of McEliece et al.

Theorem 6 [14] *For* $0 \leqslant R \leqslant H(\alpha)$, $0 \leqslant \delta \leqslant 2\alpha(1-\alpha)$,

$$\begin{aligned} \delta(R,\alpha) &\leqslant \delta^{lp}(R,\alpha) = 2\frac{\alpha(1-\alpha) - H^{-1}(R)(1-H^{-1}(R))}{1+2\sqrt{H^{-1}(R)(1-H^{-1}(R))}}, && (10)\\ R(\delta,\alpha) &\leqslant R^{lp}(\delta,\alpha) = H\left(\frac{1}{2}\left(1-\sqrt{1-(\sqrt{4\alpha(1-\alpha)-\delta(2-\delta)}-\delta)^2}\right)\right). && (11) \end{aligned}$$

Comparing (11) with Theorem 5 we see that

$$R_1^{lp}(\delta) = \min_{0 \leqslant \alpha \leqslant 1/2} 1 - H(\alpha) + R^{lp}(\delta,\alpha). \tag{12}$$

Denote by $\alpha_{1,m}(\delta)$ the value of α that furnishes the minimum to the right-hand side of (12). Likewise, let $\alpha_{2,m}(R)$ be the value of α that furnishes the minimum to the right-hand side of (6) (note that β in (6) is a dummy variable whose value is determined uniquely given α and R).

Proposition 7

$$\begin{aligned} \alpha_{1,m}(\delta) &= \alpha_{2,m}(R_1^{lp}(\delta)),\\ \alpha_{1,m}(\delta_1^{lp}(R)) &= \alpha_{2,m}(R). \end{aligned}$$

PROOF. Direct substitution. ∎

The linear programming bound for constant weight codes can be improved by using a recurrence relation suggested in [12]. We give it here in the asymptotic form.

Theorem 8 [12] *For* $0 \leqslant \delta \leqslant 2\alpha(1-\alpha)$,

$$R(\delta,\alpha) \leqslant \min_{\substack{0 \leqslant \nu-\xi \leqslant 2(1-\alpha)\\ 0 \leqslant \nu+\xi \leqslant 2\alpha}} \Big(H(\alpha-\xi) - \alpha H\left(\frac{\nu+\xi}{2\alpha}\right) - (1-\alpha)H\left(\frac{\nu-\xi}{2(1-\alpha)}\right) + R^{up}(\delta,\nu)\Big), \tag{13}$$

where $R^{up}(\delta,\nu)$ *is any upper bound on* $R(\delta,\nu)$.

This bound combined with (10) gives the best bound for constant weight codes currently known. Interestingly, in a certain interval of values of α one can determine the optimal parameters of the recursion and arrive at a simpler expression.

The following proposition can be derived from Theorem 8, see [12].

Proposition 9 *For any* $0 \leqslant \delta \leqslant 1/2$, *the function* $R(\delta,\alpha) + 1 - H(\alpha)$ *is nonincreasing on* α *for* $\alpha \in [\frac{1-\sqrt{1-2\delta}}{2}, \frac{1}{2}]$.

A simple consequence of this fact, observed in [15], gives a closed from of (13) under certain restrictions.

Theorem 10 *For any $\alpha_{1,m}(\delta) \leqslant \alpha \leqslant 1/2$ we have*

$$R(\delta,\alpha) \leqslant R^{sm}(\delta,\alpha) = R_1^{lp}(\delta) + H(\alpha) - 1.$$

PROOF. We have

$$\begin{aligned} R(\delta,\alpha) &\overset{\text{(a)}}{\leqslant} R(\delta,\alpha_{1,m}(\delta)) + H(\alpha) - H(\alpha_{1,m}(\delta)) \\ &\overset{\text{(b)}}{\leqslant} R^{lp}(\delta,\alpha_{1,m}(\delta)) + H(\alpha) - H(\alpha_{1,m}(\delta)) \\ &\leqslant R^{lp}(\delta,\alpha_{1,m}(\delta)) + 1 - H(\alpha_{1,m}(\delta)) + H(\alpha) - 1 \\ &\overset{\text{(c)}}{=} R_1^{lp}(\delta) + H(\alpha) - 1. \end{aligned}$$

Here inequality (a) follows from Proposition 9, inequality (b) is implied by (11), and (c) follows from (12). ∎

Corollary 11 *If $\alpha_{2,m}(R) \leqslant \alpha \leqslant 1/2$, then*

$$\delta(R,\alpha) \leqslant \delta^{sm}(R,\alpha) = \delta_1^{lp}(1 + R - H(\alpha)). \tag{14}$$

PROOF. Follows from Proposition 7. ∎

It is easy to see that when bound (14) is applicable, it is better than the linear programming bound (10).

3 Bounds on spectra of codes

The second ingredient that we need in order to prove the main theorem is a lower bound on the components of the weight distribution of a code. Let A_i, $i = 0, 1, \ldots, n$, denote the number of codewords of Hamming weight i in the code.

The following result is from [13].

Theorem 12 [13] *For every code of rate R and sufficiently large length n there exists a number ξ,*

$$\xi \in \left(0, 2\frac{\alpha(1-\alpha) - \beta(1-\beta)}{1 + 2\sqrt{\beta(1-\beta)}}\right], \tag{15}$$

such that

$$\frac{1}{n}\log_2 A_{\xi n} \geqslant R - 1 + H(\beta) + 2H(\alpha) - 2q(\alpha,\beta,\xi/2) - \xi - (1-\xi)H\left(\frac{\alpha - \xi/2}{1-\xi}\right),$$

where α and β are arbitrary numbers satisfying

$$0 \leqslant \beta \leqslant \alpha \leqslant 1/2, \quad H(\alpha) - H(\beta) \geqslant 1 - R, \tag{16}$$

and

$$q(\alpha,\beta,\gamma) = H(\beta) + \int_0^\gamma \log_2\Big(\frac{\alpha(1-\alpha)-y(1-2y)-\beta(1-\beta)}{2(\alpha-y)(1-\alpha-y)} + \frac{\sqrt{(\alpha(1-\alpha)-y(1-2y)-\beta(1-\beta))^2-4(\alpha-y)(1-\alpha-y)y^2}}{2(\alpha-y)(1-\alpha-y)}\Big)dy. \quad (17)$$

Choosing α and β so that ξ be restricted to the shortest possible interval, one can prove [13] that there exists an exponentially large component of the weight distribution for $\xi \in [0, \delta^{lp}(R)]$. Moreover, comparing this component to the "binomial"weight distribution

$$\hat{A}_i = \frac{\binom{n}{i}|C|}{2^n},$$

i.e., the weight distribution of a typical long code, one can check that this theorem implies the following corollary.

Corollary 13 [13] *For every code of sufficiently large length n and rate R, and any $\eta \geqslant \delta_1^{lp}(R)$, there exists a ξ,*

$$\xi \in (0, \eta]\,,$$

such that

$$\frac{1}{n}\log_2 A_{\xi n} \geqslant \max(0, H(\xi)+R-1),$$

where the equality is achieved only if $\xi = \eta$.

Let us analyse some consequences of Theorem 10. Let R_0 be the solution of

$$\alpha_{2,m}(R) = \delta_1^{lp}(R),$$

or $R_0 = 0.421\ldots$.

Theorem 14 *Suppose a code of rate $R_0 \leqslant R \leqslant 1$, and sufficiently large length n meets the linear programming bound (6), i.e., is of relative distance $\delta_1^{lp}(R)$. Then for $\delta_1^{lp}(R) \leqslant \xi \leqslant 1-\delta_1^{lp}(R)$,*

$$\frac{1}{n}\log_2 A_{\xi n} \quad \leqslant \quad H(\xi)+R-1. \quad (18)$$

Moreover, every subinterval of the interval $[\delta_1^{lp}(R), 1/2]$ of length $(\mathrm{const})\cdot n^{\frac{1}{2}+\epsilon}$, $\epsilon > 0$, *contains a component of the weight distribution such that*

$$\frac{1}{n}\log_2 A_{\xi n} \quad = \quad H(\xi)+R-1. \quad (19)$$

Proof. By Theorem 10, if $\xi > \alpha_{1,m}(\delta_1^{lp}(R)) = \alpha_{2,m}(R)$,

$$R(\delta_1^{lp}(R),\xi) \leqslant R_1^{lp}(\delta_1^{lp}(R)) + H(\xi) - 1 = R + H(\xi) - 1. \quad (20)$$

The inequality on R follows by solving $\alpha_{2,m}(R) \leqslant \delta_1^{lp}(R)$ with respect to R. The second claim for every $\eta \geqslant \delta_1^{lp}(R)$ follows from Corollary 13 and Theorem 14 (technical details are omitted). ∎

4 New bounds on generalized weights, I

Now we are in a position to formulate the main theorem.

Theorem 15 *For* $0 \leqslant R \leqslant 1$,

$$\delta_2(R) \leqslant \min_{\substack{0\leqslant\beta\leqslant\alpha\leqslant 1/2\\ H(\alpha)-H(\beta)\geqslant 1-R}} \max_{0<\xi\leqslant 2\frac{\alpha(1-\alpha)-\beta(1-\beta)}{1+2\sqrt{\beta(1-\beta)}}} \left(\xi + \frac{\delta^{up}(R',\xi)}{2}\right) \tag{21}$$

where $\delta^{up}(R,\xi)$ *is any upper bound on* $\delta(R,\xi)$,

$$R' = R - 1 + H(\beta) + 2H(\alpha) - 2q(\alpha,\beta,\xi/2) - \xi - (1-\xi)H\left(\frac{\alpha-\xi/2}{1-\xi}\right), \tag{22}$$

and $q(\alpha,\beta,\gamma)$ *is defined in* (17).

Proof. By Theorem 12, for any α,β satisfying (16) and ξ as in (15), there exists a constant weight code $\mathcal{D}(\xi)$ of size $A_{\xi n} \geqslant R'$ and weight ξn. Then $\mathcal{D}(\xi)$ contains a pair of codewords x, y at a distance at most $\delta^{up}(R',\xi)n$ apart. The size of the support of $(x, y, x+y)$ equals

$$|\mathsf{supp}\,(x,y)| = 2\xi n - |x \cap y| = \xi n + \frac{\mathsf{dist}\,(x,y)}{2}.$$

This completes the proof. ∎

Now we can use bounds (10) and (14) in (21) to obtain more explicit bounds on $\delta_2(R)$.

First, let us apply (14). We obtain the following surprising result. Here R_0 is as defined before Theorem 14.

Corollary 16 *For* $R_0 \leqslant R < 1$,

$$\delta_2(R) \leqslant \frac{3}{2}\delta_1^{lp}(R). \tag{23}$$

Proof. We can take any α,β satisfying (16). Let $\alpha = \alpha_{2,m}(R)$, $\beta = H^{-1}(H(\alpha_{2,m}(R)) - 1 + R)$. Computations with Mathematica show that for all rates $0 < R < 1$, the right-hand side of (21) is a growing function of ξ. Therefore, let

$$\xi = 2\frac{\alpha(1-\alpha)-\beta(1-\beta)}{1+2\sqrt{\beta(1-\beta)}}.$$

Then by (6) we have $\xi = \delta_1^{lp}(R)$. Further, for this choice of α,β,ξ, expression (22) takes on the form

$$R' = H(\delta_1^{lp}(R)) - R + 1$$

(see [13]; this is proved similarly to the way Corollary 13 is derived from Theorem 12). Now we can rewrite (21) using (14) as follows:

$$\delta_2(R) \leqslant \delta_1^{lp}(R) + \frac{1}{2}\delta^{sm}(R', \delta_1^{lp}(R)) = \delta_1^{lp}(R) + \frac{1}{2}\delta_1^{lp}(1 + R' - H(\delta_1^{lp}(R)))$$
$$= \frac{3}{2}\delta_1^{lp}(R).$$

∎

For code rates $0 < R < R_0$ inequality (14) is not applicable. So we have to stick with the bound (21), where for δ^{up} we take the best upper bound available, i.e., (10). Upon choosing α, β, ξ the same as in the above corollary, we get the bound on $\delta_2(R)$ for low rates. Thus, the new bound on $\delta_2(R)$ that we derive, is combined of two pieces as follows.

Proposition 17

$$\delta_2(R) \leqslant \delta_2^*(R) = \begin{cases} \delta_1^{lp}(R) + \frac{1}{2}\delta^{lp}(R - 1 + H(\delta_1^{lp}(R)), \delta_1^{lp}(R), & 0 \leqslant R < R_0 \\ \frac{3}{2}\delta_1^{lp}(R), & R_0 \leqslant R \leqslant 1, \end{cases} \tag{24}$$

where $\delta_1^{lp}(R)$ *and* $\delta^{lp}(R, \alpha)$ *are given by* (6) *and* (10), *respectively.*

Bound (24) is better than the previously known bounds. For reference purposes we tabulate δ_2^* (24), the Elias bound δ_2^{el} (9), the Vlăduţ bound δ_2^{vl} (8), and the lower Gilbert-Varshamov bound δ_2^{gv} (2).

bound R	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
δ_2^* (24)	0.5831	0.4917	0.4140	0.3425	0.2737	0.2078	0.1456	0.0884	0.0381
δ_2^{el} (9)	0.6484	0.5518	0.4604	0.3743	0.2938	0.2192	0.1512	0.0905	0.0385
δ_2^{vl} (8)	0.5996	0.5129	0.4362	0.3628	0.2917	0.2234	0.1585	0.0979	0.0433
δ_2^{gv} (2)	0.5047	0.3977	0.3157	0.2476	0.1893	0.1385	0.0943	0.0560	0.0238

To visualize these results, in Fig. 1 we plot bounds (24), (9), (8), (2).

Since the bound in Proposition 17 is better than the bounds previously known, its application in (5) improves known bounds on generalized weight of order r greater than 2. Let us illustrate this for $r = 3$. Computing the bounds in (5) shows that the minimum is attained for $s = 1$. This gives the following bound:

$$\delta_3(R) \leqslant \delta_3^*(R) = \delta_1(R) + (1 - \delta_1(R))\delta_2^*\left(\frac{R}{1 - \delta_1(R)}\right), \tag{25}$$

where $\delta_1(R)$ is given in (6) and $\delta_2^*(R)$ in (24). Bound $\delta_3^*(R)$ is better than the Elias bound (3) for $0 < R \leqslant 0.84$ and fails to improve it for larger rates (see the table in the next section).

5 New bounds on generalized weights, II

In this section we present another way of using Theorem 12 to derive bounds on generalized weights. We begin with two auxiliary lemmas.

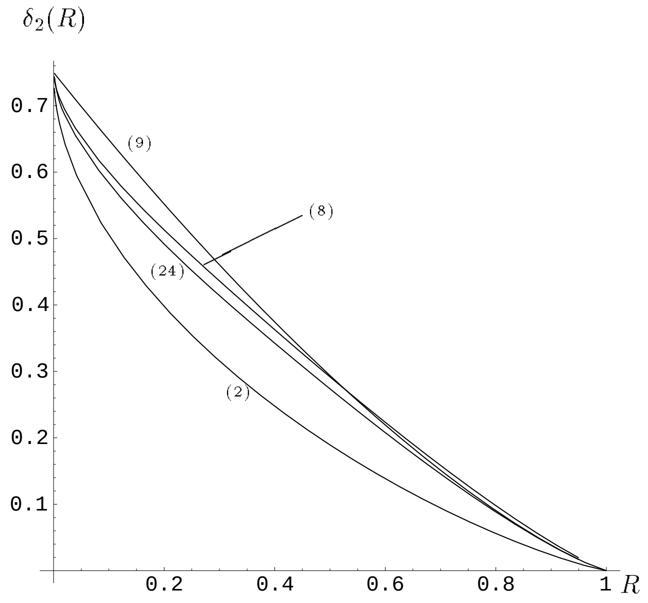

Figure 1: Bounds on the 2nd weight of a code of rate R

Lemma 18 *Let W be a constant weight code of length n and weight w. If $0 \leqslant w_1 \leqslant w$, and*

$$\frac{|W| \sum_{i=w_1}^{\min(\ell,w)} \binom{w}{i}\binom{n-w}{\ell-i}}{\binom{n}{\ell}} \geqslant M, \quad 1 \leqslant M \leqslant |W|,$$

then there exist ℓ positions such that at least M codewords of W have weight at least w_1 on them.

Proof. We will find the average weight of subwords of the code over all possible choices of ℓ positions. Let $L \subset \{1, 2, \dots, n\}$, $|L| = \ell$. For a codeword $\mathbf{c} \in W$, define the indicator $\chi_L(\mathbf{c})$ by letting $\chi_L(\mathbf{c}) = 1$ if the total number of 1's in the positions L of $\mathbf{c}$ is at least w_1. We have

$$X = \sum_{\mathbf{c}\in W} \sum_{|L|=\ell} \chi(\mathbf{c}) = |W| \sum_{i=w_1}^{\min(\ell,w)} \binom{w}{i}\binom{n-w}{\ell-i}.$$

Hence there exists a choice of L such that the number of "good" codewords is at least $X/\binom{n}{\ell}$, giving the claim. ∎

Below we use the statement of this lemma to derive an asymptotic bound. Let us choose M so that if $n \to \infty$,

$$M \to \infty,\ \log_2 M \to \infty,\ \log_2 M = o(n).$$

Out of the M nonzero codewords whose existence is guaranteed by this lemma, there are at least $\lfloor \log_2 M \rfloor + 1$ linearly independent (indeed, $\lfloor \log_2 M \rfloor$ codewords account for at most

$2^{\lfloor \log_2 M \rfloor} - 1$ different nontrivial linear combinations). Denote this subset of codewords by $\mathcal{W}$.

The second auxiliary result that we use is a standard double ("row-column") counting argument for the average support of r given vectors of a code $\mathcal{D}$ (here we do not assume linearity). In the matrix with codewords of $\mathcal{D}$ as rows let u_i be the number of ones in the ith column.

Lemma 19 *Let $\mathcal{D}$ be a code of length n and size D. Then*

$$\min \mathsf{supp}\,(\mathbf{c}_1, \ldots, \mathbf{c}_r) \leqslant \binom{D}{r}^{-1} \sum_{i=1}^{n} \left[\binom{D}{r} - \binom{D-u_i}{r} \right],$$

where the minimum is taken over all r-tuples of codewords of $\mathcal{D}$.

Proof. Let us count the cumulative support of all r-tuples. An r-tuple does not contribute to the support in the ith column if all the vectors in it have 0 in this column. Thus, the number of such choices is $\binom{D-u_i}{r}$. So we get

$$\binom{D}{r} \min \mathsf{supp}\,(\mathbf{c}_1, \ldots, \mathbf{c}_r) \leqslant \sum_{i=1}^{n} \left[\binom{D}{r} - \binom{D-u_i}{r} \right].$$

Hence the lemma. ∎

Now let us use the last two lemmas together with Theorem 12 to derive the main result of this section. Below $w = \xi n, w_1 = \omega n, \ell = \nu n$.

Theorem 20 *Let C be a binary code of rate R. Let*

$$R' = R'(\alpha, \beta, \xi) = R - 1 + H(\beta) + 2H(\alpha) - 2q(\alpha, \beta, \xi/2) - \xi - (1-\xi) H\left(\frac{\alpha - \xi/2}{1-\xi}\right),$$

where $q(\alpha, \beta, \gamma)$ is defined in (17)*. Then*

$$\delta_r(R) \leqslant \delta_r^{**}(R) = \min_{\alpha,\beta} \max_{\xi} \min_{0 \leqslant \omega \leqslant \xi} \left[\nu + (1-\nu)\Big(1 - \Big(1 - \frac{\xi - \omega}{1-\nu}\Big)^r\Big)\right]. \qquad (26)$$

where α, β, ξ satisfy (15)-(16) *and $\nu = \nu(R', \xi, \omega)$ is a solution of the equation*

$$R' + \xi H\left(\frac{\omega}{\xi}\right) + (1-\xi) H\left(\frac{\nu - \omega}{1-\xi}\right) - H(\nu) = 0,$$

such that $\omega \leqslant \nu$.

Proof. The proof consists of three steps: take a constant weight code W given by Theorem 12, apply Lemma 18 on it, and apply Lemma 19 on the code obtained by a restriction of W to $n - \ell$ coordinates.

We need to present r linearly independent codewords of C with support given by the right-hand side of (26). Theorem 12 guarantees that there is a subset of vectors of C at a distance w from a certain codeword $\mathbf{a} \in C$, or, upon shifting the entire space by $\mathbf{a}$, a code W of constant weight w. Further, there is a subset of W of size M that satisfies the weight restrictions of Lemma 18. By the remark after this lemma, there is a subset $\mathcal{W} \subset W$ of $\log_2 M$ linearly independent codewords that also satisfy these restrictions, i.e., are of weight w_1 on a certain subset of ℓ coordinates, $1 \leqslant \ell \leqslant n$. Consider the restriction of $\mathcal{W}$ to the remaining $n-\ell$ coordinates, denote this code by $\mathcal{D}$, and apply Lemma 19 on it. We have

$$\min_{(\mathbf{c}_1,\dots,\mathbf{c}_r)\in\mathcal{D}} \mathsf{supp}\,(\mathbf{c}_1,\dots,\mathbf{c}_r) \leqslant \binom{D}{r}^{-1} \sum_{i=1}^{n-\ell} \Big[\binom{D}{r} - \binom{D-u_i}{r}\Big],$$

where the notation is the same as in Lemma 19.

Rewrite the last inequality keeping only the main terms:

$$\min_{(\mathbf{c}_1,\dots,\mathbf{c}_r)\in\mathcal{D}} \mathsf{supp}\,(\mathbf{c}_1,\dots,\mathbf{c}_r) \leqslant \frac{1}{D^r}\sum_{i=1}^{n-\ell}[D^r-(D-u_i)^r] = (n-\ell)\Big(1-\frac{1}{D^r}\sum_{i=1}^{n-\ell}(D-u_i)^r\Big). \tag{27}$$

Recall that $\sum_{i=1}^{n-\ell} u_i = D(w-w_1)$. Summation terms in (27) are $\cup$-convex functions of u_i. Finally, the right-hand side of (27) is symmetric in u_i. Invoking Lagrange multipliers now implies that it attains maximum for $u_i = D(w-w_1)/(n-\ell)$, and that the maximum is strict. Hence we get

$$\min_{(\mathbf{c}_1,\dots,\mathbf{c}_r)\in\mathcal{D}} \mathsf{supp}\,(\mathbf{c}_1,\dots,\mathbf{c}_r) \leqslant (n-\ell)\Big[1-\Big(1-\frac{w-w_1}{n-\ell}\Big)^r\Big].$$

Thus, we have proved the existence of r linearly independent codewords of C with support at most

$$\ell + (n-\ell)\Big[1-\Big(1-\frac{w-w_1}{n-\ell}\Big)^r\Big].$$

This completes the proof. ∎

Bound (26) for $r=3$ is always better than the Elias bound and better than the bound in (25) for $0.74 \leqslant R \leqslant 1$. We give a short table of values of these bounds together with the GV lower bound.

bound $\quad R$	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
δ_3^{**} (26)	0.7394	0.6365	0.5399	0.4471	0.3574	0.2713	0.1907	0.1166	0.0504
δ_3^{el} (3)	0.7712	0.6681	0.5668	0.4679	0.3725	0.2816	0.1965	0.1188	0.0509
δ_3^{*} (25)	0.7076	0.6068	0.5165	0.4300	0.3463	0.2658	0.1892	0.1174	0.0839
δ_3^{gv} (2)	0.6207	0.4987	0.4018	0.3193	0.2470	0.1829	0.1260	0.0758	0.0328

We plot bounds δ_3^{gv}, δ_3^{el}, $\delta_3^*(R)$, and $\delta_3^{**}(R)$ in Fig. 2.

The following proposition gives the best bound on $\delta_3(R)$ currently known.

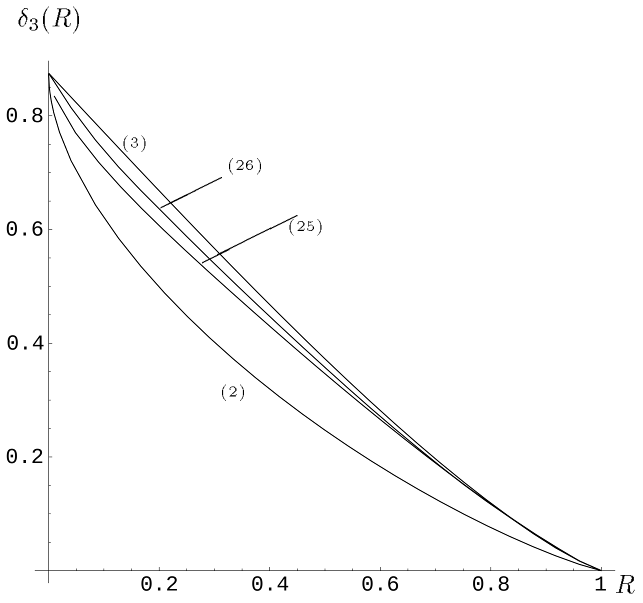

Figure 2: Bounds on the 3rd weight of a code of rate R

Proposition 21

$$\delta_3(R) \leqslant \min(\delta_3^*(R), \delta_3^{**}(R)),$$

where $\delta_3^*(R)$ *is given in* (25) *and* $\delta_3^{**}(R)$ *in* (26.)

Analytical difficulties have prevented us from comparing bounds (3), (26), and (5) in the general case. However, computations show that (26) is better than the Elias bound also for large r. Clearly, bound (26) is in general much easier to compute than (5).

References

[1] A. Ashikhmin, "On generalized Hamming weights for Galois ring linear codes," *Designs, Codes and Cryptography,* **14** (1998), 107–126.

[2] A. Ashikhmin and A. Barg, "Binomial moments of the distance distribution: Bounds and applications," *IEEE Trans. Inform. Theory,* to appear.

[3] A. Barg, "The matroid of supports of a linear code," *Appl. Alg. Engrg. Commun. Comput.,* **8** (2) (1997), 165-172.

[4] L.A. Bassalygo, "Supports of a code," in G. Cohen, M. Giustu, and T. Mora, Eds., *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes,* (AAECC-11), Lect. Notes Comput. Science, **948**, Springer-Verlag (1995), pp. 1–3.

[5] G. Cohen, L. Huguet, and G. Zémor, "Bounds on generalized weights," in G. Cohen et al., Eds., *Algebraic Coding. Proc. First French-Israeli Workshop*, Lect. Notes Comput. Science, Springer-Verlag **781**,(1994), pp. 270-277.

[6] G. Cohen, S. Litsyn, and G. Zémor, "Upper bounds on generalized distances," *IEEE Trans. Inform. Theory*, **40** (1994), 2090-2092.

[7] G. Cohen and G. Zémor, "Intersecting codes and independent families," *IEEE Trans. Inform. Theory*, **40** (6) (1994), 1872–1881.

[8] T. Helleseth, T. Kløve, V.I. Levenshtein, and Ø. Ytrehus, "Bounds on the minimum support weights," *IEEE Trans. Inform. Theory*, **41** (2) (1995), 432-440.

[9] T. Helleseth, T. Kløve, and J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$," *Discrete Mathematics*, **18** (1977), 179-211.

[10] G. Kabatianski, "On second generalized Hamming weight," in *Proc. Int. Workshop on Algebraic and Combinatorial Coding Theory* (Voneshta Voda, Bulgaria, June 22-28, 1992), pp. 98-100.

[11] T. Kløve, "The weight distribution of linear codes over $GF(q^l)$ having generator matrices over $GF(q)$," *Discrete Math.* **23** (1978), 159–168.

[12] V.I. Levenshtein, "Upper-bound estimates for fixed-weight codes," *Problemy Peredachi Informatsii*, **7**(4) (1971), 3–12, in Russian. English translation in *Probl. Inform. Trans.* **7** (1971), 281–287.

[13] S. Litsyn, "New bounds on error exponents," *IEEE Trans. Inform. Theory*, to appear.

[14] 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** (2) (1977), 157–166.

[15] A. Samorodnitsky, "On the optimum of Delsarte's linear program," *J. Combinatorial Theory, Ser. A*, to appear.

[16] J. Simonis, "The effective length of subcodes," *Appl. Alg. Engrg. Commun. Comput.*, **5** (1994), 371–377.

[17] M.A. Tsfasman and S.G. Vlăduţ, "Geometric approach to higher weights," *IEEE Trans. Inform. Theory*, **41** (1995), 1564–1588.

[18] S.G. Vlăduţ, "An upper bound for generalized Hamming weights," in R. Pellikaan and S.G. Vlăduţ, Eds., *Arithmetic, Geometry and Coding Theory*, (Luminy, 1993), Berlin: W. de Gruyter, (1996), 263–267.

[19] V. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, **37** (5) (1991), 1412–1418.