



## CHAPTER III

### BOUNDS ON LINEAR ERROR-BLOCK CODES

Given an  $[n, k, d; \pi]$  code  $\mathcal{C}$  over  $\mathbb{F}_q$ , where  $n$  and  $\pi$  are fixed, the dimension  $k$  (or the size  $q^k$ ) is a measure of the efficiency of the code and the minimum  $\pi$ -distance  $d$  is an indication of its error-correction. Enlarging both parameters is an impossible task since they work in opposite directions as shown in the following examples.

**Example 3.1.** Let  $\pi$  be a partition of a given integer  $n$ . Consider a linear error-block code  $\mathcal{C} = \mathbb{F}_q^n$  over  $\mathbb{F}_q$  with type  $\pi$ . Clearly,  $\mathcal{C}$  is an  $[n, n, 1; \pi]$  code. This code has the maximum possible dimension, while its minimum  $\pi$ -distance is 1. As the minimum  $\pi$ -distance of a code related closely to its error-correcting capability, a low minimum  $\pi$ -distance implies a low error-correcting capability.

**Example 3.2.** Let  $\alpha$  be a primitive element of the finite field  $\mathbb{F}_q$ . Consider a repetition linear error-block code  $\mathcal{C} = \{ \underbrace{00 \dots 0}_{n \text{ copies}}, \underbrace{11 \dots 1}_{n \text{ copies}}, \underbrace{\alpha \alpha \dots \alpha}_{n \text{ copies}}, \underbrace{\alpha^2 \alpha^2 \dots \alpha^2}_{n \text{ copies}}, \dots, \underbrace{\alpha^{q-2} \alpha^{q-2} \dots \alpha^{q-2}}_{n \text{ copies}} \}$  over  $\mathbb{F}_q$  with type  $\pi = [n_1][n_2] \dots [n_s]$ . Clearly,  $\mathcal{C}$  is an  $[n, 1, s; \pi]$  code. As this code has the largest possible minimum  $\pi$ -distance, it has an excellent error-correcting potential. However, this is achieved at the cost of very low efficiency.

The above examples indicate that a compromise between the dimension and the quantity of error-correction is necessary. Here, we emphasize on maximizing either the dimension  $k$  where  $n, d$  and  $\pi$  are fixed or the minimum  $\pi$ -distance  $d$  where  $n, k$  and  $\pi$  are fixed.

**Definition 3.1.** Let  $q$  be a prime power and  $\pi$  a partition of a given positive integer  $n$ .

- i) For each positive integer  $d$ , let  $\mathbf{k}_{\max}(n, d, q; \pi)$  denote the largest possible dimension  $k$  for which there exists an  $[n, k, d; \pi]$  code over  $\mathbb{F}_q$ . Thus

$$\mathbf{k}_{\max}(n, d, q; \pi) = \max\{k \mid \text{there exists an } [n, k, d; \pi] \text{ code over } \mathbb{F}_q\}.$$

An  $[n, k, d; \pi]$  code  $\mathcal{C}$  over  $\mathbb{F}_q$  that  $k = \mathbf{k}_{\max}(n, d, q; \pi)$  is called a **maximal dimension code**.

- ii) For each positive integer  $k$ , let  $\mathbf{d}_{\max}(n, k, q; \pi)$  denote the largest possible minimum  $\pi$ -distance  $d$  for which there exists an  $[n, k, d; \pi]$  code over  $\mathbb{F}_q$ .

Thus

$$\mathbf{d}_{\max}(n, k, q; \pi) = \max\{d \mid \text{there exists an } [n, k, d; \pi] \text{ code over } \mathbb{F}_q\}.$$

An  $[n, k, d; \pi]$  code  $\mathcal{C}$  over  $\mathbb{F}_q$  that  $d = \mathbf{d}_{\max}(n, k, q; \pi)$  is called a **maximal minimum  $\pi$ -distance code**.

Here, we choose to focus on  $\mathbf{k}_{\max}(n, d, q; \pi)$  and  $\mathbf{d}_{\max}(n, k, q; \pi)$ , thus an **optimal code** means a code which has the maximum dimension or largest minimum  $\pi$ -distance.

This chapter is devoted to developing several lower bounds for  $\mathbf{k}_{\max}$  and  $\mathbf{d}_{\max}$  along with other upper bounds beside the  $\pi$ -singleton bound and the  $\pi$ -Hamming bound which are studied by K. Feng, L. Xu and F. J. Hickernell [3]

### 3.1 Lower Bounds

Lower bounds for  $\mathbf{k}_{\max}(n, d, q; \pi)$  and  $\mathbf{d}_{\max}(n, k, q; \pi)$  can be obtained by proving the existence of  $[n, k, d; \pi]$  code. For convenience, we would construct an

$[n, k, d'; \pi]$  code with  $d' \geq d$  which certainly implies the existence of an  $[n, k, d; \pi]$  code. This can be done by replacing (arbitrary)  $d' - d$  blocks by zeros. Both lower bounds offered here are given in terms of the number of elements of a sphere centered at a codeword.

**Definition 3.1.1.** A sphere of radius  $r$  centered at  $u$  in  $\mathbb{F}_q^n$  with respect to the partition  $\pi$  of  $n$ , denoted  $S_\pi(u, r)$ , is defined by

$$S_\pi(u, r) = \{v \in \mathbb{F}_q^n \mid d_\pi(u, v) \leq r\}.$$

The number of elements in a sphere of radius  $r$  is denoted by  $V_q^n(r; \pi)$ .

**Lemma 3.1.1.** Let  $\pi = [n_1][n_2] \dots [n_s]$  be a partition of a given integer  $n$ . Then for each integer  $r \leq s$ ,

$$V_q^n(r; \pi) = 1 + \sum_{j=1}^r \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq s} \prod_{z=1}^j (q^{n_{i_z}} - 1).$$

*Proof.* Let  $u = u_1 u_2 \dots u_s \in \mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2} \times \dots \times \mathbb{F}_q^{n_s}$  and  $r \leq s$ . For each block  $i$ , there are  $q^{n_i} - 1$  choices of  $v_i \in \mathbb{F}_q^{n_i}$  such that  $v_i \neq u_i$ . Thus, for each  $j$  blocks, say  $i_1, i_2, \dots, i_j$ , there are  $\prod_{z=1}^j (q^{n_{i_z}} - 1)$  choices of  $v$ 's in  $\mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2} \times \dots \times \mathbb{F}_q^{n_s}$  such that  $d_\pi(u, v) = j$ . Hence

$$|\{v \in \mathbb{F}_q^n \mid d_\pi(u, v) = j\}| = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq s} \prod_{z=1}^j (q^{n_{i_z}} - 1).$$

Consequently,

$$\begin{aligned} V_q^n(r; \pi) &= |S_\pi(u, r)| \\ &= \left| \bigcup_{j=0}^r \{v \in \mathbb{F}_q^n \mid d_\pi(u, v) = j\} \right|. \end{aligned}$$

Since the union is disjoint,

$$\begin{aligned} V_q^n(r; \pi) &= \sum_{j=0}^r |\{v \in \mathbb{F}_q^n \mid d_\pi(u, v) = j\}| \\ &= 1 + \sum_{j=1}^r \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq s} \prod_{z=1}^j (q^{n_{i_z}} - 1). \end{aligned}$$

□

**Remark 3.1.1.** Let  $\pi = [n_1][n_2] \dots [n_s]$  be a partition of a given integer  $n$ .

i) For  $r \geq s$ , a sphere of radius  $r$  covers the whole space  $\mathbb{F}_q^n$  and hence

$$V_q^n(r; \pi) = q^n.$$

ii) For a partition  $\pi = [m]^s$  of  $n$ ,  $V_q^n(r; \pi)$  can be simplified as follows :

$$\begin{aligned} V_q^n(r; [m]^s) &= 1 + \sum_{j=1}^r \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq s} \prod_{z=1}^j (q^m - 1) \\ &= 1 + \sum_{j=1}^r \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq s} (q^m - 1)^j \\ &= 1 + \sum_{j=1}^r \binom{s}{j} (q^m - 1)^j \\ &= \sum_{j=0}^r \binom{s}{j} (q^m - 1)^j. \end{aligned}$$

In particular,

$$V_q^n(r; [1]^n) = \sum_{i=0}^r \binom{n}{i} (q - 1)^i,$$

and it is simply denoted by  $V_q^n(r)$ .

Recall that an  $[n, k, d]$  code may be viewed as an  $[n, k, d; \pi]$  code where  $\pi = [1]^n$ . In this sense, we generalize two well-known lower bounds, the Gilbert bound and the Gilbert-Varshamov bound, and name them  $\pi$ -Gilbert bound and  $\pi$ -Gilbert-Varshamov bound, respectively.

The construction of codes in the proof of the  $\pi$ -Gilbert bound uses the sphere covering concept whereas parity-check matrices are constructed in the case of the  $\pi$ -Gilbert-Varshamov bound.

**Theorem 3.1.2 ( $\pi$ -Gilbert bound).** *Let  $\pi = [n_1][n_2] \dots [n_s]$  be a partition of a given positive integer  $n$  and  $q$  a prime power. Let  $k, d \in \mathbb{N}$  be such that  $k \leq n$  and  $d \leq s$ . If*

$$V_q^n(d - 1; \pi) < q^{n-k+1},$$

then there exists an  $[n, k; \pi]$  code over  $\mathbb{F}_q$  with minimum  $\pi$ -distance at least  $d$ .

*Proof.* We will construct an  $[n, k; \pi]$  code with minimum  $\pi$ -distance at least  $d$  recursively on  $k$ . The code in Example 3.2 takes care the case  $k = 1$ . For  $k \geq 2$ , let  $\mathcal{C}_{k-1}$  be an  $[n, k-1, d; \pi]$  code over  $\mathbb{F}_q$ . By the assumption,

$$q^{k-1}V_q^n(d-1; \pi) < q^n.$$

Hence the union of all spheres of radius  $d-1$  around the codewords in  $\mathcal{C}_{k-1}$  does not cover the whole space  $\mathbb{F}_q^n$ . This implies that there is a word  $x \in \mathbb{F}_q^n$  such that  $\min_{c \in \mathcal{C}_{k-1}} d_\pi(x, c) \geq d$ . Let  $\mathcal{C} = \langle x \rangle \oplus \mathcal{C}_{k-1}$ . Then  $\mathcal{C}$  is an  $[n, k; \pi]$  code. To compute  $d_\pi(\mathcal{C})$ , let  $u \in \mathcal{C} \setminus \{0\}$ . If  $u \in \mathcal{C}_{k-1}$ , then we are done. Assume that  $u \notin \mathcal{C}_{k-1}$ . Then  $u = \lambda x + v$  where  $v \in \mathcal{C}_{k-1}$  and  $\lambda \in \mathbb{F}_q \setminus \{0\}$ . Hence

$$w_\pi(u) = w_\pi(\lambda x + v) = w_\pi(x + \lambda^{-1}v) = d_\pi(x, -\lambda^{-1}v) \geq \min_{c \in \mathcal{C}_{k-1}} d_\pi(x, c) \geq d.$$

As a result  $\mathcal{C}$  is an  $[n, k; \pi]$  code with minimum  $\pi$ -distance at least  $d$ .  $\square$

**Corollary 3.1.3.** *Let  $q$  be a prime power and  $\pi = [n_1][n_2] \dots [n_s]$  a partition of a given positive integer  $n$ . For each integer  $d$ , if  $1 \leq d \leq s$ , then*

$$k_{\max}(n, d, q; \pi) \geq n + 1 - \lceil \log_q(1 + V_q^n(d-1; \pi)) \rceil.$$

*Proof.* By Theorem 3.1.2,  $k_{\max}(n, d, q; \pi)$  is not less than the largest  $k$  satisfying the inequality

$$1 + V_q^n(d-1; \pi) \leq q^{n-k+1}.$$

That is

$$\log_q(1 + V_q^n(d-1; \pi)) \leq n - k + 1.$$

Thus, the largest  $k$  is

$$n + 1 - \lceil \log_q(1 + V_q^n(d-1; \pi)) \rceil.$$

$\square$

**Theorem 3.1.4 ( $\pi$ -Gilbert-Varshamov bound).** *Let  $q$  be a prime power and let  $n, k, d$  and  $s$  be positive integers satisfying  $2 \leq d \leq s$  and  $k \leq n$ . Let  $\pi = [n_1][n_2] \dots [n_s]$  be a partition of  $n$  such that  $n_i = 1$  for all  $i \geq d - 1$ . If*

$$V_q^{n-1}(d-2, \pi') < q^{n-k}$$

where  $\pi' = [n_1][n_2] \dots [n_{s-1}]$ , then there exists an  $[n, k; \pi]$  code over  $\mathbb{F}_q$  with minimum  $\pi$ -distance at least  $d$ .

*Proof.* An  $[n, k, d; \pi]$  code over  $\mathbb{F}_q$  can be obtained by constructing an  $(n-k) \times n$  matrix  $H = [H_1 \ H_2 \ \dots \ H_s]$  for which any  $d-1$  blocks are linearly independent. If  $d = 2$ ,  $\pi$  is the trivial partition  $[1]^n$ . Thus a matrix  $\mathbf{H} = [H_1 \ H_2 \ \dots \ H_n]$  where  $H_i$  is a nonzero column vector in  $\mathbb{F}_q^{n-k}$  is a desired parity-check matrix.

Assume that  $d > 2$ . We first claim that

$$n_1 + n_2 + \dots + n_{d-2} < n - k.$$

Since the number of vectors in the linear span of  $d-2$  linearly independent blocks which is  $q^{n_1+n_2+\dots+n_{d-2}}$  can be counted in blocks to obtain

$$1 + \sum_{j=1}^{d-2} \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq d-2} \prod_{z=1}^j (q^{n_{i_z}} - 1),$$

we conclude that

$$\begin{aligned} q^{n_1+n_2+\dots+n_{d-2}} &= 1 + \sum_{j=1}^{d-2} \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq d-2} \prod_{z=1}^j (q^{n_{i_z}} - 1) \\ &\leq 1 + \sum_{j=1}^{d-2} \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq s-1} \prod_{z=1}^j (q^{n_{i_z}} - 1) \\ &= V_q^{n-1}(d-2, \pi') \\ &< q^{n-k}. \end{aligned}$$

Hence  $n_1 + n_2 + \dots + n_{d-2} < n - k$ . In this case,  $H_i$ 's are constructed recursively as follows :

Let  $H_1$  be an  $(n - k) \times n_1$  matrix whose columns are linearly independent. (This can be done since  $n_1 < n - k$ .) For  $2 \leq l \leq d - 2$ , let block  $H_l$  be an  $(n - k) \times n_l$  matrix such that the columns are linearly independent and are not in the linear span of  $H_1, H_2, \dots, H_{l-1}$ . These choices are possible since

$$n_1 + n_2 + \dots + n_{d-2} < n - k.$$

For  $d - 1 \leq l \leq s$ , let block  $H_l$  be a nonzero  $(n - k) \times 1$  matrix such that  $H_l$  are not in the linear span of  $d - 2$  blocks of  $H_1, H_2, \dots, H_{l-1}$ . Such a block exists since the number of vectors in the linear span of arbitrary  $d - 2$  blocks of  $H_1, H_2, \dots, H_{l-1}$  is

$$1 + \sum_{j=1}^{d-2} \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq l-1} \prod_{z=1}^j (q^{n_{i_z}} - 1)$$

which is less than  $q^{n-k}$  by the above verification. Hence any  $d - 1$  blocks of  $\mathbf{H} = [H_1 \ H_2 \ \dots \ H_s]$  are linearly independent. Consequently,  $\mathbf{H}$  is a parity-check matrix of an  $[n, k; \pi]$  code over  $\mathbb{F}_q$  whose minimum  $\pi$ -distance is at least  $d$ .  $\square$

When  $\pi = [1]^n$ , the  $\pi$ -Gilbert-Varshamov bound is obviously the Gilbert-Varshamov bound for linear codes.

**Corollary 3.1.5 (Gilbert-Varshamov bound,[6]).** *Let  $q$  be a prime power and let  $n, k$  and  $d$  be positive integers satisfying  $2 \leq d \leq n$  and  $k \leq n$ . If*

$$V_q^{n-1}(d-2) < q^{n-k}, \tag{3.1.1}$$

*then there exists an  $[n, k]$  code over  $\mathbb{F}_q$  with minimum Hamming distance at least  $d$ .*

A nice application of the  $\pi$ -Gilbert-Varshamov bound is an easily manual computing bound for  $\mathbf{k}_{\max}(n, d, q; \pi)$ . However, both the  $\pi$ -Gilbert bound and the  $\pi$ -Gilbert-Varshamov bound do not lead to the explicit lower bound for  $\mathbf{d}_{\max}(n, k, q; \pi)$ .

**Corollary 3.1.6.** *Let  $q$  be a prime power and  $n, d$  and  $s$  be positive integers satisfying  $2 \leq d \leq s$ . If  $\pi = [n_1][n_2] \dots [n_s]$  is a partition of  $n$  such that  $n_i = 1$  for all  $i \geq d - 1$ , then*

$$k_{\max}(n, d, q; \pi) \geq n - \lceil \log_q(1 + V_q^{n-1}(d-2; \pi')) \rceil$$

where  $\pi' = [n_1][n_2] \dots [n_{s-1}]$ .

*Proof.* By Theorem 3.1.4,  $k_{\max}(n, d, q; \pi)$  is not less than the largest  $k$  satisfying the inequality

$$1 + V_q^{n-1}(d-2; \pi') \leq q^{n-k}.$$

Thus,

$$\log_q(1 + V_q^{n-1}(d-2; \pi')) \leq n - k.$$

That is

$$k \leq n - \log_q(1 + V_q^{n-1}(d-2; \pi')).$$

Thus, the largest  $k$  is

$$n - \lceil \log_q(1 + V_q^{n-1}(d-2; \pi')) \rceil.$$

□

## 3.2 Upper Bounds

The purpose of having several upper bounds is that one may be smaller than another. In general, one would like an upper bound as tight as possible so that there is hope that codes meeting this bound actually exist.

Since an  $[n, k, d]$  code can be viewed as an  $[n, k, d; \pi]$  code where  $\pi = [1]^n$ . Two well-known upper bounds for linear codes, the singleton bound and the Hamming bound, were generalized by K. Feng, L. Xu and F. J. Hickernell. Both generalized bounds are named  $\pi$ -singleton bound and  $\pi$ -Hamming bound, respectively [3].



The  $\pi$ -singleton bound was derived based on the fact that the number of linearly independent columns of a matrix is not greater than the number of rows.

**Theorem 3.2.1 ( $\pi$ -singleton bound, [3]).** *Let  $\mathcal{C}$  be an  $[n, k, d; \pi]$  code over  $\mathbb{F}_q$  with type  $\pi = [n_1][n_2] \dots [n_s]$ . Then*

$$k \leq n_d + n_{d+1} + \dots + n_s.$$

**Corollary 3.2.2.** *Let  $n, d$  and  $s$  be positive integers satisfying  $d \leq s$ . For each partition  $\pi = [n_1][n_2] \dots [n_s]$  of  $n$ ,*

$$k_{\max}(n, d, q; \pi) \leq n_d + n_{d+1} + \dots + n_s.$$

The sphere packing concept was used in proving the  $\pi$ -Hamming bound.

**Theorem 3.2.3 ( $\pi$ -Hamming bound, [3]).** *Let  $\mathcal{C}$  be an  $[n, k, d; \pi]$  code with type  $\pi = [n_1][n_2] \dots [n_s]$  over  $\mathbb{F}_q$  and  $\pi' = [n_2][n_3] \dots [n_s]$ . Then*

$$q^{n-k} \geq \begin{cases} V_q^n(l; \pi) & \text{if } d = 2l + 1, \\ q^{n_1} V_q^{n-n_1}(l-1; \pi') & \text{if } d = 2l \geq 2. \end{cases}$$

**Corollary 3.2.4.** *Let  $q$  be a prime power and  $\pi = [n_1][n_2] \dots [n_s]$  a partition of a given positive integer  $n$ . For each integer  $d$ , if  $1 \leq d \leq s$ ,*

$$k_{\max}(n, d, q; \pi) \leq \begin{cases} n - \lceil \log_q(V_q^n(l; \pi)) \rceil & \text{if } d = 2l + 1, \\ n - n_1 - \lceil \log_q(V_q^{n-n_1}(l-1; \pi')) \rceil & \text{if } d = 2l \geq 2, \end{cases}$$

where  $\pi' = [n_2][n_3] \dots [n_s]$ .

As the  $\pi$ -singleton bound and the  $\pi$ -Hamming bound cannot determine the explicit upper bound for  $k_{\max}(n, k, q; \pi)$ , we study other upper bounds.

In the next theorem we prove the  $\pi$ -Plotkin bound which is a generalization of the Plotkin upper bound for linear codes. That is the Plotkin bound for linear codes of length  $n$  is the  $[1]^n$ -Plotkin bound.

**Theorem 3.2.5 (Plotkin Bound, [2]).** For each linear  $[n, k, d]$  code over  $\mathbb{F}_q$ , the following holds:

$$d \leq \frac{nq^{k-1}(q-1)}{q^k-1}.$$

**Theorem 3.2.6 ( $\pi$ -Plotkin Bound).** For each  $[n, k, d; \pi]$  code  $\mathcal{C}$  over  $\mathbb{F}_q$  with type  $\pi = [n_1][n_2] \dots [n_s]$ , the following holds:

$$d \leq \frac{q^k(s - \sum_{i=1}^s \frac{1}{q^{n_i}})}{q^k - 1}. \quad (3.2.1)$$

*Proof.* Consider the double sum of distances

$$D := \sum_{c \in \mathcal{C}} \sum_{c' \in \mathcal{C}} d_{\pi}(c, c').$$

Since  $d \leq d_{\pi}(c, c')$  for all  $c \neq c' \in \mathcal{C}$ , we obtain

$$dq^k(q^k - 1) \leq D. \quad (3.2.2)$$

To determine an upper bound for  $D$ , we compute number  $D$  in different way. For each  $i \in \{1, 2, \dots, s\}$ , we denote the elements of  $\mathbb{F}_q^{n_i}$  by  $v_{i1}, v_{i2}, \dots, v_{iq^{n_i}}$ . For  $1 \leq i \leq s$  and  $1 \leq j \leq q^{n_i}$ , let  $D_{ji}$  denote the number of codewords which have their  $i^{\text{th}}$  block the element  $v_{ij}$ . In the term of this notation, we obtain

$$D = \sum_{i=1}^s \sum_{j=1}^{q^{n_i}} D_{ji}(q^k - D_{ji}).$$

Since  $\sum_{j=1}^{q^{n_i}} D_{ji} = q^k$ ,

$$\begin{aligned} D &= \sum_{i=1}^s \sum_{j=1}^{q^{n_i}} D_{ji}q^k - \sum_{i=1}^s \sum_{j=1}^{q^{n_i}} D_{ji}^2 \\ &= \sum_{i=1}^s q^{2k} - \sum_{i=1}^s \sum_{j=1}^{q^{n_i}} D_{ji}^2 \\ &= sq^{2k} - \sum_{i=1}^s \sum_{j=1}^{q^{n_i}} D_{ji}^2. \end{aligned} \quad (3.2.3)$$

For each  $i \in \{1, 2, \dots, s\}$ , the following is true:

$$\begin{aligned}
 0 &\leq \sum_{j=1}^{q^{n_i}} \sum_{t=j+1}^{q^{n_i}} (D_{ji} - D_{ti})^2 \\
 &= \sum_{j=1}^{q^{n_i}} \sum_{t=j+1}^{q^{n_i}} D_{ji}^2 - \sum_{j=1}^{q^{n_i}} \sum_{t=j+1}^{q^{n_i}} 2D_{ji}D_{ti} + \sum_{j=1}^{q^{n_i}} \sum_{t=j+1}^{q^{n_i}} D_{ti}^2 \\
 &= \sum_{j=1}^{q^{n_i}} (q^{n_i} - j)D_{ji}^2 - \sum_{j=1}^{q^{n_i}} \sum_{t=j+1}^{q^{n_i}} 2D_{ji}D_{ti} + \sum_{j=1}^{q^{n_i}} (j-1)D_{ji}^2 \\
 &= \sum_{j=1}^{q^{n_i}} (q^{n_i} - 1)D_{ji}^2 - \sum_{j=1}^{q^{n_i}} \sum_{t=j+1}^{q^{n_i}} 2D_{ji}D_{ti} \\
 &= q^{n_i} \sum_{j=1}^{q^{n_i}} D_{ji}^2 - \sum_{j=1}^{q^{n_i}} D_{ji}^2 - \sum_{j=1}^{q^{n_i}} \sum_{t=j+1}^{q^{n_i}} 2D_{ji}D_{ti}.
 \end{aligned}$$

This yields the inequality

$$\begin{aligned}
 q^{n_i} \sum_{j=1}^{q^{n_i}} D_{ji}^2 &\geq \sum_{j=1}^{q^{n_i}} D_{ji}^2 + \sum_{j=1}^{q^{n_i}} \sum_{t=j+1}^{q^{n_i}} 2D_{ji}D_{ti}. \\
 &= \left( \sum_{j=1}^{q^{n_i}} D_{ji} \right)^2 \\
 &= q^{2k}.
 \end{aligned}$$

Thus

$$\sum_{j=1}^{q^{n_i}} D_{ji}^2 \geq q^{2k-n_i}. \tag{3.2.4}$$

From (3.2.3) and (3.2.4), we obtain

$$\begin{aligned}
 D &= sq^{2k} - \sum_{i=1}^s \sum_{j=1}^{q^{n_i}} D_{ji}^2 \\
 &\leq sq^{2k} - \sum_{i=1}^s (q^{2k-n_i}) \\
 &= sq^{2k} - q^{2k} \sum_{i=1}^s \frac{1}{q^{n_i}} \\
 &= q^{2k} \left( s - \sum_{i=1}^s \frac{1}{q^{n_i}} \right). \tag{3.2.5}
 \end{aligned}$$

Combining bounds in (3.2.2) and (3.2.5) we conclude that

$$dq^k(q^k - 1) \leq D \leq q^{2k}(s - \sum_{i=1}^s \frac{1}{q^{n_i}}).$$

Hence

$$d \leq \frac{q^k(s - \sum_{i=1}^s \frac{1}{q^{n_i}})}{q^k - 1}.$$

□

The  $\pi$ -Plotkin bound can formulate upper bounds for both the maximum dimension  $k_{\max}(n, d, q; \pi)$  and the largest minimum  $\pi$ -distance  $d_{\max}(n, k, q; \pi)$ .

**Corollary 3.2.7.** *Let  $q$  be a prime power and  $\pi = [n_1][n_2] \dots [n_s]$  a partition of a positive integer  $n$ . For each positive integer  $k \leq n$ ,*

$$d_{\max}(n, k, q; \pi) \leq \lfloor \frac{q^k(s - \sum_{i=1}^s \frac{1}{q^{n_i}})}{q^k - 1} \rfloor.$$

**Corollary 3.2.8.** *Let  $q$  be a prime power and  $\pi = [n_1][n_2] \dots [n_s]$  a partition of a positive integer  $n$ . For each integer  $d$ , if  $s - \sum_{i=1}^s \frac{1}{q^{n_i}} < d \leq s$ , then*

$$k_{\max}(n, d, q; \pi) \leq \lfloor \log_q \left( \frac{d}{d - s + \sum_{i=1}^s \frac{1}{q^{n_i}}} \right) \rfloor.$$

*Proof.* Since

$$d \leq \frac{q^k(s - \sum_{i=1}^s \frac{1}{q^{n_i}})}{(q^k - 1)},$$

$$q^k d - d \leq q^k(s - \sum_{i=1}^s \frac{1}{q^{n_i}}).$$

That is

$$q^k \leq \frac{d}{d - s + \sum_{i=1}^s \frac{1}{q^{n_i}}}.$$



As a result,

$$k_{\max}(n, d, q; \pi) \leq \lfloor \log_q \left( \frac{d}{d - s + \sum_{i=1}^s \frac{1}{q^{n_i}}} \right) \rfloor.$$

□

**Theorem 3.2.9.** *The equality holds in (3.2.1) provided that*

- i) the  $\pi$ -distance between any two distinct codewords equals a constant, and*
- ii) for each block  $i$ , each element in  $\mathbb{F}_q^{n_i}$  appears exactly often.*

*Proof.* By *i*), the equality in (3.2.1) holds, that is,

$$D = dq^k(q^k - 1). \quad (3.2.6)$$

By *ii*), for  $1 \leq i \leq s$  and  $1 \leq j \leq q^{n_i}$ ,

$$D_{ij} = \frac{q^k}{q^{n_i}}.$$

Thus

$$\begin{aligned} D &= \sum_{i=1}^s \sum_{j=1}^{q^{n_i}} \frac{q^k}{q^{n_i}} \left( q^k - \frac{q^k}{q^{n_i}} \right) \\ &= \sum_{i=1}^s q^{n_i} \frac{q^k}{q^{n_i}} \left( q^k - \frac{q^k}{q^{n_i}} \right) \\ &= \sum_{i=1}^s q^k \left( q^k - \frac{q^k}{q^{n_i}} \right) \\ &= \sum_{i=1}^s q^{2k} - \sum_{i=1}^s \frac{q^{2k}}{q^{n_i}} \\ &= sq^{2k} - q^{2k} \sum_{i=1}^s \frac{1}{q^{n_i}} \\ &= q^{2k} \left( s - \sum_{i=1}^s \frac{1}{q^{n_i}} \right). \end{aligned} \quad (3.2.7)$$

Combining (3.2.6) and (3.2.7),

$$dq^k(q^k - 1) = D = q^{2k} \left( s - \sum_{i=1}^s \frac{1}{q^{n_i}} \right).$$

Hence

$$d = \frac{q^k(s - \sum_{i=1}^s \frac{1}{q^{n_i}})}{(q^k - 1)}$$

as required.  $\square$

Now, we give an example of a linear error-block code attaining the  $\pi$ -Plotkin bound.

**Example 3.2.1.** Let

$$\mathcal{C} = \{00|0|0|0|0|0|0, 10|1|0|1|0|1|1, 01|0|1|0|1|1|1, 11|1|1|1|1|0|0\}.$$

Then  $\mathcal{C}$  is an  $[8, 2, 5; \pi]$  with type  $\pi = [2][1]^6$  over  $\mathbb{F}_2$ . Since

$$5 = \frac{2^2[7 - (\frac{1}{4} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2})]}{2^2 - 1},$$

$\mathcal{C}$  attains the  $\pi$ -Plotkin bound. It is easy to see that  $\mathcal{C}$  satisfies both conditions in Theorem 3.2.9.

### 3.3 Applications

Our ultimate goal is to find optimal codes. We first search maximal dimension codes. In section 2.1, two lower bounds for  $k_{\max}(n, d, q; \pi)$  were studied in Corollaries 3.1.3 and 3.1.6. Both bounds are computed and the maximum one is chosen. On the other hand, the minimum among upper bounds is obtained by Corollaries 3.2.2, 3.2.4 and 3.2.8 is selected. For fixed  $n$ ,  $d$  and  $\pi$ , a maximal dimension linear error-block code is rewarded when these two candidates are coincide.

Table 3.3.1 displays lower bounds and an upper bounds for  $k_{\max}(8, d, 2; \pi)$  of linear error-block codes with given partitions and minimum distances.

$\pi \backslash d$	1	2	3	4	5	6	7	8
[8]	$8_{GS}$							
[7][1]	$8_{GS}$	1						
[6][2]	$8_{GS}$	$2_{GS}$						
[6][1][1]	$8_{GS}$	$2_{GS}$	1					
[5][3]	$8_{GS}$	$3_{GS}$						
[5][2][1]	$8_{GS}$	$3_{GS}$	1					
[5][1][1][1]	$8_{GS}$	$3_{GS}$	$2_{VS}$	1				
[4][4]	$8_{GS}$	$4_{GS}$						
[4][3][1]	$8_{GS}$	$4_{GS}$	1					
[4][2][2]	$8_{GS}$	$4_{GS}$	$2_{GS}$					
[4][2][1][1]	$8_{GS}$	$4_{GS}$	$2_{GS}$	1				
[4][1][1][1][1]	$8_{GS}$	$4_{GS}$	$3_{VS}$	1	1			
[3][3][2]	$8_{GS}$	$4_G - 5_S$	$2_{GS}$					
[3][3][1][1]	$8_{GS}$	$4_G - 5_S$	$2_{GS}$	1				
[3][2][2][1]	$8_{GS}$	$5_{GS}$	$2_G - 3_S$	1				
[3][2][1][1][1]	$8_{GS}$	$5_{GS}$	$2_G - 3_S$	$2_{VS}$	1			
[3][1] <sup>5</sup>	$8_{GS}$	$5_{GS}$	$4_{VS}$	$2_{VH}$	1	1		
[2] <sup>4</sup>	$8_{GS}$	$5_G - 6_S$	$2_G - 4_S$	$1_V - 2_S$				
[2] <sup>3</sup> [1] <sup>2</sup>	$8_{GS}$	$5_G - 6_S$	$3_G - 4_S$	$1_V - 2_S$	1			
[2] <sup>2</sup> [1] <sup>4</sup>	$8_{GS}$	$5_G - 6_S$	$3_G - 4_S$	$2_V - 3_S$	1	1		
[2][1] <sup>6</sup>	$8_{GS}$	$5_G - 6_S$	$4_{VH}$	$2_V - 3_H$	$1_V - 2_H$	1	1	
[1] <sup>8</sup>	$8_{GS}$	$7_{VS}$	$4_{VH}$	$3_V - 4_H$	$1_V - 2_H$	1	1	1

Table 3.3.1: Lower and upper bounds for  $\mathbf{k}_{\max}(8, d, 2; \pi)$ 

For given  $d$  and  $\pi$ , Table 3.3.1 shows either the exact value of  $\mathbf{k}_{\max}(8, d, 2; \pi)$ , or the interval consisting of a lower bound and an upper bound. Subscripts are used to indicate which rule led to the bound. The subscripts  $G$ ,  $V$ ,  $S$ ,  $P$  and  $H$  stand for the  $\pi$ -Gilbert,  $\pi$ -Gilbert-Varshamov,  $\pi$ -singleton,  $\pi$ -Plotkin and  $\pi$ -Hamming bounds, respectively. For example, the table entry  $d = 3$  and  $\pi = [3][1]^5$  reads  $4_{VS}$  which stands for the exact value  $\mathbf{k}_{\max}(8, 3, 2; [3][1]^5) = 4$ ;  $4 \leq \mathbf{k}_{\max}(8, 3, 2; [3][1]^5)$  by the  $\pi$ -Gilbert-Varshamov bound and  $\mathbf{k}_{\max}(8, 3, 2; [3][1]^5) \leq 4$  due to the  $\pi$ -singleton bound. For the partition  $[2]^4$ , the interval  $5_G - 6_S$  stands for two bounds  $5 \leq \mathbf{k}_{\max}(8, 2, 2; [2]^4)$  by the  $\pi$ -Gilbert bound and  $\mathbf{k}_{\max}(8, 2, 2; [2]^4) \leq 6$  due to the  $\pi$ -singleton bound.

Similarly, to obtain maximal minimum  $\pi$ -distance codes, we compute bounds for  $d_{\max}(n, k, q; \pi)$ . Maximal minimum  $\pi$ -distance codes can be obtained whenever a lower bound for  $d_{\max}(n, k, q; \pi)$  meets its upper bound. From Theorems 3.1.2, 3.1.4, 3.2.1 and 3.2.3, the explicit lower and upper bounds for  $d_{\max}(n, k, q; \pi)$  cannot be derived. We use a numerical computation to compute these values. Now, we give examples of lower and upper bounds for  $d_{\max}(8, k, 2; \pi)$  of linear error-block codes with given partitions and dimensions as shown in Table 3.3.2.

$\pi \backslash k$	1	2	3	4	5	6	7	8
[8]	1	1	1	1	1	1	1	1
[7][1]	$2_{GH}$	1	1	1	1	1	1	1
[6][2]	$2_{GS}$	$2_{GH}$	1	1	1	1	1	1
[6][1][1]	$3_{VS}$	$2_{GH}$	1	1	1	1	1	1
[5][3]	$2_{GS}$	$2_{GS}$	$2_{GH}$	1	1	1	1	1
[5][2][1]	$3_{GS}$	$2_{GS}$	$2_{GH}$	1	1	1	1	1
[5][1][1][1]	$4_{VH}$	$3_{VS}$	$2_{GH}$	1	1	1	1	1
[4][4]	$2_{GS}$	$2_{GS}$	$2_{GS}$	$2_{GH}$	1	1	1	1
[4][3][1]	$3_{GS}$	$2_{GS}$	$2_{GS}$	$2_{GH}$	1	1	1	1
[4][2][2]	$3_{GS}$	$3_{GS}$	$2_{GS}$	$2_{GH}$	1	1	1	1
[4][2][1][1]	$4_{VS}$	$3_{GS}$	$2_{GS}$	$2_{GH}$	1	1	1	1
[4][1][1][1][1]	$5_{VS}$	$3_{VP}$	$3_{VS}$	$2_{GH}$	1	1	1	1
[3][3][2]	$3_{GS}$	$3_{GS}$	$2_{GS}$	$2_{GH}$	$1_G - 2_H$	1	1	1
[3][3][1][1]	$4_{VS}$	$3_{GS}$	$2_{GS}$	$2_{GH}$	$1_G - 2_H$	1	1	1
[3][2][2][1]	$4_{GS}$	$3_{GS}$	$2_G - 3_S$	$2_{GS}$	$2_{GH}$	1	1	1
[3][2][1][1][1]	$5_{VS}$	$4_{VH}$	$2_G - 3_S$	$2_{GS}$	$2_{GH}$	1	1	1
[3][1] <sup>5</sup>	$6_{VH}$	$4_{VP}$	$3_{VP}$	$3_{VS}$	$2_{GH}$	1	1	1
[2] <sup>4</sup>	$4_{GS}$	$3_G - 4_H$	$2_G - 3_S$	$2_G - 3_S$	$2_{GH}$	$1_G - 2_H$	1	1
[2] <sup>3</sup> [1] <sup>2</sup>	$5_{VS}$	$3_G - 4_S$	$3_{GS}$	$2_G - 3_S$	$2_{GH}$	$1_G - 2_H$	1	1
[2] <sup>2</sup> [1] <sup>4</sup>	$6_{VS}$	$4_{VP}$	$3_G - 4_H$	$2_G - 3_S$	$2_{GH}$	$1_G - 2_H$	1	1
[2][1] <sup>6</sup>	$7_{VS}$	$4_V - 5_P$	$3_V - 4_H$	$3_V - 4_H$	$2_{GH}$	$1_G - 2_H$	1	1
[1] <sup>8</sup>	$8_{VH}$	$4_V - 5_P$	$4_{VH}$	$3_V - 4_H$	$2_{VH}$	$2_{VH}$	$2_{VH}$	1

Table 3.3.2: Lower and upper bounds for  $d_{\max}(8, k, 2; \pi)$ .

For given  $k$  and  $\pi$ , Table 3.3.2 shows either the coincident bound of  $d_{\max}(8, k, 2; \pi)$ , or the interval. Subscripts are used to indicate which rule led to the bound as the previous. For the partition  $[3][1]^5$ ,  $4_{VP}$  stands for the exact value  $d_{\max}(8, 2, 2; [3][1]^5)$



which is confirmed by the  $\pi$ -Gilbert-Varsharmov lower bound and the  $\pi$ -Plotkin upper bound. For the partition  $[2]^2[1]^4$ , the interval  $3_G - 4_H$  shows a lower bound and upper bound for  $d_{\max}(8, 3, 2; [2]^2[1]^4)$  due to the  $\pi$ -Gilbert bound and the  $\pi$ -Hamming bound, respectively.