DIMACS Technical Report 98-41
August 1998

Strengthening the Varshamov-Gilbert bound

by

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

Sugi Guritman
Delft University of Technology
Faculty of Information Technology and Systems
P.O. Box 5031
2600 GA Delft, the Netherlands
S.Guritman@twi.tudelft.nl

Juriaan Simonis [2]
Delft University of Technology
Faculty of Information Technology and Systems
P.O. Box 5031
2600 GA Delft, the Netherlands
J.Simonis@twi.tudelft.nl

[1] Permanent Member
[2] Research done while visiting Bell Labs, Lucent Technologies, as a DIMACS visitor.

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

The paper discusses some ways to strengthen (nonasymptotically) the Gilbert-Varshamov bound for linear codes. The unifying idea is to study a certain graph constructed on vectors of low weight in the cosets of the code, which we call the Varshamov graph. Various simple estimates of the number of its connected components account for better lower bounds on the minimum distance of codes, some of them known in the literature.

1 Introduction

Let $\mathcal{C}$ be a q-ary linear code of length n, dimension k and minimum distance d, in short an $[n,k,d]_q$-code. The Varshamov bound [12] guarantees, for any given q,n,k, the existence of a linear $[n,k,d]_q$ code with a certain relation between the parameters n,k,d,q (see Prop. 10 below). Moreover, [12] suggests a greedy procedure of constructing a parity-check matrix for a code whose parameters meet the bound. Gilbert [5] suggested a similar greedy algorithm that produces (not necessarily linear) codes whose parameters satisfy a similar relation. Asymptotically, both bounds give the same function; therefore, it became common to join them into the "Varshamov–Gilbert bound."

To improve the Varshamov–Gilbert bound asymptotically is a notoriously difficult task [10]. However, for any small values of n,k,d,q, the best codes that we know are usually better than this bound. Therefore, the question whether better nonasymptotic bounds are possible seems to be a natural one. In Section 2 we introduce a graph on the standard array of the code and relate its parameters to those of the code. Simple estimates on the number of connected components of the graph lead to improvements of the Varshamov–Gilbert bound given in Proposition 9, Proposition 11 [6], Proposition 12, and Corollary 17 [4].

2 The Varshamov graph

Definition 1 *The code $\mathcal{C}$ is said to be* maximal *if it cannot be obtained by shortening an $[n+1,k+1,d]_q$-code.*

The following is a useful characterization of maximal codes.

Proposition 2 *The code $\mathcal{C}$ is maximal if and only if its covering radius does not exceed $d-2$.*

Proof. If $\mathbf{x} \in \mathbb{F}_q^n$ has distance $\geq d-1$ to $\mathcal{C}$, then the code $\mathcal{C}'$ spanned by $(\mathbf{x},1)$ and $\{(\mathbf{c},0) \mid \mathbf{c} \in \mathcal{C}\}$ has the parameters $[n+1,k+1,d]_q$, and shortening $\mathcal{C}'$ with respect to the last coordinate position gives $\mathcal{C}$. Conversely, if $\mathcal{C}$ is obtained by shortening an $[n+1,k+1,d]_q$-code $\mathcal{C}'$, then any word in $\mathcal{C}'$ which is nonzero in the shortening position yields a vector $\mathbf{x} \in \mathbb{F}_q^n$ at distance $\geq d-1$ from $\mathcal{C}$. ∎

Let $\mathcal{C}$ be an $[n,k,d]_q$-code.

Definition 3 *The undirected graph with the vertex set*

$$V_\alpha := \{\mathbf{x} \mid \mathbf{x} \in \mathbb{F}_q^n \text{ and } \mathsf{wt}(\mathbf{x}) \leq \alpha\}$$

and the edge set

$$E_\alpha := \{\{\mathbf{a},\mathbf{b}\} \mid \mathbf{a},\mathbf{b} \in V_\alpha \text{ and } \mathbf{a}-\mathbf{b} \in \mathcal{C} \setminus \{0\}\}$$

is denoted by $G_\alpha(\mathcal{C})$. The graph $G(\mathcal{C}) := G_{d-2}(\mathcal{C})$ is called the Varshamov graph *of $\mathcal{C}$.*

Obviously, the number of vertices in G_α is equal to

$$|V_\alpha| = \sum_{i=0}^{\alpha} (q-1)^i \binom{n}{i}.$$

The number of edges will turn out to be a function of the weight distribution $(A_i(\mathcal{C}))_{i=0,1,\ldots,n}$ of $\mathcal{C}$.

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ be any two vectors with $d(\mathbf{x}, \mathbf{y}) = w$. Then the integers

$$p_{i,j}^w := |\{\mathbf{z} \in \mathbb{F}_q^n \mid d(\mathbf{x}, \mathbf{z}) = i \text{ and } d(\mathbf{y}, \mathbf{z}) = j\}| \tag{1}$$

are known to be independent of the choice of $\mathbf{x}$ and $\mathbf{y}$. They are the so-called *intersection numbers* of the Hamming scheme $H(n, q)$. Sometimes the $p_{i,j}^w$ are also called the *linearization coefficients* of the Hamming scheme (cf. Remark 5). See [3], Chapter 21 of [8] or Chapter 30 of [7] for a detailed description of the Hamming scheme and other association schemes. Finally, the numbers $p_{i,j}^w$ arise naturally in estimating the error probability of bounded distance decoding on the q-ary symmetric channel [1].

In the sequel we need an explicit formula for the $p_{i,j}^w$.

Proposition 4 ([1])

$$p_{i,j}^w = \sum_{\delta=0}^{\lfloor \frac{i+j-w}{2} \rfloor} (q-2)^{i+j-w-2\delta} (q-1)^\delta \binom{w}{j-\delta} \binom{j-\delta}{w-i+\delta} \binom{n-w}{\delta}. \tag{2}$$

For $q = 2$, this reduces to

$$p_{i,j}^w = \begin{cases} 0 & \text{if } i+j-w \text{ is odd,} \\ \binom{w}{(w+i-j)/2} \binom{n-w}{(i+j-w)/2} & \text{if } i+j-w \text{ is even.} \end{cases}$$

Proof. In (1), we may assume that $\mathbf{x} = 0$ and $\mathsf{wt}(\mathbf{y}) = w$. So $p_{i,j}^w$ counts the number of $\mathbf{z}$ with $\mathsf{wt}(\mathbf{z}) = i$ and $\mathsf{wt}(\mathbf{z} - \mathbf{y}) = j$. Put

$$\begin{array}{rcl} \alpha & := & |\{u \mid z_u = y_u, z_u \neq 0\}|, \\ \beta & := & |\{u \mid z_u \neq y_u, z_u \neq 0, y_u \neq 0\}|, \\ \gamma & := & |\{u \mid z_u = 0, y_u \neq 0\}|, \\ \delta & := & |\{u \mid z_u \neq 0, y_u = 0\}|. \end{array}$$

Then

$$p_{i,j}^w = \sum (q-2)^\beta (q-1)^\delta \binom{w}{\alpha} \binom{w-\alpha}{\gamma} \binom{n-w}{\delta}, \tag{3}$$

where the sum is taken over all nonnegative integer solutions of the system

$$\left\{ \begin{array}{rcl} w & = & \alpha + \beta + \gamma \\ i & = & \alpha + \beta + \delta \\ j & = & \beta + \gamma + \delta \end{array} \right.$$

Solve for α, β and γ, and substitute in (3). ∎

Remark 5 *Another formula for* $p_{i,j}^w$ *is*

$$p_{i,j}^w = q^{-n} \sum_{u=0}^{n} K_i(u) K_j(u) K_u(w),$$

with

$$K_x(y) := \sum_{m=0}^{x} (-1)^m (q-1)^{x-m} \binom{y}{m} \binom{n-y}{x-m}.$$

The $K_x(y)$ *are polynomials of degree* x *in* y*, the so-called* Krawtchouk polynomials*. Again, we refer to the relevant sections of* [3], [8]*, and* [7]*.*

Proposition 6 *The size of the edge set* E_α *of* $G_\alpha(\mathcal{C})$ *is equal to*

$$\frac{1}{2} \sum_{w=d}^{2\alpha} A_w(\mathcal{C}) \sum_{i,j=0}^{\alpha} p_{i,j}^w.$$

A more explicit formula in the binary *case is*

$$|E_\alpha| = \frac{1}{2} \sum_{w=d}^{2\alpha} A_w(\mathcal{C} \sum_{v=0}^{2\alpha-w} \sum_{u=0}^{\lfloor v/2 \rfloor} \binom{w}{\alpha+u-v} \binom{n-w}{u}).$$

Proof. If $\mathbf{c} \in \mathcal{C}$ is a codeword of weight $w > 0$, then the set

$$X_{\mathbf{c}} := \{\{\mathbf{a}, \mathbf{b}\} \mid \mathbf{a}, \mathbf{b} \in V_\alpha \text{ and } \mathbf{a} - \mathbf{b} = \mathbf{c}\}$$

has size $\sum_{i,j=0}^{\alpha} p_{i,j}^w$ or $\frac{1}{2} \sum_{i,j=0}^{\alpha} p_{i,j}^w$, depending on whether q is odd or even. By definition, E_α is equal to

$$\bigcup_{\mathbf{c} \in \mathcal{C} \setminus \{\mathbf{o}\}} X_{\mathbf{c}}.$$

Now observe that $X_{\mathbf{c}} = X_{-\mathbf{c}}$ and that $X_{\mathbf{c}} \cap X_{\mathbf{c}'} = \emptyset$ if $\mathbf{c} \neq \pm \mathbf{c}'$. ■

The graph $G_\alpha(\mathcal{C})$ has a very simple structure: its components are complete graphs whose vertices are the intersections of V_α with the cosets of weight $\leq \alpha$ of $\mathcal{C}$. Let $c_\alpha(\mathcal{C})$ be the number of components of $G_\alpha(\mathcal{C})$. It is also the size of the largest coclique in G. Applying Turán's theorem ([11] or [9]) we get a relation between c_α and E_α.

Proposition 7 *If* $c_\alpha \leq K$*, then*

$$E_\alpha \geq \left\lfloor \frac{V_\alpha}{K} \right\rfloor V_\alpha - \frac{1}{2} \left\lfloor \frac{V_\alpha}{K} \right\rfloor (\left\lfloor \frac{V_\alpha}{K} \right\rfloor + 1) K.$$

Hence the integer

$$\min\{K \mid E_\alpha \geq \left\lfloor \frac{V_\alpha}{K} \right\rfloor V_\alpha - \frac{1}{2} \left\lfloor \frac{V_\alpha}{K} \right\rfloor \Big(\left\lfloor \frac{V_\alpha}{K} \right\rfloor + 1 \Big) K\}$$

is a lower bound for c_α*.*

Another useful invariant of the graph $G_\alpha(\mathcal{C})$ is $\mu_\alpha(\mathcal{C})$, the size of its largest component (i.e. clique). Turán's theorem for the complementary graph $\overline{G}_\alpha$ yields the following lower bound for $\mu_\alpha(\mathcal{C})$.

Proposition 8 *If $\mu_\alpha(\mathcal{C}) \leq M$, then*

$$E_\alpha \leq \binom{V_\alpha}{2} - \left\lfloor \frac{V_\alpha}{M} \right\rfloor V_\alpha + \frac{1}{2} \left\lfloor \frac{V_\alpha}{M} \right\rfloor \Big(\left\lfloor \frac{V_\alpha}{M} \right\rfloor + 1 \Big) M.$$

Hence

$$\min\{M \mid E_\alpha \leq \binom{V_\alpha}{2} - \left\lfloor \frac{V_\alpha}{M} \right\rfloor V_\alpha + \frac{1}{2} \left\lfloor \frac{V_\alpha}{M} \right\rfloor \Big(\left\lfloor \frac{V_\alpha}{M} \right\rfloor + 1 \Big) M\}$$

is a lower bound for μ_α.

However, the next proposition shows that good upper bounds for $\mu(\mathcal{C}) := \mu_{d-2}(\mathcal{C})$ are much more useful. What we really need are upper bounds for the number of words of weight up to $d-2$ in the cosets of $\mathcal{C}$.

Proposition 9 *An $[n,k,d]_q$-code $\mathcal{C}$ with*

$$\sum_{i=0}^{d-2} (q-1)^i \binom{n}{i} - 2\frac{|E(\mathcal{C})|}{\mu(\mathcal{C})} < q^{n-k}$$

is not maximal.

Proof. Consider the Varshamov graph $G(\mathcal{C})$. For $i = 1, 2, \ldots, \mu := \mu(\mathcal{C})$, let ν_i denote the number of components of size i. Then

$$\begin{aligned} c(\mathcal{C}) &= \sum_{i=1}^{\mu} \nu_i, \\ |V| &= \sum_{i=1}^{\mu} i\nu_i, \text{ and} \\ |E| &= \sum_{i=1}^{\mu} \binom{i}{2} \nu_i. \end{aligned}$$

Hence $c(\mathcal{C})$ is upperbounded by the maximal value of $\sum_{i=1}^{\mu} x_i$ under the constraints.

$$\begin{aligned} \sum_{i=1}^{\mu} i x_i &= |V|, \\ \sum_{i=1}^{\mu} \binom{i}{2} x_i &= |E|, \\ x_i &\geq 0, \quad 1 \leq i \leq \mu. \end{aligned}$$

We claim that

$$x_\mu = \frac{|E|}{\binom{\mu}{2}}, x_1 = |V| - \mu x_\mu, x_i = 0 \text{ otherwise},$$

is an optimal solution. So the maximal value of $\sum_{i=1}^{\mu} x_i$ is equal to

$$|V| - \mu\frac{|E|}{\binom{\mu}{2}} + \frac{|E|}{\binom{\mu}{2}} = |V| - 2\frac{|E|}{\mu}.$$

Indeed, the dual linear program

$$\begin{array}{rcl} |V|\, z_1 + |E|\, z_2 & \rightarrow & \min \\ iz_1 + \binom{i}{2} z_2 & \geq & 0, \quad 1 \leq i \leq \mu, \\ z_1, z_2 & \gtrless & 0 \end{array}$$

has a feasible solution,

$$z_1 = 1, z_2 = -\frac{2}{\mu},$$

that produces the same value of the objective function. ■

3 Varshamov–Gilbert type results

The number $c_\alpha(\mathcal{C})$ of components of $G_\alpha(\mathcal{C})$ cannot exceed q^{n-k}, the total number of cosets. Obviously, $\mathcal{C}$ is maximal if and only if the number of components $c(\mathcal{C})$ of the Varshamov graph $G(\mathcal{C}) := G_{d-2}(\mathcal{C})$ equals q^{n-k}.

Our goal is to find upper bounds on $c(\mathcal{C})$. For if such an upper bound is smaller then q^{n-k}, then $\mathcal{C}$ is not maximal. The simplest upper bound is

$$c(\mathcal{C}) \leq |V| = \sum_{i=0}^{d-2} (q-1)^i \binom{n}{i},$$

which immediately gives the classical Varshamov-Gilbert bound.

Proposition 10 (Varshamov [12].) *If*

$$\sum_{i=0}^{d-2} (q-1)^i \binom{n}{i} < q^{n-k},$$

then no $[n,k,d]_q$-code is maximal.

A general approach to find Varshamov-Gilbert type bounds would be to estimate the number of components of specific subgraphs of the Varshamov graph. We discuss two examples, basically due to Hashim [6] and Edel [4] respectively.

The first idea to consider a *forest* F in G. If $F' \supseteq F$ is a spanning forest of G, then

$$c(\mathcal{C}) = |V| - |E(F')| \leq |V| - |E(F)|, \tag{4}$$

So if we can find a forest in G with many edges, we have a good upper bound for $c(\mathcal{C})$.

An interesting example was found by Hashim. Put $t := \left\lfloor \frac{d-1}{2} \right\rfloor$.

Proposition 11 (Hashim [6].)*An* $[n,k,d]_q$*-code* $\mathcal{C}$ *with*

$$\sum_{w=d}^{d-2+t} \sum_{i=w-d+2}^{t} \binom{w}{i} A_w(\mathcal{C}) > \sum_{i=0}^{d-2} (q-1)^i \binom{n}{i} - q^{n-k}$$

is not maximal.

Proof. Consider the two disjoint subsets

$$X_1 := \{\mathbf{a} \mid 2 \leq \mathsf{wt}\,(\mathbf{a}) \leq t\}, X_2 := \{\mathbf{b} \mid \ t < \mathsf{wt}\,(\mathbf{b}) \leq d-2\}$$

of $\mathbb{F}_q^n$. The bipartite graph on $\{X_1, X_2\}$ with the edge set

$$E' := \{\{\mathbf{a},\mathbf{b}\} \mid \mathbf{a}-\mathbf{b} \in \mathcal{C} \text{ and } \mathsf{supp}\,\mathbf{a} \cap \mathsf{supp}\,\mathbf{b} = \emptyset\}$$

is a forest in G because all its vertices in X_2 have degree ≤ 1. Indeed, if $\{\mathbf{a},\mathbf{b}\}, \{\mathbf{a}',\mathbf{b}\} \in E'$, then $(\mathbf{a}-\mathbf{b}) - (\mathbf{a}'-\mathbf{b}) = \mathbf{a}-\mathbf{a}' \in \mathcal{C}$ and $\mathsf{wt}\,(\mathbf{a}-\mathbf{a}') \leq 2t < d$, whence $\mathbf{a} = \mathbf{a}'$. Each word of weight w in $\mathcal{C}$ contributes $\sum_{i=w-d+2}^{t} \binom{w}{i}$ to E'. Hence

$$|E'| = \sum_{w=d}^{d-2+t} \sum_{i=w-d+2}^{t} \binom{w}{i} A_w(\mathcal{C})$$

and, by (4),

$$c(\mathcal{C}) \leq \sum_{i=0}^{d-2} (q-1)^i \binom{n}{i} - \sum_{w=d}^{d-2+t} \sum_{i=w-d+2}^{t} \binom{w}{i} A_w(\mathcal{C}).$$

■

Hashim's result admits a simple improvement.

Proposition 12 *An* $[n,k,d]_q$*-code* $\mathcal{C}$ *with*

$$\sum_{w=d}^{d-2+t} \sum_{i=w-d+2}^{t} \sum_{j=w-i}^{d-2} p_{i,j}^{w} A_w(\mathcal{C}) > \sum_{i=0}^{d-2} (q-1)^i \binom{n}{i} - q^{n-k}$$

is not maximal.

Proof. Now consider the bipartite graph with the same vertex sets X_1, X_2 as in the preceding proposition, but with edge set

$$E'' := \{\{\mathbf{a}, \mathbf{b}\} \mid \mathbf{a} \in X_1, \mathbf{b} \in X_2 \text{ and } \mathbf{a} - \mathbf{b} \in \mathcal{C}\}.$$

By the same reasoning, this bipartite graph is seen to be a forest. Its number of edges is

$$\sum_{w=d}^{d-2+t} \sum_{i=w-d+2}^{t} \sum_{j=w-i}^{d-2} p_{i,j}^{w} A_w(\mathcal{C}). \tag{5}$$

Again we apply (4). ∎

Remark 13 *In the* binary *case, Expression (5) takes the form*

$$\sum_{\delta=0}^{t-2} \sum_{v=0}^{t-2-\delta} \sum_{u=0}^{\lfloor v/2 \rfloor} \binom{d+\delta}{d-2+u-v} \binom{n-d-\delta}{u} A_{d+\delta}(\mathcal{C}). \tag{6}$$

Now we come to the second idea. First we fix some notation. Let T be a subset of the coordinate index set $\{1, 2, \ldots, n\}$. The *projection* of an $\mathbf{x} \in \mathbb{F}_q^n$ to T is denoted by $\mathbf{x}_T$ and the code obtained by $\mathcal{C}$ through *shortening* with respect to T by $\mathcal{C}^{\overline{T}}$. (Here $\overline{T}$ denotes the complement of T in $\{1, 2, \ldots, n\}$.) We define $s_\alpha(\mathcal{C}) := c_\alpha(\mathcal{C}) - c_{\alpha-1}(\mathcal{C})$. Note that

$$s_\alpha(\mathcal{C}) \le (q-1)^\alpha \binom{n}{\alpha}, \tag{7}$$

with equality for $\alpha \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

We need two obvious lemmas.

Lemma 14 *If $\mathcal{C} := \mathcal{C}_1 \oplus \mathcal{C}_2$, then*

$$c_\alpha(\mathcal{C}) = \sum_{j=0}^{\alpha} s_j(\mathcal{C}_1) c_{\alpha-j}(\mathcal{C}_2).$$

Lemma 15 *If $\mathcal{D} \subseteq \mathcal{C}$, then $c_\alpha(\mathcal{D}) \ge c_\alpha(\mathcal{C})$.*

The following relation between the values of c_α for $\mathcal{C}$, $\mathcal{C}^T$ and $\mathcal{C}^{\overline{T}}$ creates a possibility of induction.

Proposition 16

$$c_\alpha(\mathcal{C}) \le \sum_{j=0}^{\min(\alpha,m)} s_j(\mathcal{C}^T) c_{\alpha-j}(\mathcal{C}^{\overline{T}}). \tag{8}$$

Proof. Note that $\mathcal{C}^T \oplus \mathcal{C}^{\overline{T}}$ is a subcode of $\mathcal{C}$ and apply the preceding lemmas. In fact, the right hand side counts the components of the subgraph G' of $G(\mathcal{C})$ with the same vertex set V, but with the edge set

$$E' := \{\{\mathbf{a}, \mathbf{b}\} \mid \mathbf{a}_T - \mathbf{b}_T \in \mathcal{C}^T \wedge \mathbf{a}_{\overline{T}} - \mathbf{b}_{\overline{T}} \in \mathcal{C}^{\overline{T}}\}.$$

■

Corollary 17 (Edel [4]) *From (7) we infer that*

$$c_\alpha(\mathcal{C}) \leq \sum_{j=0}^{\min(\alpha,m)} (q-1)^j \binom{n}{j} c_{\alpha-j}(\mathcal{C}^{\overline{T}}).$$

We can embed any $[n, k, d]_q$-code $\mathcal{C}$ in an $[n+1, k, d]_q$-code $\mathcal{C}'$ by adding one zero coordinate to each codeword. Let us call this construction *trivial lengthening.* Corollary 17, with $m = 1$, immediately gives the bound

$$c_\alpha(\mathcal{C}') \leq c_\alpha(\mathcal{C}) + (q-1)c_{\alpha-1}(\mathcal{C}). \tag{9}$$

If an $[n, k, d]_q$-code $\mathcal{C}$ is not maximal, we can embed it in an $[n+1, k+1, d]_q$-code $\mathcal{C}'$. Let us call this a *Varshamov step.* The component sizes $c_\alpha(\mathcal{C}')$ of the new code $\mathcal{C}'$ satisfy the bounds

$$c_\alpha(\mathcal{C}') \leq c_\alpha(\mathcal{C}) + (q-1)c_{\alpha-1}(\mathcal{C}). \tag{10}$$

Indeed, let $n+1$ be the extra coordinate index in $\mathcal{C}'$. We can split the vertex set $V_\alpha(\mathcal{C}')$ of $\mathcal{C}'$ into the q subsets

$$W_i := \{\mathbf{u} \in V_\alpha(\mathcal{C}') \mid u_{n+1} = i\}.$$

Then the restriction of $G_\alpha(\mathcal{C}')$ to W_i is isomorphic to $G_\alpha(\mathcal{C})$ if $i = 0$, and isomorphic to $G_{\alpha-1}(\mathcal{C})$ if $i \neq 0$.

Now Edel's idea in [4] is as follows. Start with an $[n_i, k_i, d]_q$-code $\mathcal{C}_0$ and build a sequence of $[n_i, k_i, d]_q$-codes $\mathcal{C}_i$, $i = 1, 2, \ldots$, of increasing length by taking Varshamov steps when our information on $c_{d-2}(\mathcal{C}_i)$ tells us that this possible. If not, apply trivial lengthening until a Varshamov step again is possible. At each step, estimate the $c_\alpha(\mathcal{C}_i)$ using (9), (10) and the trivial bound $c_\alpha(\mathcal{C}_i) \leq q^{n_i - k_i}$. By this simple method, Edel improved quite a few lower bounds in Brouwer's tables [2] on bounds for optimal linear ternary and quaternary linear codes. Without doubt, the method will work for larger alphabets as well.

References

[1] Blahut, Richard E. Theory and practice of error control codes. *Addison-Wesley Publishing Co.*, Reading, Mass., 1983. xi+500 pp. ISBN: 0-201-10102-5

[2] Brouwer, A. E. Bounds on the size of linear codes. To appear in V. Pless and W. Cary Huffman, Eds, Handbook of coding theory *Elsevier Science*, 1998. Online version: `http://www.win.tue.nl/math/dw/voorlincod.html`.

[3] Delsarte, P. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.* No. 10 (1973), vi+97 pp.

[4] Edel, Y. Eine Verallgemeinerung von BCH-Codes. PhD Thesis, Univ. Heidelberg, 1996.

[5] Gilbert, E. N. A comparison of signalling alphabets. *Bell Syst. Tech. J.* **31** (1952), 504–522.

[6] Hashim, A. A. Improvement on Varshamov-Gilbert lower bound on minimum Hamming distance of linear codes. *Proc. Inst. Elec. Engrs.* **125** (1978), no. 2, 104–106.

[7] van Lint, J. H.; Wilson, R. M. A course in combinatorics. *Cambridge University Press, Cambridge,* 1992, xii+530 pp. ISBN: 0-521-41057-6; 0-521-42260-4.

[8] MacWilliams, F. J.; Sloane, N. J. A. The theory of error-correcting codes. 2nd reprint. North-Holland Mathematical Library, Vol. 16. *North-Holland Publishing Co., Amsterdam - New York - Oxford,* 1983, xx+762 pp. ISBN: 0-444-85009-0 and 0-444-85010-4.

[9] Ore, O. Theory of graphs. Third printing, with corrections. American Mathematical Society Colloquium Publications, Vol. XXXVIII *American Mathematical Society, Providence, R.I.* 1967 x+270 pp.

[10] Tsfasman, M. A.; Vlăduţ, S. G. Algebraic-geometric codes. *Kluwer Academic Publishers Group*, Dordrecht, 1991. xxiv+667 pp. ISBN: 0-7923-0727-5

[11] Turán, P. Eine Extremalaufgabe aus der Graphentheorie. (Hungarian. German summary.) *Mat. Fiz. Lapok* **48** (1941), 436–452.

[12] Varshamov, R.R. Estimate of the number of signals in error correcting codes. *Dokl. Acad. Nauk SSSR,* **117** (1957), 739–741.