World Applied Sciences Journal 14(12):1900-1907, 2011
ISSN 1818-4952

Linear Partition Codes in Arihant Metric

Sapna Jain

[1] Department of Mathematics, University of Delhi, Delhi 110 007, India

sapnajain@gmx.com

Abstract: Linear partition codes in Arihant metric are block metric codes and are a generalization of the classical error correcting codes endowed with the Lee metric [1, 2, 3] and has applications over non binary channel. In this paper, we formulate the concept of a linear partition Arihant code (LPA code) and derive results pertaining to error detection and error correction capabilities of these codes.

Key words: Linear codes, Lee metric, Error block code

INTRODUCTION

Feng, Xu and Hickernell [4] initiated the concept of linear partition block code which is a natural generalization of the classical Hamming metric and is suitable for binary channels since any digital change in one block place is a single error, no matter what the magnitude of the change is. Also, we know that classical Lee metric codes [1, 2, 3] are more suitable for non binary channels as a digital change of "$\pm t$" in one place contributes "t" errors. Motivated by the idea to have linear partition block code endowed with a metric generalizing the classical Lee metric, we formulate the concept of a linear partition code equipped with Arihant metric which is a block metric generalizing the classical Lee metric and the block metric introduced by Feng et al. [4]. We derive basic results for linear partition Arihant codes including various upper and lower bounds on their parameters and study their error detection and error correction capabilities. Linear partition Arihant codes will find applications in phase-modulation and in the construction of block Nega-cyclic codes and are suitable for non binary channels.

2. DEFINITIONS AND NOTATIONS

Let q, n be positive integers with $q > 1$. Let $\mathbf{F}_q$ be the ring of integers modulo q. Let $\mathbf{F}_q^n$ be the set of all n-tuples over $\mathbf{F}_q$. Then $\mathbf{F}_q^n$ is a module over $\mathbf{F}_q$. For q prime, $\mathbf{F}_q$ becomes a field and $\mathbf{F}_q^n$ becomes a vector space over $\mathbf{F}_q$. A partition P of the positive integer n is defined as

$$\begin{aligned} P \quad : \quad & n = n_1 + n_2 \cdots + n_s \quad \text{where} \\ & 1 \leq n_1 \leq n_2 \leq \cdots \leq n_s, s \geq 1. \end{aligned}$$

The partition P is denoted as

$$P : n = [n_1][n_2] \cdots [n_s].$$

In the case, when

$$\begin{aligned} P : n \quad = \quad & \underbrace{[m_1] \cdots [m_1]}_{l_1\text{- copies}} \underbrace{[m_2] \cdots [m_2]}_{l_2\text{- copies}} \\ & \cdots \underbrace{[m_r] \cdots [m_r]}_{l_r\text{- copies}}, \end{aligned}$$

we write

$$P : n = [m_1]^{l_1}[m_2]^{l_2} \cdots [m_r]^{l_r},$$

where $m_1 < m_2 < \cdots < m_r$.

Given a partition $P : n = [n_1][n_2] \cdots [n_s]$ of the positive integer n, the module space $\mathbf{F}_q^n$ over $\mathbf{F}_q$ can be viewed as a direct sum

$$\begin{aligned} \mathbf{Z}_q^n \quad = \quad & \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{ns}, \\ & \text{or} \\ V \quad = \quad & V_1 \oplus V_2 \oplus \cdots V_s, \end{aligned}$$

where $V = \mathbf{Z}_q^n$ and $V_i = \mathbf{Z}_q^{n_1}$ for all $1 \leq i \leq s$.

Consequently, each vector $v \in \mathbf{Z}_q^n$ can be uniquely written as $v = (v_1, v_2, \cdots, v_s)$ where $v_i \in V_i = \mathbf{Z}_q^{n_i}$ for all $1 \leq i \leq s$.

Here $v_i (1 \leq i \leq s)$ is called the i^{th} *block of block size* n_i of the vector v.

Further, we define the modular value $|a|$ of an element $a \in \mathbf{Z}_q$ by

$$|a| = \begin{cases} a & \text{if} \quad 0 \leq a \leq q/2 \\ q - a & \text{if} \quad q/2 < a \leq q - 1. \end{cases}$$

Corresponding Author: Sapna Jain, sapnajain@gmx.com

We note that nonzero modular value $|a|$ can be obtained by two different elements viz. a and $q-a$ of $\mathbf{Z}_q$ provided $\{q$ is odd$\}$ or $\{q$ is even and $a \neq [q/2]\}$ i.e.

$$|a| = |q-a| \quad \text{if} \quad \begin{cases} q \quad \text{is odd} \\ \text{or} \\ q \text{ is even and} \\ \quad a \neq q/2. \end{cases}$$

If q is even and $a = [q/2]$ or if $a = 0$, then $|a|$ is obtained in only one way viz. $|a| = a$. Thus there may be one or two equivalent values of $|a|$ which we shall refer to as repetitive equivalent values of a. The number of repetitive equivalent values of a will be denoted by e_a where

$$e_a = \begin{cases} 1 \quad \text{if } \{ q \quad \text{is even and} \\ a = [q/2]\} \text{ or } \{a = 0\} \\ 2 \quad \text{if } \{ q \text{ is odd and } a \neq 0\} \\ \text{or } \{q \text{ is even, } a \neq 0 \\ \text{and } a \neq [q/2]\}. \end{cases}$$

Throughout this paper, we shall use the following notations:

1. $[x]$ = The largest integer less than or equal to x.
2. $\lceil x \rceil$ = The smallest integer greater than or equal to x.
3. Q_i=The sum of repetitive equivalent values up to i i.e.,
$$Q_i = e_0 + e_1 + \cdots + e_i$$
where e_i denotes the repetitive equivalent value of i.

3. LINEAR PARTITION ARIHANT CODES

Let n, q be positive integers with $q > 1$. Let $P : n = [n_1][n_2]\cdots[n_s]$ be a partition of n. We define *Arihant metric* on $\mathbf{Z}_q^n$ corresponding to the partition P as follows:

Let $v = (v_1, v_2, \cdots, v_s) \in \mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$. The Arihant weight of i^{th} block $v_i \in \mathbf{Z}_q^{n_i} (1 \leq i \leq s)$ of the vector v corresponding to the partition P of n is defined as

$$w_A^P(v_i) = \max_{j=1}^{n_i} |v_j^{(i)}|$$

where

$$v_i \quad = \quad (v_1^{(i)}, v_2^{(i)}, \cdots, v_{n_i}^{(i)}) \in \mathbf{Z}_q^{n_i}.$$

Thus the Arihant weight of a block is the maximum modular value amongst all its components. Then the Arihant weight of the vector $v = (v_1, v_2, \cdots, v_s) \in \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$ corresponding to the partition P is defined as the sum of Arihant weights of all its blocks i.e.

$$W_A^P(v) = \sum_{i=1}^{s} w_A^P(v_i).$$

For any $u = (u_1, u_2, \cdots, u_s)$ and $v = (v_1, v_2, \cdots, v_s) \in \mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$, we define the Arihant distance (or Arihant metric) $d_A^P(u, v)$ between u and v as

$$d_A^P(u, v) = w_A^P(u - v).$$

Then d_A^P is a metric on $\mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$.

If the partition P is clear from the context, we shall denote Arihant weight by w_A and Arihant metric by d_A only.

Definition 1. A linear partition Arihant (LPA) code corresponding to the partition $P : n = [n_1]\cdots[n_s]$ is a $\mathbf{F}_q$-submodule of $\mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$ equipped with the Arihant metric and is denoted as $[n, k, d_A; P]$ or $[n, k; P]$ code where

$$k = \text{rank}_{\mathbf{Z}_q}(V),$$

and

$$\begin{aligned} d_A &= d_A(V) \\ &= \text{minimum Arihant distance} \\ &\quad \text{of } V \\ &= \min\{d_A(u, u') \mid u, u' \in V, \\ &\quad u \neq u'\}. \end{aligned}$$

Remark 2.

1. For $P : n = [1]^n$, the linear partition Arihant codes reduce to the classical Lee weight codes [1, 2, 3]. For this partition, the Arihant distance and Arihant weight reduce to classical Lee distance and Lee weight respectively.
2. For $q = 2, 3$, the linear partition Arihant codes reduce to the linear error-block codes [4] and the Arihant metric reduces to the π-metric introduced by Feng et al. [4].
3. In general, we have
$$\begin{aligned} \pi\text{-metric} &\leq \text{Arihant metric} \\ &\leq \text{Lee metric,} \\ &\text{or} \\ \pi\text{-weight} &\leq \text{Arihant weight} \\ &\leq \text{Lee weight.} \end{aligned}$$

Example 3. Let $n = q = 5$. Let $P : 5 = [1][2][2]$ be a partition of $n = 5$. Then $\mathbf{Z}_q^n = \mathbf{Z}_5^5 = \mathbf{Z}_5^1 \oplus \mathbf{Z}_5^2 \oplus \mathbf{Z}_5^2$.

Let $v = (1\vdots23\vdots41) = (v_1\vdots v_2\vdots v_3) \in \mathbf{Z}_5^5 = \mathbf{Z}_5^1 \oplus \mathbf{Z}_5^2 \oplus \mathbf{Z}_5^2$ where

$$\begin{aligned} v_1 &= (1) \in \mathbf{Z}_5^1, \\ v_2 &= (2,3) \text{ or } (23) \in \mathbf{Z}_5^2, \\ v_3 &= (4,1) \text{ or } (41) \in \mathbf{Z}_5^2. \end{aligned}$$

Let $V =< (v_1, v_2, v_3) >$ be the subspace generated by (v_1, v_2, v_3) over $\mathbf{Z}_5$.

The codewords in code V are given by

$$\begin{aligned} v &= (1\vdots23\vdots41) = (1, 23, 41); \\ & \quad w_A(v) = 1 + 2 + 1 = 4, \\ 0v &= (0, 00, 00); w_A(0v) = 0, \\ 2v &= (2, 41, 32); w_A(2v) \\ & \quad = 2 + 1 + 2 = 5, \\ 3v &= (3, 14, 23); w_A(3v) \\ & \quad = 2 + 1 + 2 = 5, \\ 4v &= (4, 32, 14); w_A(4v) \\ & \quad = 1 + 2 + 1 = 4. \end{aligned}$$

Thus V is a $[5, 1, 4; P]$ linear partition code $\mathbf{Z}_5$ with minimum Arihant distance 4.

4. SOME PROPERTIES OF LPA CODES

We begin by stating two results for LPA codes without proof as the proof is straightforward:

Theorem 4. *The minimum Arihant weight and minimum Arihant distance of an LPA code V coincide*. QED

Theorem 5. *An LPA code V corrects all errors of Arihant weight t or less iff the minimum Arihant distance of the code is at least $2t + 1$*. QED

The generator and parity check matrices of an $[n, k, d_A; P]$ LPA code can be viewed in terms of blocks corresponding to the partition P. For a parity check matrix H, it is viewed as

$$H = [H_1, H_2, \cdots, H_s]$$

where $H_i (1 \leq i \leq s)$ is an $(n - k) \times n_i$ matrix and is said to be the i^{th} block of size n_i of the parity check matrix H. The columns of the i^{th} block H_i are denoted as $h_1^{(i)}, h_2^{(i)}, \ldots, h_{n_i}^{(i)}$.

Definition 6. A set of blocks $\{H_{i_1}, H_{i_2}, \cdots, H_{i_l}\} \subseteq \{H_1, H_2, \cdots, H_s\}$ of the parity check matrix H is said to be linearly independent if the union of all column vectors in blocks $H_{i_1}, H_{i_2}, \cdots, H_{i_l}$ is a linearly independent set. Otherwise, we say that the set of blocks of $\{H_{i_1}, H_{i_2}, \cdots, H_{i_l}\}$ is linearly dependent.

Definition 7. A set of blocks $\{H_{i_1}, H_{i_2}, \cdots, H_{i_l}\} \subseteq \{H_1, H_2, \cdots, H_s\}$ of the parity check matrix H is said to be linearly dependent of Arihant weight w if there exists scalars $\alpha_1^{(i_1)}, \alpha_2^{(i_1)}, \cdots, \alpha_{n_{i_1}}^{(i_1)}, \alpha_1^{(i_2)}, \cdots, \alpha_{n_{i_2}}^{(i_2)}, \cdots, \alpha_1^{(i_l)}, \alpha_2^{(i_l)}, \cdots, \alpha_{n_{i_l}}^{(i_l)}$ not all zero such that

$$\sum_{j=1}^{n_{i_1}} \alpha_j^{(i_1)} h_j^{(i_1)} + \sum_{k=1}^{n_{i_2}} \alpha_k^{(i_2)} h_k^{(i_2)} + \cdots + \sum_{m=1}^{n_{i_l}} \alpha_m^{(i_l)} h_m^{(i_l)} = 0 \quad (1)$$

and

$$\begin{aligned} w &= w_A(\alpha_1^{(i_1)}, \cdots, \alpha_{n_{i_1}}^{(i_l)}, \alpha_1^{(i_2)}, \cdots, \\ & \quad \alpha_{n_{i_2}}^{(i_2)}, \cdots, \alpha_1^{(i_l)}, \cdots, \alpha_{n_{i_l}}^{(i_l)}) \\ &= w_1 + w_2 + \cdots + w_l \end{aligned} \quad (2)$$

where

$$\begin{aligned} w_j &= \max\{|\alpha_1^{(i_j)}|, |\alpha_2^{(i_j)}|, \\ & \quad \cdots, |\alpha_{n_{i_j}}^{(i_j)}|\} \\ & \quad for\ all\ 1 \leq j \leq l. \end{aligned} \quad (3)$$

Remark 8. We can denote the n_{i_j}-tuple $(\alpha_1^{(i_j)}, \alpha_2^{(i_j)}, \cdots, \alpha_{n_{i_j}}^{(i_j)})$ by α_{i_j}. Then (1) can be rewritten as

$$\alpha_{i_1}.H_{i_1} + \alpha_{i_2}.H_{i_2} + \cdots + \alpha_{i_l}.H_{i_l} = 0$$

where '." denotes the Euclidean inner product of α_{i_j} and H_{i_j} for all $1 \leq j \leq l$. Also (2) can be written as

$$\begin{aligned} w &= w_A(\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_l}) \\ &= w_A(\alpha_{i_1}) + w_A(\alpha_{i_2}) + \cdots \\ & \quad \cdots + w_A(\alpha_{i_l}) \\ &= w_1 + w_2 + \cdots + w_l \end{aligned}$$

where

$$\begin{aligned} w_j = w_A(\alpha_{i_j}) &= \max_{r=1}^{n_{i_j}}\{|\alpha_r^{(i_j)}|\} \\ & \quad \text{for all } 1 \leq j \leq l. \end{aligned}$$

The following result is now obvious:

Theorem 9. *Let $H = [H_1, H_2, \cdots, H_s]$ be a parity check matrix of an $[n, k; P]$ LPA code V over $\mathbf{F}_q$ with partition $P : n = [n_1][n_2]\cdots[n_s]$. Then $d_A(V) = d$ if and only if there does not exist a linear dependence relation between blocks of H of Arihant weight $(d - 1)$ or less and there exists a linear dependance relation between blocks of H of Arihant weight d.* QED

We now prove a characterization of LPA codes in terms of the parity check matrix H which will lead to the Singleton's bound for LPA codes.

Theorem 10. *If the minimum Arihant distance (or minimum Arihant weight) of an $[n,k;P]$ LPA code over $\mathbf{F}_q$ is at least d, then every set of $\left[\frac{d-1}{[q/2]}\right]$ or fewer blocks of H is linearly independent.*

Proof. Let, if possible, there exists a linear dependence relation between some r blocks of H say $\{H_{i_1}, H_{i_2}, \cdots, H_{i_r}\}$ where $r \leq \left[\frac{d-1}{[q/2]}\right]$. Then there exists scalar tuples $\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_r}$ (with not all zero) with $\alpha_{i_j} = (\alpha_1^{(i_j)}, \alpha_2^{(i_j)}, \cdots, \alpha_{n_{i_j}}^{(i_j)}) \in \mathbf{Z}_q^{n_{i_j}}$ for all $1 \leq j \leq r$ such that

$$\alpha_{i_1}.H_{i_1} + \alpha_{i_2}.H_{i_2} + \cdots + \alpha_{i_r}.H_{i_r} = 0.$$

This implies that there exists a codeword

$$u = (0 \cdots \alpha_{i_1}, \cdots, \alpha_{i_2}, \cdots, \alpha_{i_r}, 0, \cdots, 0)$$

such that

$$\begin{aligned} w_A(u) &= w_A(\alpha_{i_1}) + w_A(\alpha_{i_2}) + \cdots \\ &\quad \cdots + w_A(\alpha_{i_r}) \\ &\leq \underbrace{[q/2] + \cdots + [q/2]}_{r \text{ times}} \\ &= r[q/2] \\ &\leq \left[\frac{d-1}{[q/2]}\right] \times [q/2] \\ &\leq d-1. \end{aligned}$$

Thus there exists a codeword of Arihant weight $d-1$ or less. A contradiction and hence the result. QED

Corollary 11. *If the minimum Arihant distance of an $[n,k;P]$ LPA code V with $P : n = [n_1][n_2]\cdots[n_s]$ is at least d, then*

$$n - k \geq n_{i_1} + n_{i_2} + \cdots + n_{i_r}, \tag{4}$$

where

$$r = \left[\frac{d-1}{[q/2]}\right],$$

and

$$\{n_{i_1}, n_{i_2}, \cdots, n_{i_r}\} \subseteq \{n_1, n_2, \cdots, n_s\}.$$

Proof. Directly follows from Theorem 10. and the fact that number of rows of parity check matrix H is $n-k$. QED

Remark 12. The inequality (4) is Singleton's bound for LPA codes and it says that for any $[n,k,d;P]$ LPA code V, the number of parity check digits must be greater than or equal to sum of block sizes of any $\left[\frac{d-1}{[q/2]}\right]$ blocks.

We now define maximum Arihant distance separable (MADS) codes:

Definition 13. An $[n,k,d;P]$ LPA code V with $P : n = \{n_1][n_2]\cdots[n_s]$ is said to be maximum Arihant distance separable (MADS) if equality holds in (4) i.e. if $(n-k)$ equals the sum of block sizes of any $\left[\frac{d-1}{[q/2]}\right]$ blocks.

Observation 14.

(i) If V is an $[n,k,d;P]$ MADS code with $P : n = [n_1][n_2]\cdots[n_s]$, then every $(n-k)\times(n-k)$ square submatrix of H comprising of any $\left[\frac{d-1}{[q/2]}\right]$ blocks of H is non-singular.

(ii) If V is an $[n,k,d;P]$ MADS code, then the partition P of n must be of the type $P : n = [n_1]^r$ for some positive integer r.

Example 15. Let $q=5$, $n=2$. Let $P : 2 = [1][1]$ be a partition of $n=2$. Let V be a $[2,1;P]$ LPA code with parity check matrix

$$H = (1\dot{:}3)_{1\times 2} \qquad \text{over } \mathbf{Z}_5.$$

The generator matrix G of the code V corresponding to the parity check matrix H is given by

$$G = (2\dot{:}1)_{1\times 2}.$$

The five code vectors of the Arihant code V are given by

$$\begin{aligned} v_0 &= (0\dot{:}0) \quad \text{or } (0,0);\ w_A(v_0) = 0, \\ v_1 &= (2\dot{:}1) \quad \text{or } (2,1);\ w_A(v_1) = 3, \\ v_2 &= (4\dot{:}2) \quad \text{or } (4,2);\ w_A(v_2) = 3, \\ v_3 &= (1\dot{:}3) \quad \text{or } (1,3);\ w_A(v_3) = 3, \\ v_4 &= (3\dot{:}4) \quad \text{or } (3,4);\ w_A(v_4) = 3. \end{aligned}$$

Therefore, the minimum Arihant weight and hence the minimum Arihant distance of the code V is 3 i.e. $d_A(V) = d = 3$.

Here $\left[\frac{d-1}{[q/2]}\right] = \left[\frac{3-1}{2}\right] = 1$.

Since for the LPA code V, $(n-k)$ equals the sum of block sizes of any $\left[\frac{d-1}{[q/2]}\right] = 1$ blocks, therefore, V is an MADS code.

5. HAMMING SPHERE UPPER BOUND FOR LPA CODES

In this section, we obtain the Hamming sphere upper bound for LPA codes. To obtain the desired bound,

we need to find $V_{d,q}^{(n_1,\cdots,n_s)}$ where $V_{d,q}^{(n_1,\cdots,n_s)}$ is the volume of a sphere of radius d in $\mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$ corresponding to the partition $P : n = [n_1][n_2]\cdots[n_s]$. This is equivalent to finding all $n = n_1 + n_2 + \cdots + n_s$-block vectors having Arihant weight d or less. We obtain the number of such block vectors in the following lemma:

Lemma 16. *If $V_{d,q}^{(n_1,\cdots,n_s)}$ denotes the number of all n-block vectors over $\mathbf{F}_q$ corresponding to the partition $P : n = [n_1][n_2]\cdots[n_s]$ having Arihant weight d or less where*
$1 \leq d \leq s[q/2]$, then

$$V_{d,q}^{(n_1,\cdots,n_s)} = \sum_{r=r_{ij}} \Bigg(\prod_{i=1}^{s} \prod_{j=0}^{[q/2]} ((Q_j)^{n_i} - (Q_{j-1})^{n_i})^{r_{ij}} \Bigg), \quad (5)$$

where $r = (r_{ij})_{i=1 \text{ to } s, j=0 \text{ to } [q/2]} = (r_{10}, r_{11}, \cdots, r_{1,[q/2]}, r_{20}, r_{21} \cdots r_{2,[q/2]} \cdots \cdots r_{s0} \cdots r_{s,[q/2]})$ satisfies

$$\begin{aligned} &For\ a\ fixed\ i\ (1 \leq i \leq s),\\ &r_{ij} = 1\\ &for\ exactly\ one\ value\ of\\ &j\ (0 \leq j \leq [q/2])\\ &and\ 0\ elsewhere,\\ &and\\ &\sum_{i=1}^{s}\sum_{j=0}^{[q/2]} j r_{ij} \leq d. \end{aligned} \quad (6)$$

Proof. For $1 \leq i \leq s, 0 \leq j \leq [q/2]$. Let r_{i_j} denotes the probability that the i^{th} block of block size n_i in an $n = n_1 + n_2 + \cdots + n_s$-block vector is having Arihant weight j.

It is clear from the definition of r_{ij} that for a fixed i, r_{ij} assumes value 1 exactly for one value of j and zero otherwise. Further, the choices for filling up entries in a block of size $n_i (1 \leq i \leq s)$ to have Arihant weight j $(0 \leq j \leq [q/2])$ is given by

$$\begin{aligned} &(e_0 + e_1 + \cdots e_j)^{n_i}\\ &-(e_0 + e_1 + \cdots + e_{j-1})^{n_i}\\ =\ &(Q_j)^{n_i} - (Q_{j-1})^{n_i} \end{aligned} \quad (7)$$

From (7) and the definition of r_{ij}, (5) satisfying constraint (6) directly follows. QED

Remark 17. If $A_{d,q}^{(n_1,\cdots,n_s)}$ denotes the number of all $n = n_1 + n_2 \cdots + n_s$-block vectors corresponding to the partition $P : n = [n_1][n_2]\cdots[n_s]$ having Arihant weight d, then $A_{d,q}^{(n_1,\cdots,n_s)}$ is given by R.H.S. of (5) satisfying

$$\begin{aligned} &For\ a\ fixed\ i\ (1 \leq i \leq s),\\ &r_{ij} = 1\\ &for\ exactly\ one\ value\ of\\ &j\ (0 \leq j \leq [q/2])\\ &and\ 0\ elsewhere,\\ &and\\ &\sum_{i=1}^{s}\sum_{j=0}^{[q/2]} j r_{ij} = d. \end{aligned} \quad (8)$$

Example 18. Let $q = 5$ and $n = 3$. Let $P : 3 = [1][2] = [n_1][n_2]$ be a partition of $n = 3$. Let $d = 1$. Then $V_{1,5}^{(n_1,n_2)}$ is given by (using (5))

$$V_{1,5}^{(n_1,n_2)} = \sum_{r=r_{ij}} \Bigg(\prod_{i=1}^{2} \prod_{j=0}^{2} ((Q_j)^{n_i} - (Q_{j-1})^{n_i})^{r_{ij}} \Bigg) \quad (9)$$

where for $1 \leq i \leq 2, 0 \leq j \leq 2$, $r = (r_{ij})$ satisfies

$$\begin{aligned} &For\ a\ fixed\ i\ (1 \leq i \leq 2),\\ &r_{ij} = 1\\ &for\ exactly\ one\ value\ of\\ &j\ (0 \leq j \leq 2)\\ &and\ 0\ elsewhere,\\ &and\\ &\sum_{i=1}^{2}\sum_{j=0}^{2} j r_{ij} \leq 1. \end{aligned} \quad (10)$$

There are only three feasible solutions for $r = (r_{ij})_{i=1\ to\ 2, j=0\ to\ 2}$ satisfying (10) viz.

$$\begin{aligned} r &= (r_{10}, r_{11}, r_{12} \vdots r_{20}, r_{21}, r_{22})\\ &= (1,0,0 \vdots 1,0,0), (1,0,0 \vdots 0,1,0),\\ &\quad (0,1,0 \vdots 1,0,0). \end{aligned}$$

Substituting these values of $r = (r_{ij})$ in (9) we get

$$\begin{aligned} V_{1,5}^{(n_1,n_2)} &= ((Q_0)^1 - (Q_{-1})^1)((Q_0)^2 - (Q_{-1})^2) + ((Q_0)^1 - (Q_{-1})^1)((Q_1)^2 - (Q_0)^2) + ((Q_1)^1 - (Q_0)^1)((Q_0)^2 - (Q_{-1})^2)\\ &= (1) + (3^2 - 1) + (3 - 1)\\ &= 1 + 2 + 8 = 11. \end{aligned}$$

(Note that $Q_{-1} = 0, Q_0 = 1, Q_1 = 3$ over $\mathbf{Z}_5$)

These 11 block vectors of length $3 = [1][2]$ and Arihant weight 1 or less are given by

$$v_0 = (0 \vdots 00), v_1 = (1 \vdots 00),$$

$$\begin{aligned} v_2 &= (4\dot{:}00), v_3 = (0\dot{:}10), \\ v_4 &= (0\dot{:}40), v_5 = (0\dot{:}01), \\ v_6 &= (0\dot{:}11), v_7 = (0\dot{:}41), \\ v_8 &= (0\dot{:}04), v_9 = (0\dot{:}14), \\ v_{10} &= (0\dot{:}44) \end{aligned}$$

Now we give the Hamming sphere upper bound for LPA codes:

Theorem 19 (Hamming Sphere Bound). *Let V be an $[n, k, d; P]$ LPA code over $\mathbf{F}_q$ corresponding to the partition $P : n = [n_1][n_2]\cdots[n_s], n_1 \leq n_2 \leq \cdots \leq n_s$. Then*

$$q^{n-k} \geq V_{[(d-1)/2],q}^{(n_1,\cdots,n_s)},$$

where $V_{[(d-1)/2],q}^{(n_1,\cdots,n_s)}$ is given by (5).

Proof. The proof follows from that fact that all the $n = n_1 + n_2 \cdots + n_s$-block vectors of Arihant weight $[(d-1)/2]$ or less must belong to distinct cosets of the standard array and the number of available cosets is q^{n-k}. QED

Remark 20. For $q = 2, 3$, the Hamming sphere bound obtained for LPA codes reduces to the corresponding bound for linear error block codes equipped with the π-metric [1].

6. GILBERT AND VARSHAMOV BOUNDS FOR LPA CODES

In this section, we obtain Gilbert bound, Varshamov bound and a bound for random error correction in LPA codes. We derive Gilbert bound first:

Theorem 21 (Gilbert Bound). *Let n, k, q be positive integers satisfying $q \geq 2, 1 \leq k \leq n$. Let $P : n = [n_1][n_2]\cdots[n_s], n_1 \leq n_2 \leq \cdots \leq n_s$ be a partition of n. Let d be a positive integer satisfying $1 \leq d \leq s[q/2]$. Then there exists an $[n, k, d; P]$ LPA code over $\mathbf{F}_q$ with minimum Arihant distance at least d provided*

$$n - k \geq log_q\left(V_{d-1,q}^{(n_1,\cdots,n_s)}\right) \tag{11}$$

where $V_{d-1,q}^{(n_1,\cdots,n_s)}$ is given by (5) satisfying (6).

Proof. We shall show that if (11) holds then there exists an $(n-k) \times n$ matrix H over $\mathbf{F}_q$ such that no linear combination of blocks of H of Arihant weight $(d-1)$ or less is zero. We define an algorithm for finding the blocks $H_1, H_2, \cdots, H_s$ of H where $H_i = (h_1^{(i)}, h_2^{(i)}, \cdots, h_{n_i}^{(i)})$ for all $1 \leq i \leq s$. From the set of all q^{n-k} columns vectors of length $(n-k)$ over $\mathbf{F}_q$, we choose blocks of columns of the parity check matrix H as follows:

(1) The n_1 column vectors in the first block H_1 can be any vectors chosen from the set of q^{n-k} column vectors of length $n-k$ over $\mathbf{F}_q$ satisfying

$$\lambda_1.H_1 \neq 0,$$

where

$$\lambda_1 = (\lambda_1^{(1)}, \lambda_2^{(1)}, \cdots, \lambda_{n_1}^{(1)}) \in \mathbf{F}_q^{n_1},$$

and

$$\begin{aligned} 1 \leq w_A(\lambda_1) &= w_A(\lambda_1^{(1)}, \lambda_2^{(1)}, \\ &\quad \cdots, \lambda_{n_1}^{(1)}) \\ &= \max_{i=1}^{n_1} |\lambda_i^{(1)}| \\ &\leq d-1. \end{aligned}$$

(2) The second block $H_2 = (h_1^{(2)}, h_2^{(2)}, \cdots, h_{n_2}^{(2)})$ can be any set of n_2 column vectors of length $(n-k)$ satisfying

$$\lambda_1.H_1 + \lambda_2.H_2 \neq 0,$$

where for $1 \leq i \leq 2$,

$$\lambda_i = (\lambda_1^{(i)}, \lambda_2^{(i)}, \cdots, \lambda_{n_i}^{(i)}) \in \mathbf{Z}_q^{n_i},$$

and

$$\begin{aligned} 1 &\leq w_A(\lambda_1) + w_A(\lambda_2) \\ &= \max_{a=1}^{n_1} |\lambda_a^{(1)}| + \max_{b=1}^{n_2} |\lambda_b^{(2)}| \\ &\leq d-1. \end{aligned}$$

$$\begin{array}{ccc} \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \end{array}$$

(l) The l^{th} block $H_l = (h_1^{(l)}, h_2^{(l)}, \cdots, h_{n_l}^{(l)})$ can be any set of n_l column vectors of length $(n-k)$ satisfying

$$\begin{aligned} &\lambda_1.H_1 + \lambda_2.H_2 + \cdots \\ &\qquad + \lambda_l.H_l \neq 0. \end{aligned} \tag{12}$$

where

$$\begin{aligned} \lambda_i &= (\lambda_1^{(i)}, \lambda_2^{(i)}, \cdots, \lambda_{n_i}^{(i)}) \in \mathbf{F}_q^{n_i} \\ &\quad \text{for all } 1 \leq i \leq l, \end{aligned}$$

and

$$\begin{aligned} 1 &\leq w_A(\lambda_1) + w_A(\lambda_2) + \cdots \\ &\quad + w_A(\lambda_l) \\ &= \max_{a=1}^{n_1} |\lambda_a^{(1)}| + \max_{b=1}^{n_2} |\lambda_b^{(2)}| + \\ &\quad \cdots + \max_{p=1}^{n_l} |\lambda_p^{(l)}| \\ &\leq d-1. \end{aligned} \tag{13}$$

$$\begin{array}{ccc} \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \end{array}$$

(s) The s^{th} block $H_s = (h_1^{(s)}, h_2^{(s)}, \cdots, h_{n_s}^{(s)})$ can be any set of n_s column vectors satisfying

$$\lambda_1.H_1 + \lambda_2.H_2 + \cdots + \lambda_s.H_s \neq 0.$$

where

$$\lambda_i = (\lambda_1^{(i)}, \lambda_2^{(i)}, \cdots, \lambda_{n_i}^{(i)}) \in \mathbf{F}_q^{n_i} \text{ for all } 1 \leq i \leq s,$$

and

$$\begin{aligned} 1 &\leq w_A(\lambda_1) + w_A(\lambda_2) + \cdots \\ &\quad + w_A(\lambda_s) \\ &= \max_{a=1}^{n_1} |\lambda_a^{(1)}| + \max_{b=1}^{n_2} |\lambda_b^{(2)}| + \\ &\quad \cdots + \max_{t=1}^{n_s} |\lambda_t^{(s)}| \\ &\leq d - 1. \end{aligned}$$

If we carry out this algorithm to completion, then, $H_1, H_2, \cdots, H_s$ are the blocks of size (or length) $n_1, n_2, \cdots, n_s$ respectively of an $(n-k)\times n$ $\left(\text{where } n = \sum_{i=1}^{s} n_i\right)$ block matrix H such that no linear combination of blocks of H of Arihant weight $(d-1)$ or less is zero and this matrix is the parity check matrix for an LPA code with minimum Arihant distance at least d. We show that the construction can indeed be completed. Let l be an integer such that $2 \leq l \leq s$ and assume that the blocks $H_1, H_2, \cdots, H_{l-1}$ have been chosen. Then the block H_l can be added to H provided (12) is satisfied. The number of distinct linear combinations in (12) satisfying (13) including the pattern of all zeros is given by

$$V_{d-1,q}^{(n_1,\cdots,n_l)}$$

where $V_{d-1,q}^{(n_1,\cdots,n_l)}$ is given by (5) satisfying (6).

As long as the set of all linear combinations occurring in (12) satisfying (13) is less than or equal to the total number of $(n-k)$-tuples, the l^{th} block H_l can be added to H. Therefore, the block H_l can be added to H provided that

$$q^{n-k} \geq V_{d-1,q}^{(n_1,\cdots,n_l)}$$

or

$$n - k \geq log_q\left(V_{d-1,q}^{(n_1,\cdots,n_l)}\right).$$

Thus the fact that the blocks $H_1, H_2, \cdots, H_s$ can be chosen follows by induction on l and we get (11).QED

Corollary 22. *For positive integer* t $\left(t \leq \dfrac{s[q/2]-1}{2}\right)$, *a sufficient condition for the existence of an* $[n, k, d; P]$ *LPA code* V *over* $\mathbf{F}_q$ *where* $P : n = [n_1][n_2]\cdots[n_s]$ *that corrects all random block errors of Arihant weight* t *or less is given by*

$$n - k \geq log_q\left(V_{2t,q}^{(n_1,\cdots,n_s)}\right).$$

Proof. The proof follows from Theorem 21 and the fact that to correct all errors of Arihant weight t or less, the minimum Arihant weight of an LPA code must be at least $2t+1$. QED

Example 23. Let $n = 3, k = 1, d = 2$ and $q = 5$. Let $P : 3 = [1][2]$ be a partition of $n = 3$. We show that for these values of the parameters, (11) is satisfied. we note that here $n_1 = 1, n_2 = 2$. Equation (11) for these parameters becomes

$$n - k \geq log_5\left(V_{1,5}^{(n_1,n_2)}\right),$$

or

$$5^{n-k} \geq V_{1,5}^{(n_1,n_2)}. \tag{14}$$

Now $V_{1,5}^{(n_1,n_2)}$ (where $n_1 = 1, n_2 = 2$) was already computed in Example 18 and is equal to 11.

Thus

$$\begin{aligned} \text{L.H.S. of } (14) &= 5^{n-k} = 5^{3-1} = 25, \\ \text{R.H.S. of } (14) &= V_{1,5}^{(n_1,n_2)} = 11. \end{aligned}$$

Thus

$$5^{n-k} = 25 \geq 11 = V_{1,5}^{(n_1,n_2)}.$$

Therefore, by Theorem 21, there exists a $[3, 1; P]$ LPA code V over $\mathbf{Z}_5$ where $P : 3 = [1][2]$ with minimum Arihant distance at least 2.

Consider the following 2×3 block matrix H of a $[3, 1; P]$ LPA code V over $\mathbf{Z}_5$ constructed by the algorithm discussed in Theorem 21:

$$H = \left(\begin{array}{c:cc} 1 & 0 & 2 \\ 0 & 1 & 3 \end{array}\right)_{2\times3}.$$

We claim that the LPA code which is the null space of the matrix H has minimum Arihant distance at least 2.

The generator matrix of the LPA code corresponding to the parity check matrix H is given by

$$G = [-2 \vdots -3 \quad 1]_{1\times3} = [3 \vdots 2 \quad 1]_{1\times3}$$

The five codewords of the LPA code V with G as generator matrix and H as parity check matrix are given by:

$$\begin{aligned} v_0 &= (0\dot{:}00); w_A(v_0) = 0, \\ v_1 &= (3\dot{:}21); w_A(v_1) = 4, \\ v_2 &= (1\dot{:}42); w_A(v_2) = 3, \\ v_3 &= (4\dot{:}13); w_A(v_3) = 3, \\ v_4 &= (2\dot{:}34); w_A(v_4) = 4. \end{aligned}$$

Therefore, the minimum Arihant weight of the LPA code V is 3 which is at least $d = 2$. Hence Theorem 21 is verified.

Theorem 24 (Varshamov Bound). *Let $B_q(n, d; P)$ denote the largest number of code vectors in an $[n, k; P]$ LPA code V over $\mathbf{F}_q$ with $P : n = [n_1][n_2] \cdots [n_s]$ having minimum Arihant distance at least d. Then*

$$B_q(n, d; P) \geq q^{n-\lceil log_q(L) \rceil},$$

where $L = V_{d-1,q}^{(n_1,\cdots,n_s)}$ is given by (5) satisfying (6).

Proof. By Theorem 21, there exists an $[n, k; P]$ LPA code over $\mathbf{F}_q$ with minimum Arihant distance at least d provided

$$\begin{aligned} q^{n-k} &\geq V_{d-1,q}^{(n_1,\cdots,n_s)} = L \\ \Rightarrow n-k &\geq log_q(L) \\ \Rightarrow k &\leq n - log_q(L). \end{aligned}$$

The largest integer k satisfying the above inequality is $n - \lceil log_q(L) \rceil$. Thus

$$B_q(n, d; P) \geq q^{n-\lceil log_q(L) \rceil}$$

where $L = V_{d-1,q}^{(n_1,\cdots,n_s)}$ is given by (5) satisfying (6). QED

Acknowledgment: The author would like to thank her husband Dr. Arihant Jain for his constant support and encouragement for pursuing research.

REFERENCES

1. Jain, S. 2005. Modification to a bound for random error correction with Lee weight, Comm. Korean Math. Soc., 20: 405-409.
2. Jain, S., Nam, K.-B. and Lee, K.-S. 2005. On some perfect codes with respect to Lee metric, Linear Algebra and its Applications, 405:104-120.
3. Lee, C.Y. 1958. Some properties of non-binary error correcting codes, IEEE Trans. Information Theory, IT-4:77-82.
4. Feng, K., Xu, L. and Hickernell, F. 2006. Linear Error-Block Codes, Finite Fields and Applications, 12:638-652.
5. Udomkavanich, P. and Jitman, S. 2010. Bounds and modifications on Linear Error-Block Codes, International Mathematical Forum, 5:35-50.
6. van Lint, J.H. 1999. Introduction to Coding Theory, Third Edition, GTM 86, Springer-Verlag.