CHAPTER IV

MODIFICATIONS OF LINEAR ERROR-BLOCK CODES

In this chapter, we restate propagation rules that proposed in [1], [3] and [6] for linear codes in terms of linear error-block codes. These rules are then applied to construct more efficient linear error-block codes based on the codes whose existences are guaranteed by lower bounds formulated in previous chapter for purpose of enlarging the minimum $\pi-$distance or the dimension of codes when certain parameters are fixed.

4.1 Methods for Modifying Linear Error-Block Codes

Linear error-block codes are linear codes viewing codewords with respect to a partition of the length of codewords. Hence all propagation rules using to construct linear codes can be applied for linear error-block codes. In order to obey the definition giving in [3], we must be aware of the descending sizes of blocks which is a partition the codewords. Equivalently, permutations on the length of new codewords are required.

Given partitions $\pi = [n_1][n_2]\ldots[n_s]$ and $\gamma = [m_1][m_2]\ldots[m_r]$ of positive integers n and m, respectively. Naturally, there exist a permutation ρ on $r+s$ and $l_1 \geq l_2 \geq \cdots \geq l_{s+r} \in \mathbb{N}$ such that

$$\pi = [l_{\rho(1)}][l_{\rho(2)}]\cdots[l_{\rho(s)}] \text{ and } \gamma = [l_{\rho(s+1)}][l_{\rho(s+2)}]\cdots[l_{\rho(s+r)}].$$

Hence, $[l_1][l_2]\dots[l_{s+r}]$ forms a partition of $n+m$. This partition is called the **partition of $n+m$ induced by** π and γ and denoted $\pi \vee \gamma$.

In particular, for each positive integer t,

$$\pi^t := \underbrace{\pi \vee \pi \vee \cdots \vee \pi}_{t \text{ copies}} = [n_1]^t[n_2]^t\dots[n_s]^t$$

forms a partition of tn.

Example 4.1.1. Let $\pi = [4][2][1][1]$ and $\gamma = [3][1][1]$ be partitions of 8 and 5, respectively. Then $\pi \vee \gamma = [4][3][2][1][1][1][1]$ is a partition of 13 induced by π and γ. Similarly, $\pi^2 = [4]^2[2]^2[1]^2[1]^2$ and $\pi^3 = [4]^3[2]^3[1]^3[1]^3$ form partitions of 16 and 24, respectively.

With respect to partitions π and γ, each pair of words $u \in \mathbb{F}_q^n$ and $v \in \mathbb{F}_q^m$ induces a word in $\mathbb{F}_q^{n+m}$ with type $\pi \vee \gamma$ in natural way. To be more precise, let ρ be a permutation on $r+s$ and $l_1 \geq l_2 \geq \cdots \geq l_{s+r} \in \mathbb{N}$ such that $\pi = [l_{\rho(1)}][l_{\rho(2)}]\dots[l_{\rho(s)}]$ and $\gamma = [l_{\rho(s+1)}][l_{\rho(s+2)}]\dots[l_{\rho(s+r)}]$. Then the word in $\mathbb{F}_q^{n+m}$ induced by $u_{\rho(1)}u_{\rho(2)}\dots u_{\rho(s)} \in \mathbb{F}_q^n$ and $u_{\rho(s+1)}u_{\rho(s+2)}\dots u_{\rho(s+r)} \in \mathbb{F}_q^m$ is $u_1u_2\dots u_su_{s+1}u_{s+2}\dots u_{s+r}$. It can be easily seen from the definition that this process does not cause any change in the minimum distance of a code. Here for simplicity of modifications, the following constructions will be left out the permutation part.

From a diagonal concatenation in [2], the statement is rewritten with respect to a partition of the length of codewords as follows:

Theorem 4.1.1. *Let* $\mathbf{G}$ *and* $\mathbf{G}'$ *be generator matrices for an* $[n,k,d;\pi]$ *code and an* $[n',k,d';\pi']$ *code over* $\mathbb{F}_q$*, respectively. Then the code* $\{u[\mathbf{G}|\mathbf{G}'] \mid u \in \mathbb{F}_q^k\}$ *is an* $[n+n',k;\pi\vee\pi']$ *code with minimum* $\pi\vee\pi'-$*distance at least* $d+d'$.

Theorem 4.1.1 is applied in the next two examples to fill up some gaps for maximal minimum $\pi-$distance codes in Table 3.3.2.

Example 4.1.2. Let

$$\mathbf{G} = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right] \text{ and } \mathbf{G}' = \left[\begin{array}{cc|c|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{array}\right]$$

be generator matrices of a $[4, 2, 2; [2]^2]$ code and a $[4, 2, 2; [2][1]^2]$ code, respectively. By Theorem 4.1.1,

$$[\mathbf{G}|\mathbf{G}'] = \left[\begin{array}{cc|cc|cc|c|c} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

generates an $[8, 2, 4; [2]^3[1]^2]$ code over $\mathbb{F}_2$. The $[8, 2, 4; [2]^3[1]^2]$ code is optimal since the $\pi-$singleton upper bound indicates that $\boldsymbol{d}_{\max}(8, 2, 2; [2]^3[1]^2) \leq 4$.

Example 4.1.3. From Table 3.3.2, we conclude from the $\pi-$Gilbert bound and the $\pi-$Hamming bound that

$$2 \leq \boldsymbol{d}_{\max}(8, 3, 2; [3][2][1]^3) \leq 3.$$

To determine the value of $\boldsymbol{d}_{\max}(n, k, q; \pi)$, it suffices to prove the existence of an $[8, 3, 3; [3][2][1]^3]$ code. This can be done by applying Theorem 4.1.1 to $[5, 3, 2; [2][1]^3]$ and $[3, 3, 1; [3]]$ codes whose existences are guaranteed by the $\pi-$Gilbert bound.

The method employed here is a generalization of $u|(u + v)$-construction in [6]. We reargue the statement corresponding to sizes of blocks and then obtained a more efficient linear error-block code.

Theorem 4.1.2. *Let C and C' be $[n, k, d; \pi]$ code and $[n, k', d'; \pi]$ code over $\mathbb{F}_q$, respectively. Then the code $\{c|(c + c') \mid c \in C \text{ and } c' \in C'\}$ is an $[2n, k + k', \min\{2d, d'\}; \pi^2]$ code over $\mathbb{F}_q$.*

Next corollary follows directly from Theorem 4.1.2 by choosing

$$C' = \{\underbrace{00\ldots0}_{n \text{ copies}}, \underbrace{11\ldots1}_{n \text{ copies}}\}.$$

Corollary 4.1.3. *Let $\mathcal{C}$ be a binary $[n, k, d; \pi = [n_1][n_2] \ldots [n_s]]$ code. Then there exists a binary $[2n, k+1, \min\{s, 2d\}; \pi^2]$ code.*

Remark 4.1.1. Let $\mathbf{G}$ and $\mathbf{G}'$ be generator matrices for $\mathcal{C}$ and $\mathcal{C}'$ codes, respectively. Then a generator matrix for the code $\{c|(c+c') \mid c \in \mathcal{C} \text{ and } c' \in \mathcal{C}'\}$ is

$$\begin{bmatrix} \mathbf{G} & \mathbf{G} \\ 0 & \mathbf{G}' \end{bmatrix}.$$

Example 4.1.4. The $\pi-$Gilbert-Varshamov bound guarantees the existences of an $[6, 3, 3; [2][1]^4]$ code and an $[6, 1, 5; [2][1]^4]$ code over $\mathbb{F}_2$. Theorem 4.1.2 yields an $[12, 4, 5; [2]^2[1]^8]$ code over $\mathbb{F}_2$. This code is optimal since the $\pi-$Plotkin bound demonstrates that $\boldsymbol{d}_{\max}(12, 4, 2;) \leq 5$.

Due to the construction X in [1], a linear error-block code with large minimum $\pi-$distance can be obtained as follows :

Theorem 4.1.4. *Let A_1, A_2 and A_3 be $[n, k_1, d_1; \pi]$, $[n, k_2, d_2; \pi]$ and $[n', k_3, d_3; \pi']$ codes over $\mathbb{F}_q$, respectively, such that A_2 is a subspace of A_1. If $k_1 - k_2 \leq k_3$, then there exists an $[n+n', k_1; \pi \vee \pi']$ code over $\mathbb{F}_q$ with minimum $\pi \vee \pi'-$distance at least $\min\{d_1 + d_3, d_2\}$.*

Next two examples present constructions of more efficient linear error-block codes by using Theorem 4.1.4 in terms of generator matrices.

Example 4.1.5. The binary $[7, 4, 2; [2][2][1]^3]$ code A_1 generated by

$$\mathbf{G}_1 = \left[\begin{array}{cc|cc|c|c|c} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{array}\right].$$

A_1 contains a $[7,3,3;[2]^2[1]^3]]$ code A_2 as a subspace with generator matrix

$$\mathbf{G}_2 = \left[\begin{array}{cc|cc|c|c|c} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right].$$

Together with the binary $[1,1,1;[1]]$ code A_3, generated by $\mathbf{G}_3 = [\ 1\ ]$. By Theorem 4.1.4, an $[8,4,3;[2]^2[1]^4]$ code with generator matrix

$$\left[\begin{array}{cc|cc|cc|c|c} 1 & 0 & 1 & 1 & 0 & 0 & 1 & \mathbf{0} \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & \mathbf{0} \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & \mathbf{0} \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{array}\right].$$

can be obtained. Moreover, this code is optimal since the $\pi-$singleton bound yields $\boldsymbol{d}_{\max}(8,4,2;[2]^2[1]^4) \leq 3$.

Example 4.1.6. The $\pi-$Gilbert bound and the $\pi-$Plotkin bound indicate that $4_G \leq \boldsymbol{d}_{\max}(14,4;[2]^4[1]^6) \leq 6_P$. Let A_1 and A_3 be a $[10,4;[2]^4[1]^2]$ code and a $[4,2;[1]^4]$ code over $\mathbb{F}_2$ with generator matrices

$$\mathbf{G}_1 = \left[\begin{array}{cc|cc|cc|cc|c|c} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

and

$$\mathbf{G}_3 = \left[\begin{array}{c|c|c|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right], \text{ respectively.}$$

It follows that $d_{[2]^4[1]^2}(A_1) = 3$ and $d_{[1]^4}(A_3) = 2$. Choose A_2 to be an $[10,2,[2]^4[1]^2]$ generated by

$$\mathbf{G}_2 = \left[\begin{array}{cc|cc|cc|cc|c|c} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right].$$

Thus $d_{[2]^4[1]^2}(A_2) = 5$. Clearly, A_2 A_1 and A_3 satisfy conditions in Theorem 4.1.4. Then a $[14, 4, 5; [2]^4[1]^6]$ code $\mathcal{C}$ with a generator matrix

$$\mathbf{G} = \left[\begin{array}{cc|cc|cc|cc|c|c|c|c|c|c} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{array}\right]$$

can be obtained. As $d_{[2]^4[1]^6}(\mathcal{C}) = 5 \leq 6$, this code may not be optimal. However, the minimum $[2]^4[1]^6-$distance is improved.

Example 4.1.7. It follows from Theorem 3.2.3 that $\boldsymbol{d}_{\max}(8, 3, 2; [2][1]^6) \leq 4$. To search for the exact value, we apply Theorem 4.1.4 where $A_1 = \{00|0|0|0$, $11|1|1|1$, $01|1|0|0$, $10|1|1|0$, $10|0|1|1$, $01|0|0|1$, $11|0|1|0$, $00|1|0|1\}$, $A_2 = \{00|0|0|0$, $11|1|1|1\}$ and $A_3 = \{0|0|0, 1|0|1, 0|1|1, 1|1|0\}$. In this way an $[8, 3, 4; [2][1]^6]$ code over $\mathbb{F}_2$ is obtained which implies that $\boldsymbol{d}_{\max}(8, 3, 2; [2][1]^6) = 4$.

Using a concept of concatenated code in [6], we state a new version which depends on sizes of blocks.

Theorem 4.1.5. *Let A be an $[N, K, D]$ code over $\mathbb{F}_{q^m}$ and B be an $[n, m, d; \pi]$ code over $\mathbb{F}_q$. Then there exists an $[Nn, Km; \pi^N]$ code over $\mathbb{F}_q$ with minimum π^N-distance at least Dd.*

Example 4.1.8. Both a $[3, 1, 3]$ code A over $\mathbb{F}_4$ and a $[5, 2, 3; [2][1]^3]$ code B over $\mathbb{F}_2$ can be construct using method in the proof of the $\pi-$Gilbert-Varshamov bound. A $[15, 2, 9; [2]^3[1]^9]$ code over $\mathbb{F}_2$ is obtained by applying Theorem 4.1.5 to codes A and B. As the $\pi-$Plotkin bound show that $\boldsymbol{d}_{\max}(15, 2, 2; [2]^3[1]^9) \leq 9$, this code is optimal.

4.2 Applications

The examples after each construction rule not only demonstrate how the rule can be applied but also offer optimal codes. Consequently, Table 3.3.1 is improved as shown in Table 4.2.1. The improvements between corresponding tables are marked by boldface numbers.

π \ k	1	2	3	4	5	6	7	8
[3][2][1][1][1]	5	4	**3**	2	2	1	1	1
[3][1][1][1][1][1]	6	4	3	3	2	1	1	1
[2][2][2][2]	4	**4**	$2_G - 3_S$	$2_G - 3_S$	2	$1_G - 2_H$	1	1
[2][2][2][1][1]	5	**4**	3	$2_G - 3_S$	2	$1_G - 2_H$	1	1
[2][2][1][1][1][1]	6	4	$3_G - 4_H$	**3**	2	$1_G - 2_H$	1	1
[2][1][1][1][1][1][1]	7	**5**	**4**	$3_V - 4_H$	2	$1_G - 2_H$	1	1
[1][1][1][1][1][1][1][1]	8	**5**	4	**4**	2	2	2	1

Table 4.2.1: Improved bounds for $\boldsymbol{d}_{\max}(8, k, 2; \pi)$.

Moreover, a lower bound for $\boldsymbol{k}_{\max}(8, d, 2; \pi)$ can be improved by retabulating Table 4.2.1. Bold dimensions show the improvements which are optimal.

π \ d	1	2	3	4	5	6	7	8
[3][2][1][1][1]	8	5	**3**	2	1			
[3][1][1][1][1][1]	8	5	4	2	1	1		
[2][2][2][2]	8	$5_G - 6_S$	$2_G - 4_S$	**2**				
[2][2][2][1][1]	8	$5_G - 6_S$	$3_G - 4_S$	**2**	1			
[2][2][1][1][1][1]	8	$5_G - 6_S$	**4**	$2_V - 3_S$	1	1		
[2][1][1][1][1][1][1]	8	$5_G - 6_S$	4	**3**	**2**	1	1	
[1][1][1][1][1][1][1][1]	8	7	4	**4**	**2**	1	1	1

Table 4.2.2: Improved bounds for $\boldsymbol{k}_{\max}(8, d, 2; \pi)$.

The following tables illustrate new minimum $\pi-$ distances which are enlarged from existing codes in last two columns (of the tables) by applying the construction rules in the previous section. The subscripts indicate the origins of codes. The subscripts G, V, S, P, H stand for the $\pi-$Gilbert, $\pi-$Gilbert-Varshamov, $\pi-$singleton, $\pi-$Plotkin, $\pi-$Hamming bound and T means Table 3.3.1. The only code without subscript in Table 4.2.4 is the code obtained previously in the same table. Observe that these tables attract our attention in this sense that most of them are optimal. These new optimal codes are the codes whose minimum distances meet the corresponding upper bounds for $\boldsymbol{d}_{\max}(n, k, 2; \pi)$.

n	π	k	$\boldsymbol{d}_{\max}(n,k,2;\pi)$	new d	$\mathcal{C}$	$\mathcal{C}'$
12	$[2]^2[1]^8$	4	$4_V - 5_P$	5	$[6,3,3;[2][1]^4]_V$	$[6,1,5;[2][1]^4]_V$
16	$[3]^2[2]^4[1]^2$	6	$3_G - 5_S$	4	$[8,4,2;[3][2]^2[1]]_G$	$[8,1,4;[3][2]^2[1]]_G$
	$[3]^2[1]^{10}$	4	$5_V - 7_P$	6	$[8,3,3;[3][1]^5]_V$	$[8,1,6;[3][1]^5]_V$
		5	$5_V - 6_P$	6	$[8,4,3;[3][1]^5]_V$	$[8,1,6;[3][1]^5]_V$
	$[2]^6[1]^4$	7	$3_G - 5_S$	4	$[8,5,2;[2]^3[1]^2]_G$	$[8,2,4;[2]^3[1]^2]_T$
	$[2]^4[1]^8$	5	$4_G - 7_P$	6	$[8,4,3;[2]^2[1]^4]_T$	$[8,1,6;[2]^2[1]^4]_V$
		7	$3_G - 6_H$	4	$[8,5,2;[2]^2[1]^4]_G$	$[8,2,4;[2]^2[1]^4]_V$
	$[2]^2[1]^{12}$	4	$4_G - 7_P$	7	$[8,3,4;[2][1]^6]_T$	$[8,1,7;[2][1]^6]_V$
		5	$3_G - 6_H$	6	$[8,4,3;[2][1]^6]_V$	$[8,1,7;[2][1]^6]_V$

Table 4.2.3: Improved bounds for $\boldsymbol{d}_{\max}(n, k, 2; \pi)$ obtained from Theorem 4.1.2.

n	π	k	$d_{\max}(n,k,2;\pi)$	new d	$\mathcal{C}$	$\mathcal{C}'$
8	$[3][2][1]^3$	3	$2_G - 3_S$	3	$[5,3,2;[2][1]^3]_G$	$[3,3,1;[3]]_G$
	$[2]^4$	2	$3_G - 4_H$	4	$[4,2,2;[2]^2]_G$	$[4,2,2;[2]^2]_G$
10	$[2]^4[1]^2$	2	$4_G - 5_S$	5	$[8,2,4;[2]^4]$	$[2,2,1;[1]^2]_G$
12	$[3]^2[1]^6$	3	$4_V - 5_P$	5	$[9,3,4;[3][1]^6]_V$	$[3,3,1;[3]]_G$
16	$[3]^4[1]^4$	3	$5_G - 6_S$	6	$[10,3,4;[3]^2[1]^4]_V$	$[6,3,2;[3]^2]_G$
	$[3]^2[1]^{10}$	3	$6_V - 7_P$	7	$[10,3,4;[3]^2[1]^4]_V$	$[6,3,3;[1]^6]_V$

Table 4.2.4: Improved bounds for $d_{\max}(n,k,2;\pi)$ obtained from Theorem 4.1.1.

$\eta = Nn$	$\pi = \omega^N$	k	$d_{\max}(\eta,k,2;\pi)$	new d	$[N,K,D]_{/\mathbb{F}_{2^2}}$	$[n,2,d;\omega]_{/\mathbb{F}_2}$
12	$[2]^6$	2	$5_G - 6_S$	6	$[3,1,3]_V$	$[4,2,2;[2]^2]_G$
	$[1]^{12}$	4	$5_V - 6_H$	6	$[4,2,3]_V$	$[3,2,2;[1]^3]_V$
		6	$3_V - 4_H$	4	$[4,3,2]_V$	$[3,2,2;[1]^3]_V$
15	$[3]^3[2]^3$	2	$5_G - 6_S$	6	$[3,1,3]_V$	$[5,2,2;[3][2]]_G$
	$[2]^3[1]^9$	2	$7_V - 9_P$	9	$[3,1,3]_V$	$[5,2,3;[2][1]^3]_V$
		4	$5_V - 7_P$	6	$[3,2,2]_V$	$[5,2,3;[2][1]^3]_V$
20	$[3]^4[2]^4$	4	$5_G - 6_P$	6	$[4,2,3]_V$	$[5,2,2;[3][2]]_G$
	$[2]^4[1]^{12}$	4	$7_V - 9_P$	9	$[4,2,3]_V$	$[5,2,3;[2][1]^3]_V$
	$[1]^{20}$	4	$8_V - 10_P$	9	$[4,2,3]_V$	$[5,2,3;[1]^5]_V$

Table 4.2.5: Improved bounds for $d_{\max}(n,k,2;\pi)$ obtained from Theorem 4.1.5.