Plotkin's Bound in Codes Equipped with the Euclidean Weight Function^{*}

Sapna Jain[†]

Department of Mathematics, University of Delhi, Delhi 110 007, India

and

Seul Hee Choi[‡]

Department of Mathematics, Jeonju University, Chon-ju 560-759, Korea

Received August 15, 2007, Accepted October 13, 2008.

Abstract

There are three standard weight (distance) functions on a linear code viz. the Hamming weight (distance), the Lee weight (distance) and the Euclidean weight (distance). Plotkin [11] obtained an upper bound on the minimum weight (distance) of a code with respect to the Hamming weight (distance). A.D. Wyner and R.L. Graham [13] proved Plotkin's bound for Lee metric codes which was also conjectured by Lee [10]. The first author also obtained another proof of Plotkin's bound with the Lee weight by a different approach [3]. In this paper, we obtain Plotkin's bound for codes equipped with the Euclidean weight function. The Euclidean weight is useful in connection with the lattice constructions where the minimum norm of vectors in the lattice is related to the minimum Euclidean weight of the code [2]. Using Plotkin's bound, we obtain a bound on the number of parity check digits required to achieve

^{*2000} Mathematics Subject Classification. 94B05.

[†]E-mail: sapna@vsnl.com

[‡]E-mail: chois@jj.ac.kr

the minimum Euclidean square distance at least d^2 in a linear code. We also make a comparative study of the bounds for the Euclidean codes obtained in this paper with the corresponding bounds for the Hamming and Lee weight codes.

Keywords and Phrases: Plotkin's bound, Linear code, Euclidean weight.

1. Introduction

The minimum distance between any pair of code words in a code cannot exceed the average distance between all pairs of different code words. Using this observation, Plotkin [11] obtained the following upper bound for the minimum distance of a linear code with respect to the Hamming distance. This bound runs as follows:

Theorem 1.1.[5] The minimum distance (or minimum weight) of an (n, k) linear code over GF(q)(q) prime or power of prime) is at most as large as the average weight $nq^{k-1}(q-1)/(q^k-1)$.

In Section 2 of this paper we obtain Plotkin's bound for linear codes equipped with the Euclidean weight function. Using this bound, in Section 3 we obtain a bound on the number of parity check digits required to achieve the minimum Euclidean square distance at least d^2 in a linear code. Finally, we make a comparative study of the bounds obtained in Section 2 and 3 of this paper with the corresponding bounds for the Hamming and Lee weight codes [3, 11].

In what follows, we consider the following:

Let Z_q be the ring of integers modulo q. Let V_q^n be the set of all n - (tuples) over Z_q . Then V_q^n is a module over Z_q . Let V be a submodule of the module V_q^n over Z_q . For q prime, Z_q becomes a field and correspondingly V_q^n and V become the vector space and subspace respectively over the field Z_q . Also, we define the Euclidean value $|a|^2$ of an element $a \in Z_q$ by

$$|a|^{2} = \begin{cases} a^{2}, & \text{if } 0 \leq a \leq q/2; \\ (q-a)^{2}, & \text{if } q/2 < a \leq q-1, \end{cases}$$

or in other words

 $|a|^{2} = \min(a^{2}, (q-a)^{2}),$

then, for a given vector $u = (a_0, a_1, ..., a_{n-1}), a_i \in Z_q$, the Euclidean weight $w_E(u)$ of u is given by

$$w_E(u) = \sum_{i=0}^{n-1} |a_i|^2.$$

Note that in determining the Euclidean weight of vector, a nonzero entry a has a contribution $|a|^2$ which is obtained by two different entries a and q - a provided $\{q \text{ is odd }\}$ or $\{q \text{ is even and } a \neq q/2\}$.

i.e.

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

If q is even and a = q/2 or if a = 0, then $|a|^2$ is obtained in only one way viz. $|a|^2 = a^2$.

Thus for the Euclidean weight, there may be one or two entries from Z_q having the same Euclidean value $|a|^2$ and we call these entries as repetitive equivalent Euclidean values of a. The number of repetitive equivalent Euclidean values of a will be denoted by e_a where

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

The Euclidean square distance between the two vectors $u = (a_0, a_1, ..., a_{n-1})$ and $v = (b_0, b_1, ..., b_{n-1})$ is defined as the Euclidean weight of their difference i.e.

$$d_E^2(u,v) = w_E(u-v).$$

The minimum Euclidean square distance of a code is the smallest Euclidean square distance between all its distinct pair of code words. Also, the minimum Euclidean square distance (d_E^2) and the minimum Euclidean weight of a code coincide.

Remark 1.1. The Euclidean square distance coincides with the Lee distance and the Hamming distance over Z_2 and Z_3 .

2. Plotkin's Bound with the Euclidean Weight

To obtain the Plotkin's bound with Euclidean weight, we need to find the sum of the Euclidean weights of all the code words in a linear code over $Z_q(q \text{ prime})$.

We obtain this sum in the next two lemmas.

Lemma 2.1. If all the code vectors in a linear code V over $Z_q(q \text{ prime})$ having M elements are arranged as rows of a matrix, then each field element appears $\frac{M}{q}$ times in each column. Assume that no column consists of all 0's.

Proof. Let X be the subset of the given code consisting of those code words whose first component is zero. Then $X \neq \phi$ as $(0, 0, 0, \dots, 0) \in V$.

The set X forms a subgroups of the additive group of V. Place all such vectors (i.e. vectors with first component as zero) as the elements of first row of an array. Pick a code vector of V which begins with 1 and place it below the first element as the leading element of the second row. Complete the second row by adding the leading vector to the vectors in the first row and placing the sum below the corresponding vector. Note that all the elements in the second row will have their first component as 1.

Again choose a code vector which begins with 2 and place it as the first element in the third row. Complete the third row as earlier. Continuing in this way, we arrive at the row whose leading vector begins with q - 1.

In the above array, we note that all the vectors in the i^{th} row have their first component as $i - 1(1 \le i \le q)$. We claim that all the vectors in the code V appear once and only once in such an array. The claim follows from the fact that the rows of such an array are nothing but cosets of the subgroup X in the group V and any two cosets are either disjoint or identically the same. Thus the entire collection of vectors in V has been expressed as an array consisting of q rows.

Since #V = M, therefore, # of elements in any row $= \frac{M}{q}$.

Thus there are $\frac{M}{q}$ code words which have their first component as 0, 1, and so on. Therefore, if all such vectors are put as rows of a matrix, then every field element appears $\frac{M}{q}$ times in the first column. Since the choice of the column is arbitrary, we conclude that every field element appears $\frac{M}{q}$ times in every column.

Remark 2.1. We can also take Z_q as ring instead of field (i.e. q different

from prime). In that case we require an additional constraint on the linear code V that it must contain at least one code word having first component as 1. The final result will be the same i.e. each ring element appears $\frac{M}{q}$ times in each column.

Lemma 2.2. The sum of the Euclidean weights of all code words in a linear code V over $Z_q(q \text{ prime})$ of length n and having M elements is

$$= \begin{cases} \frac{nM(q^2-1)}{12} \text{ if } q \text{ is odd} \\ \\ \frac{nM(q^2+2)}{12} \text{ if } q \text{ is even }. \end{cases}$$

Proof. To compute the sum of the Euclidean weights of all the code words, put all the code vectors as rows of a matrix. Then, in any column of such a matrix

Now, there are two cases:

(i) When q is odd (ii) when q is even

Case (i): When q is odd

The Euclidean weight of a column is this case is

$$= 2\left[1^{2} \cdot \frac{M}{q} + 2^{2} \cdot \frac{M}{q} + \dots + \left(\frac{q-1}{2}\right)^{2} \cdot \frac{M}{q}\right]$$

$$= \frac{2M}{q} \left[1^{2} + 2^{2} + \dots + \left(\frac{q-1}{2}\right)^{2}\right]$$

$$= \frac{2M}{q} \cdot \frac{\frac{(q-1)}{2} \cdot \frac{(q+1)}{2}}{6}$$

$$= \frac{M(q^{2}-1)}{12}.$$

Case (ii): When q is even

The Euclidean weight of a column is this case is

$$= 2\frac{M}{q} \left[1^2 + 2^2 + \dots + \left(\frac{q-2}{2}\right)^2 \right] + \left(\frac{q}{2}\right)^2 \cdot \frac{M}{q}$$

$$= \frac{M(q-1)(q-2)}{12} + \frac{Mq}{4}$$

$$= \frac{M(q^2+2)}{12}.$$

Since there are n columns in all, therefore, the total Euclidean weight of n columns is

$$= \begin{cases} \frac{nM(q^2-1)}{12} & \text{if } q \text{ is odd} \\ \frac{nM(q^2+2)}{12} & \text{if } q \text{ is even} \end{cases}$$

Since total column weight = total row weight, therefore, we conclude that sum of Euclidean weights of all code words in a linear code V having M elements is

$$= \begin{cases} \frac{nM(q^2-1)}{12} \text{ if } q \text{ is odd} \\ \frac{nM(q^2+2)}{12} \text{ if } q \text{ is even }. \end{cases}$$

Theorem 2.1. (Plotkin's Upper Bound) The minimum Euclidean square distance (or the minimum Euclidean weight) of a linear code V over $Z_q(q \text{ prime})$ of length n and having M elements is at most as large as the average Euclidean weight

$$\begin{cases} \frac{nM(q^2 - 1)}{12(M - 1)} \text{ if } q \text{ is odd} \\ \\ \frac{nM(q^2 + 2)}{12(M - 1)} \text{ if } q \text{ is even }. \end{cases}$$

Proof. By Lemma 2.2, the sum of the Euclidean weights of all the code words in a linear code over $Z_q(q \text{ prime })$ having M elements is

$$= \begin{cases} \frac{nM(q^2-1)}{12} \text{ if } q \text{ is odd} \\ \frac{nM(q^2+2)}{12} \text{ if } q \text{ is even} \end{cases}$$

Also, # nonzero code words in V = M - 1,

 \Rightarrow the average Euclidean weight of code words is

$$= \begin{cases} \frac{nM(q^2 - 1)}{12(M - 1)} \text{ if } q \text{ is odd} \\ \\ \frac{nM(q^2 + 2)}{12(M - 1)} \text{ if } q \text{ is even }. \end{cases}$$

Since the minimum Euclidean weight can not exceed the average Euclidean weight, therefore, the weight of the minimum Euclidean weight code word is at most as large as

$$\begin{cases} \frac{nM(q^2-1)}{12(M-1)} \text{ if } q \text{ is odd} \\\\ \frac{nM(q^2+2)}{12(M-1)} \text{ if } q \text{ is even }. \end{cases}$$

Therefore, if d^2 is the minimum Euclidean square distance of the code, then

$$d^{2} \leq \begin{cases} \frac{nM(q^{2}-1)}{12(M-1)} \text{ if } q \text{ is odd} \\ \\ \frac{nM(q^{2}+2)}{12(M-1)} \text{ if } q \text{ is even }. \end{cases}$$

Remark 2.2. The Plotkin's bound still holds for non prime q provided we choose the linear code V such that it contains at least one code vector having first component as 1.

3. Bound on Parity Check Digits for the Linear Euclidean Weight Codes

We first prove a lemma.

Lemma 3.1. Let $B_q(n, d^2)$ denote the maximum number of code words possible in a linear code over $Z_q(q \text{ prime})$ of length n and the minimum Euclidean square distance at least d^2 , then

$$B_q(n, d^2) \leq q B_q(n-1, d^2).$$

Proof. Let V be a linear code with n symbols and minimum Euclidean square distance (or the minimum Euclidean weight) at least d^2 that has $B_q(n, d^2)$ code words. Consider X to be a subset of V consisting of those code words of V which have the last component as zero. Then $X \neq \phi$ as $0 = (0, 0, \dots, 0) \in V$. The set X forms a subspace of V.

Now, as in Lemma 2.1, if we form cosets of X in V, we shall get q cosets. Obviously,

Vectors in
$$X = \frac{1}{q} \# V$$

= $\frac{1}{q} B_q(n, d^2).$ (1)

Consider the set X' obtained from the vectors of X by deleting the last component of all its vectors. Since the last component of all the vectors in X is zero, therefore, the set X' is a linear code of length n-1 having the same number of elements and the same minimum Euclidean weight as that of X. Since the minimum Euclidean square distance of code V is at least d^2 , therefore, the Euclidean square distance between any two vectors of X is also at least d^2 . This implies that the Euclidean square distance between any two vectors of X' is also at least d^2 . Since $B_q(n-1, d^2)$ denotes the maximum

214

number of code words possible in a linear code of length n-1 having the minimum Euclidean square distance at least d^2 , therefore,

$$\# X' \leq B_q(n-1, d^2).$$

Also,

$$\# X = \# X'.$$

Therefore,

$$#X \leq B_q(n-1, d^2)$$

$$\Rightarrow \frac{1}{q}B_q(n, d^2) \leq B_q(n-1, d^2) \quad (\text{using (1)})$$

$$\Rightarrow B_q(n, d^2) \leq qB_q(n-1, d^2).$$

Theorem 3.1. If $n \ge \frac{4(3d^2-1)}{q^2-1}$, the number of parity check digits required to achieve the minimum Euclidean square distance at least d^2 in an (n, k) linear code V over $Z_q(q \text{ prime})$ is at least

$$\begin{cases} 4\left(\frac{3d^2-1}{q^2-1}\right) - \log_q 3d^2, & \text{if } q \ge 3\\ (2d^2-2) - \log_2 d^2, & \text{if } q = 2. \end{cases}$$

Proof. Number of elements in an (n, k) linear code V over the field $Z_q = M = q^k$.

There are two cases.

(i) $q \ge 3$, a prime number (ii) q = 2

Case (i): When $q \ge 3$, a prime number.

Since $q \ge 3$, a prime number is always an odd number, therefore from Plotkin's bound we have

$$d^{2} \leq \frac{n(q^{2}-1)M}{12(M-1)} = \frac{n(q^{2}-1)q^{k}}{12(q^{k}-1)}.$$

For a code of length i, we get

$$\begin{aligned} d^2 &\leq \frac{i(q^2-1)q^k}{12(q^k-1)} \\ \Rightarrow & 12d^2(q^k-1) \leq i(q^2-1)q^k \\ \Rightarrow & 12(q^kd^2-d^2) \leq i(q^2-1)q^k \\ \Rightarrow & 12q^kd^2 - i(q^2-1)q^k \leq 12d^2 \\ \Rightarrow & q^k \left(3d^2 - \frac{i}{4}(q^2-1)\right) \leq 3d^2, \end{aligned}$$

and if $3d^2-\frac{i}{4}(q^2-1)>0$, we get

$$q^{k} \leq \frac{3d^{2}}{3d^{2} - \frac{i}{4}(q^{2} - 1)}$$

$$\Rightarrow B_{q}(i, d^{2}) = q^{k} \leq \frac{3d^{2}}{3d^{2} - \frac{i}{4}(q^{2} - 1)} .$$
(2)

Choose i such that

$$\frac{3d^2-1}{q^2-1} = \frac{i}{4} + f \text{ where } i \text{ is an integer and } 0 \le f < 1,$$
(3)

then

$$3d^2 - \frac{i}{4}(q^2 - 1) = 1 + f(q^2 - 1).$$
(4)

Using (4) in (2) gives

$$B_q(i, d^2) \le \frac{3d^2}{1 + f(q^2 - 1)}.$$
(5)

If $n \geq i$, then

$$B_{q}(n, d^{2}) \leq q^{n-i}B_{q}(i, d^{2}) \text{ (using repeated application of Lemma 3.1)} \leq q^{n+4(f-\frac{3d^{2}-1}{q^{2}-1})} \cdot \frac{3d^{2}}{1+f(q^{2}-1)} \text{ (using (3) and (5))} = q^{n-4(\frac{3d^{2}-1}{q^{2}-1})} \cdot q^{4f} \cdot \frac{3d^{2}}{1+f(q^{2}-1)} = q^{n-4(\frac{3d^{2}-1}{q^{2}-1})} \cdot 3d^{2} \cdot \frac{q^{4f}}{1+f(q^{2}-1)}.$$
(6)

Now

$$q^{4f} = [1 + (q - 1)]^{4f}$$

$$\leq 1 + 4f(q - 1)$$

$$\leq 1 + (q + 1)f(q - 1) \quad (\text{since } q \geq 3)$$

$$= 1 + (q^2 - 1)f$$

$$\Rightarrow \frac{q^{4f}}{1 + f(q^2 - 1)} \leq 1.$$
(7)

Using (7) in (6) gives

$$B_{q}(n, d^{2}) \leq q^{n-4(\frac{3d^{2}-1}{q^{2}-1})}.3d^{2}$$

$$\Rightarrow q^{k} \leq q^{n-4(\frac{3d^{2}-1}{q^{2}-1})}.3d^{2}$$

$$\Rightarrow k \leq n-4\left(\frac{3d^{2}-1}{q^{2}-1}\right) + \log_{q}3d^{2}.$$

$$\Rightarrow n-k \geq 4\left(\frac{3d^{2}-1}{q^{2}-1}\right) - \log_{q}3d^{2}.$$

Case 2. For q = 2.

Since 2 is an even number, therefore, from Plotkin's bound, we have

$$d^{2} \leq \frac{nM(q^{2}+2)}{12(M-1)} = \frac{n.2^{k-1}}{2^{k}-1}.$$

For a code of length i, we get

$$d^{2} \leq \frac{i \cdot 2^{k-1}}{2^{k} - 1}$$

$$\Rightarrow \quad 2^{k-1} (2d^{2} - i) \leq d^{2}$$

$$\Rightarrow \quad 2^{k-1} \leq \frac{d^{2}}{2d^{2} - i}$$

$$\Rightarrow \quad B_{2}(i, d^{2}) = 2^{k} \leq \frac{2d^{2}}{2d^{2} - i}.$$
(8)

Choose i such that

$$2d^2 - 1 = i + f$$
 where *i* is an integer and $0 \le f < 1$,

then

$$2d^2 - i = 1 + f. (9)$$

Using (9) in (8) gives

$$B_2(i,d^2) \le \frac{2d^2}{1+f}.$$
(10)

Again, if $n \ge i$, then

$$\begin{array}{rcl} B_2(n,d^2) &\leq& 2^{n-i}B_2(i,d^2) \text{ (using repeated application of Lemma 3.1)} \\ &\leq& 2^{n-(2d^2-1)}.2^f.\frac{2d^2}{1+f} & \text{(using (8) and (10))} \\ &=& 2^{n-(2d^2-1)}.2d^2.\frac{2^f}{1+f} \\ &\leq& 2^{n-(2d^2-1)}.2d^2.1 & \text{(since } 2^f = (1+1)^f \leq 1+f) \\ \Rightarrow& B_2(n,d^2) &\leq& 2^{n-(2d^2-1)}.2d^2 \\ \Rightarrow& 2^k &\leq& 2^{n-2d^2+2}.d^2 \end{array}$$

Taking log on both sides, we get

$$k \leq n - 2d^2 + 2 + \log_2 d^2$$

$$\Rightarrow k \leq n - (2d^2 - 2) + \log_2 d^2$$

$$\Rightarrow n - k \geq (2d^2 - 2) - \log_2 d^2.$$

Combining the two cases, we get the result.

Remark 3.1. For q = 2, 3, the Euclidean square distance bound obtained in Theorem 3.1 coincides with the corresponding bound for the Hamming distance codes [11, Theorem 4.1] and the Lee distance codes [3, Theorem 3] using the fact that the Euclidean square distance reduces to the Hamming and Lee distance for binary and ternary cases.

For q = 3, the bound in Theorem 3.1 becomes

$$n-k \ge \left(\frac{3d^2-1}{2}\right) - 1 - \log_3 d^2.$$

218

or, equivalently

$$n-k \ge \left(\frac{3d_L-1}{2}\right) - 1 - \log_3 d_L. \quad ([3], \text{ Theorem 3})$$

or, equivalently

$$n-k \ge \left(\frac{3d_H-1}{2}\right) - 1 - \log_3 d_H.$$
 ([11], Theorem 4.1)

where d_L and d_H are the minimum Lee and Hamming distances respectively.

4. Comparative Study

In this section, we compare Plotkin's bound for an (n, k) linear code over $Z_q(q \ prime)$ equipped with the Hamming distance, Lee distance and Euclidean square distance respectively. The comparison has been presented in the form of a table. Similar type of comparative study has been made for the bound obtained in Theorem 3.1 of this paper.

4.1. Comparison of Plotkin's bound

Plotkin's bound for the Hamming distance codes is stated in Theorem 1.1 of this paper and the same has been obtained for Euclidean square distance codes in Theorem 2.1 of this paper. We further state Plotkin's bound for the Lee distance codes [3].

Theorem 4.1.[3, Theorem 2] The minimum Lee distance (or the minimum Lee weight) d of a linear code over $Z_q(q \text{ prime})$ of length n having M elements is atmost as large as the average Lee weight

$$\begin{cases} \frac{nM(q^2-1)}{4q(M-1)} & \text{if } q \text{ is odd} \\ \frac{nMq}{4(M-1)} & \text{if } q \text{ is even} \end{cases}.$$

Now, we make a comparison of Plotkin's bound for an (n, k) linear code over $Z_q(q \ prime)$ with respect to the Hamming distance, Lee distance and Euclidean square distance.

Table 4	4.1
-----------	-----

Value of q	Hamming distance	Lee distance	Euclidean square distance
q=2,	$\frac{n2^{k-1}}{2^k - 1}$	$\frac{n2^{k-1}}{2^k - 1}$	$\frac{n2^{k-1}}{2^k - 1}$
q = 3,	$\frac{2n3^{k-1}}{3^k-1}$	$\frac{2n3^{k-1}}{3^k - 1}$	$\frac{2n3^{k-1}}{3^k-1}$
q=5,	$\frac{4n5^{k-1}}{5^k-1}$	$\frac{6n5^{k-1}}{5^k - 1}$	$\frac{10n5^{k-1}}{5^k - 1}$
q = 7,	$\frac{6n7^{k-1}}{7^k - 1}$	$\frac{12n7^{k-1}}{7^k - 1}$	$\frac{28n7^{k-1}}{7^k - 1}$
q = 11,	$\frac{10n11^{k-1}}{11^k - 1}$	$\frac{30n11^{k-1}}{11^k - 1}$	$\frac{110n11^{k-1}}{11^k - 1}$
q = 13	$\frac{12n13^{k-1}}{13^k - 1}$	$\frac{42n13^{k-1}}{13^k - 1}$	$\frac{182n13^{k-1}}{13^k - 1}$
q = 17	$\frac{16n17^{k-1}}{17^k - 1}$	$\frac{72n17^{k-1}}{17^k - 1}$	$\frac{408n17^{k-1}}{17^k - 1}$

From the above table, we observe that the maximum value of minimum weight in an (n, k) linear code over $Z_q(q \text{ prime})$ with respect to the Hamming, Lee and Euclidean weight functions coincides for q = 2, 3 and for $q \ge 5(q \text{ prime})$, the ratio of maximum value of minimum weight attainable in an (n, k) linear code over Z_q is given by

Hamming weight : Lee weight
$$= 1: \frac{q+1}{4}$$

Hamming weight : Euclidean weight $= 1: \frac{q(q+1)}{12}$
Lee weight : Euclidean weight $= 1: \frac{q}{3}$.

Thus maximum value of weight of minimum weight code word in the Lee metric codes over $Z_q (q \ge 5, a \text{ prime})$ is $\frac{q+1}{4}$ times maximum value of minimum weight code word in the Hamming metric codes over $Z_q (q \ge 5, a \text{ prime})$. Similarly, maximum value of the minimum Euclidean weight is $\frac{q(q+1)}{12}$ times maximum minimum Hamming weight and $\frac{q}{3}$ times maximum minimum Lee weight over $Z_q (q \ge 5, a \text{ prime})$.

4.2. Comparison of the Euclidean weight bound obtained in Theorem 3.1 with the corresponding Hamming and Lee weight bounds

The bound under comparison for the Euclidean code is obtained in Theorem 3.1 of this paper. The corresponding bounds for the Hamming and Lee weight codes are stated below:

Theorem 4.2 ([11], Theorem 4.1). If $n \ge \frac{(qd-1)}{(q-1)}$, the number of check symbols required to achieve minimum distance(weight) in an n-symbol linear block code is at least $\left[\frac{(qd-1)}{(q-1)}\right] - 1 - \log_q d$.

Theorem 4.3 ([3], Theorem 3). If $n \ge \frac{4(qd-1)}{(q^2-1)}$, the number of parity check digits required to achieve the minimum Lee distance at least d in an (n,k) linear code V over $Z_q(qprime)$ is at least

$$= \begin{cases} \frac{4(q-1)}{q^2-1} - 1 - \log_q d & \text{if } q \ge 3\\ (2d-2) - \log_2 d & \text{if } q = 2. \end{cases}$$

Value of q	Hamming distance	Lee distance	Euclidean square distance
q = 2	$2d_H - 2 - \log_2 d_H$	$2d_L - 2 - log_2d_L$	$2d_E^2 - 2 - \log_2 d_E^2$
q = 3	$1.5d_H - 1.5 - \log_3 d_H$	$1.5d_L - 1.5 - \log_3 d_L$	$1.5d_E^2 - 1.5 - \log_3 d_E^2$
q = 5	$1.25d_H - 1.25 - log_5d_H$	$0.83d_L - 1.17 - log_5d_L$	$0.5d_E^2 - 0.17 - \log_5 3d_E^2$
q = 7	$1.67d_H - 1.67 - log_7d_H$	$0.58d_L - 1.08 - log_7d_L$	$0.25d_E^2 - 0.08 - \log_7 3d_E^2$
q = 11	$1.1d_H - 1.1 - log_{11}d_H$	$0.37d_L - 1.03 - log_{11}d_L$	$0.1d_E^2 - 0.03 - \log_{11}3d_E^2$
q = 13	$1.08d_H - 1.08 - log_{13}d_H$	$0.31d_L - 1.02 - \log_{13}d_L$	$0.07d_E^2 - 0.02 - \log_{13}3d_E^2$
q = 17	$1.06d_H - 1.06 - \log_{17}d_H$	$0.24d_L - 1.01 - \log_{17}d_L$	$0.04d_H^2 - 0.01 - \log_{17}3d_E^2$

Table 4.2

Note. The fractions in the above table have been rounded off up to two decimals places.

We observe from table 4.2 that the three bounds coincide for q = 2, 3 using the fact that $d_E^2 = d_L = d_H$ over \mathbf{Z}_2 and \mathbf{Z}_3 .

Acknowledgment

The first author would like to thank her husband Dr. Arihant Jain for his constant inspiration and encouragement for pursuing research.

References

[1] E. R. Berlekamp, Algebraic Coding Theory, McGraw Hill, New York, 1968.

- [2] A. Bonnecaze, P. Sole and A. R. Calderbank, Quaternary quadratic residue codes and unimodular lattices, *IEEE Trans. Inform. Theory*, 41(1995), 366-377.
- [3] S. Jain, *Plotkin's Bound with Lee Weight*, Proc. of 2004 IMCC entitled "Advances in Algebra Towards Millennium Problems" (International Maths Conference, Chonbuk National University, Chonbuk, Korea, August 04-06, 2004, pp.133-145., Eds.: Ki-Bong Nam et al., 2005, 133-145.
- [4] S. Jain, Error Detecting and Error Correcting Capabilities of Euclidean Codes, Ed. Vol.: Pragmatic Algebra, Eds.: Ki-Bong Nam et al., 2006, 51-66.
- [5] S. Jain, Modification to a Bound for Random error Correction with Lee Weight, Communications of the Korean Mathematical Society, 20(2005), 405-409.
- [6] S. Jain, K.-B. Nam and K.-S. Lee, On Some Perfect Codes with respect to Lee Metric, *Linear Algebra and Its Applications*, 405(2005), 104-120.
- [7] S. Jain and K.-B. Nam, Lower Bounds for Codes Correcting Moderate-Density Bursts of Fixed Length with Lee Weight Consideration, *Linear Algebra and Its Applications*, 412(2006), 122-129.
- [8] S. Jain and K. P. Shum, Sufficient Condition over the Number of Parity Checks for Burst Error Detection/Correction in Linear Lee Weight Codes, *Algebra Colloquium*, 14(2007), 341-350.
- S. Jain and K.-B. Nam, Varshamov-Gilbert-Sacks Bound for Linear Lee Weight Codes, Algebras Groups and Geometries, 24(2007), 349-360.
- [10] C. Y. Lee, Some properties of non-binary error correcting codes, *IEEE Trans. Information Theory*, IT-4(1958), 77-82.
- [11] M. Plotkin, Binary Codes with specified minimum distance, *IRE Trans. Inform. Theory*, **IT-6**(1960), 445-450.
- [12] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, The MIT Press, Massachusetts, 1972.

[13] A. D. Wyner and R. L. Graham, An upper Bound on Minimum Distance for a k-ary Code, *Information and Control*, 13(1968), 46-52.