Linear Algebra and its Applications 307 (2000) 119–129

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

# Strengthening the Gilbert–Varshamov bound

Alexander Barg [a], Sugi Guritman [b], Juriaan Simonis [b,*]

[a] *Lucent Technologies, Bell Labs, 600 Mountain avenue 2C-375, Murray Hill, NJ 07974-0636, USA*
[b] *Faculty of Information Technology and Systems, Delft University of Technology, P.O. Box 5031, 2600 GA Delft, Netherlands*

Received 12 October 1998; accepted 10 December 1999

Submitted by R.A. Brualdi

**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. © 2000 Elsevier Science Inc. All rights reserved.

*Keywords:* Linear code; Maximal code; Intersection number; Lengthening

## 1. Introduction

Let 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 [13] 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 Proposition 12). Moreover, Varshamov [13] suggests a greedy procedure of constructing a parity-check matrix for a code whose parameters meet the bound. Gilbert [6] suggested a similar greedy algorithm that produces (not

* Corresponding author.
*E-mail addresses:* abarg@research.bell-labs.com (A. Barg), simonis@twi.tudelft.nl (J. Simonis), S.Guritman@twi.tudelft.nl (S. Guritman).

PII: S 0 0 2 4 - 3 7 9 5 ( 9 9 ) 0 0 2 7 1 - 2

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 [11]. 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 Propositions 10 and 14 [7], Proposition 15 and Corollary 21 [4].

## 2. The Varshamov graph

**Definition 1.** The code $\mathsf{C}$ 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* $\mathsf{C}$ *is maximal if and only if its covering radius* $\rho(\mathsf{C})$ *does not exceed* $d-2$*.*

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

So an $[n, k, d]_q$-code $\mathsf{C}$ with $\rho(\mathsf{C}) > d-2$ is not maximal. The following proposition, a generalization of a result by Elia [5], extends this observation to codes with arbitrary covering radius. The proof is completely analogous to that of the preceding proposition.

**Proposition 3.** *An* $[n, k, d]_q$*-code* $\mathsf{C}$ *with* $\rho(\mathsf{C}) > \alpha$, $\alpha < d$, *can be extended to an* $[n+d-\alpha-1, k+1, d]_q$ *-code.*

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

**Definition 4.** The undirected graph with the vertex set

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

and the edge set

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

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

Obviously, the number of vertices in $G_\alpha$ 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 $(A_i(\mathsf{C}))_{i=0,1,\ldots,n}$ of $\mathsf{C}$.

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

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

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 6). See [3], [9, Chapter 21] or [8, Chapter 30] 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 5** [1].

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

*For $q = 2$, this reduces to*

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

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

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

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

$$\begin{cases} w = \alpha+\beta+\gamma, \\ i = \alpha+\beta+\delta, \\ j = \beta+\gamma+\delta. \end{cases}$$

Solve for $\alpha$, $\beta$ and $\gamma$, and substitute in (3 ). □

**Remark 6.** 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 [3,8,9].

**Proposition 7.** *The size of the edge set $E_\alpha$ of $G_\alpha(\mathsf{C})$ is equal to*

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

*A more explicit formula in the binary case is*

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

**Proof.** If $\mathbf{c} \in \mathsf{C}$ 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, $E_\alpha$ is equal to

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

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 $G_\alpha(\mathsf{C})$ has a very simple structure: its components are complete graphs whose vertices are the intersections of $V_\alpha$ with the cosets of weight $\leqslant \alpha$ of $\mathsf{C}$. Let

$c_\alpha(\mathsf{C})$ be the number of components of $G_\alpha(\mathsf{C})$. It is also the size of the largest co-clique in $G$. Applying Turán's theorem ([10] or [12]) we get a relation between $c_\alpha$ and $E_\alpha$.

**Proposition 8.** *If $c_\alpha \leqslant K$, then*

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

*Hence the integer*

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

*is a lower bound for $c_\alpha$.*

Another useful invariant of the graph $G_\alpha(\mathsf{C})$ is $\mu_\alpha(\mathsf{C})$, 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 $\mu_\alpha(\mathsf{C})$.

**Proposition 9.** *If $\mu_\alpha(\mathsf{C}) \leqslant M$, then*

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

*Hence*

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

*is a lower bound for $\mu_\alpha$.*

However, the next proposition shows that good upper bounds for $\mu(\mathsf{C}) := \mu_{d-2}(\mathsf{C})$ 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 $\mathsf{C}$.

**Proposition 10.** *An $[n,k,d]_q$-code $\mathsf{C}$ with*

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

*is not maximal.*

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

$$c(\mathsf{C}) = \sum_{i=1}^{\mu} \nu_i,$$

$$|V| = \sum_{i=1}^{\mu} i v_i,$$
$$|E| = \sum_{i=1}^{\mu} \binom{i}{2} v_i.$$

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

$$\sum_{i=1}^{\mu} i x_i = |V|,$$
$$\sum_{i=1}^{\mu} \binom{i}{2} x_i = |E|,$$
$$x_i \geqslant 0, \quad 1 \leqslant i \leqslant \mu.$$

We claim that

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

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

$$|V| z_1 + |E| z_2 \to \min$$
$$i z_1 + \binom{i}{2} z_2 \geqslant 0, \quad 1 \leqslant i \leqslant \mu,$$
$$z_1, z_2 \gtrless 0$$

has a feasible solution

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

that produces the same value of the objective function. □

**Remark 11.** Following the idea of Proposition 3, we can generalize this result: An $[n, k, d]_q$-code $\mathsf{C}$ with

$$\sum_{i=0}^{\alpha} (q-1)^i \binom{n}{i} - 2\frac{|E_\alpha(\mathsf{C})|}{\mu_\alpha(\mathsf{C})} < q^{n-k}$$

for some $\alpha \leqslant d - 1$ can be extended to an $[n + d - \alpha - 1, k + 1, d]_q$ -code.

## 3. Varshamov–Gilbert type results

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

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

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

which immediately gives the classical Varshamov–Gilbert bound.

**Proposition 12** [13]. *If*

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

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

**Remark 13.** By Proposition 3, we can generalize this:
If

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

for some $\alpha \leqslant d-1$, then any $[n,k,d]_q$-code can be extended to an $[n+d-\alpha-1, k+1, d]_q$-code.

For $\alpha = d-3$ this reduces to Elia's result [5].

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 [4,7], respectively.

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

$$c(\mathsf{C}) = |V| - |E(F')| \leqslant |V| - |E(F)|. \tag{4}$$

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

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

**Proposition 14** [7]. *An* $[n,k,d]_q$*-code* $\mathsf{C}$ *with*

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

*is not maximal.*

**Proof.** Consider the two disjoint subsets

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

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

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

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

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

and by (4),

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

Hashim’s result admits a simple improvement.

**Proposition 15.** *An $[n, k, d]_q$-code $\mathsf{C}$ with*

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

*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

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

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

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

Again we apply (4). □

**Remark 16.** In the *binary* case, Expression (5) takes the form

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

**Remark 17.** Proposition 3 enables us to generalize Proposition 15 in the following way:
An $[n, k, d]_q$-code $\mathsf{C}$ with

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

for some $\alpha \leqslant d-1$ can be extended to an $[n+d-\alpha-1, k+1, d]_q$ -code.

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 $\mathbf{x} \in \mathsf{F}_q^n$ to $T$ is denoted by $\mathbf{x}_T$ and the code obtained by $\mathsf{C}$ through *shortening* with respect to $T$ by $\mathsf{C}^{\overline{T}}$. (Here $\overline{T}$ denotes the complement of $T$ in $\{1, 2, \ldots, n\}$.) We define $s_\alpha(\mathsf{C}) := c_\alpha(\mathsf{C}) - c_{\alpha-1}(\mathsf{C})$. Note that

$$s_\alpha(\mathsf{C}) \leqslant (q-1)^\alpha \binom{n}{\alpha} \tag{7}$$

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

We need two obvious lemmas.

**Lemma 18.** *If* $\mathsf{C} := \mathsf{C}_1 \oplus \mathsf{C}_2$, *then*

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

**Lemma 19.** *If* $\mathsf{D} \subseteq \mathsf{C}$, *then* $c_\alpha(\mathsf{D}) \geqslant c_\alpha(\mathsf{C})$.

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

**Proposition 20.**

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

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

$$E' := \left\{ \{\mathbf{a}, \mathbf{b}\} \mid \mathbf{a}_T - \mathbf{b}_T \in \mathsf{C}^T \wedge \mathbf{a}_{\overline{T}} - \mathbf{b}_{\overline{T}} \in \mathsf{C}^{\overline{T}} \right\}. \qquad \square$$

**Corollary 21** [4]. *From* (7) *we infer that*

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

We can embed any $[n,k,d]_q$-code $\mathsf{C}$ in an $[n+1,k,d]_q$-code $\mathsf{C}'$ by adding one zero coordinate to each codeword. Let us call this construction *trivial lengthening*. Corollary 21 with $m=1$, immediately gives the bound

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

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

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

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

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

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

Now Edel's idea in [4] is as follows. Start with an $[n_i,k_i,d]_q$-code $\mathsf{C}_0$ and build a sequence of $[n_i,k_i,d]_q$-codes $\mathsf{C}_i$, $i=1,2,\ldots,$ of increasing length by taking Varshamov steps when our information on $c_{d-2}(\mathsf{C}_i)$ tells us that this possible. If not, apply trivial lengthening until a Varshamov step again is possible. At each step, estimate the $c_\alpha(\mathsf{C}_i)$ using (9), (10) and the trivial bound $c_\alpha(\mathsf{C}_i) \leqslant q^{n_i-k_i}$. 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] R.E. Blahut, Theory and Practice of Error Control Codes, Addison-Wesley, Reading, MA, 1983.

[2] A.E. Brouwer, Bounds on the size of linear codes, in: V. Pless, W. Cary Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998. Online version of the tables: http://www.win.tue.nl/math/dw/voorlincod.html.

[3] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. 10 (1973).

[4] Y. Edel, Eine Verallgemeinerung von BCH-Codes, Ph.D. Thesis, University of Heidelberg, 1996.

[5] M. Elia, Some results on the existence of binary linear codes, IEEE Trans. Inform. Theory 29 (1983) 933–934.

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

[7] A.A. Hashim, Improvement on Varshamov–Gilbert lower bound on minimum Hamming distance of linear codes, Proc. Inst. Elec. Engrs. 125 (1978) 104–106.

[8] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, Cambridge University Press, Cambridge, 1992.

[9] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, vol. 16, North-Holland Mathematical Library, North-Holland, Amsterdam, 1983 (Second reprint).

[10] O. Ore, Theory of Graphs (Third printing, with corrections), American Mathematical Society Colloquium Publications, Vol. XXXVIII American Mathematical Society, Providence, RI, 1967.

[11] M.A. Tsfasman, S.G. Vladut, Algebraic-Geometric Codes (Translated from the Russian by the authors), Mathematics and its Applications (Soviet Series), vol. 58. Kluwer Academic Publishers, Dordrecht, 1991.

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

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