International Research Journal of Pure Algebra-5(10), 2015, 168-176
Available online through www.rjpa.info ISSN 2248–9037

A NOTE ON SOME ELEMENTARY BOUNDS ON CODES

AVINASH J. KAMBLE*[1], T. VENKATESH[2]

[1]Department of Mathematics,
Alva's Institute of Engineering and Technology, Moodbidri - 574 225, Karnataka, India.

[2]Department of Mathematics,
Rani Channamma University, Belgavi -591156, Karnataka, India.

(Received On: 19-10-15; Revised & Accepted On: 26-10-15)

ABSTRACT

In this paper, we will discuss certain limitations of codes in the form of upper and lower bounds on the rate of codes as a function of their relative distance. Further we will give concrete bounds on the size of codes and then infer as corollaries the asymptotic statement for code families relating rate and relative distance.

AMS Mathematics Subject Classification (2010): *94B05, 94B65.*

Keywords: *Linear codes, Optimal code, Minimum distance, Rate and Relative distance of a code, Entropy function.*

1. INTRODUCTION

Coding theory is an important study which attempts to minimize data loss due to errors introduced in transmission from noise, interference or other forces. with a wide range of theoretical and practical applications from digital data transmission to modern medical research, coding theory has helped enable much of growth in the 20th century. It is particularly important to ensure reliable transmission when large computer files are rapidly transmitted or when data are sent over long distances, such as data transmitted from space probes billions of miles away. To guarantee reliable transmission or recover degraded data, techniques from coding theory are used. Messages, in the form of bit strings, are encoded by translating them into longer bit strings, called codeword. A set of codeword is called a code. We can detect errors when we use certain codes, as long as not too many errors have been made, we can determine whether one or more errors have been introduced when a bit string was transmitted. Furthermore, when codes with more redundancy are used, we can correct errors.

A rough gauge of the quality of a linear code C is provided by two invariants, the transmission rate $R(C):=k/n$ and the relative distance $\delta(C):=d/n$, where n is the length of C, k is its dimension and d its minimum distance. In essence, the purpose of coding theory is to find codes that optimize these invariants. In this paper, we will discuss certain elementary upper and lower bounds on the rate of codes as a function of their relative distance.

2. PRE-REQUISITES

Definition 2.1: A code is any non-empty subset of F_q^n. The code is called linear if it is an F_q-linear subspace of F_q^n. The number n is the length of the code.

Definition 2.2: The Hamming distance d on $F_q^n \times F_q^n$ is given by $d(x,y):=\left|\{i/1\le i\le n, x_i \ne y_i\}\right|$,
Where $x=(x_1,\ldots,x_n)$ and $y=(y_1,\ldots,y_n)$.
The weight of x is defined by $w(x):=d(x,0)$, where $0:=(0,\ldots,0)$.

***Corresponding Author: Avinash J. Kamble*[1]**

Remark 2.3: The Function d is metric on $F_q^n \times F_q^n$.

Definition 2.4: The minimum distance of a code $C \subseteq F_q^n$ is given by
$d(C) := \min\{d(x,y) : x, y \in C, x \neq y\}$

Remark 2.5: For $C \subseteq F_q^n$ a linear code, we have $d(C) = \min\{w(x) : x \in C \setminus \{0\}\}$.

Definition 2.6: If $|F| = q$ and $C \subset F^n$, then $R := n^{-1} \log_q |C|$ is called the (information) rate of C.

For a linear $[n,k]$-code we can write $R(C) = k/n$.

Definition 2.7: For a code C with length n and minimum distance d, let $\delta = d/n$ be the relative distance of the code. The relative distance is often defined as d/n; however taking $\dfrac{d-1}{n}$ makes some of the calculations simpler.

Definition 2.8: Let $C \subseteq F_q^n$ be a linear code of dimension k. A generator matrix of C is a $k \times n$ matrix whose rows form an F_q-base of C.

Definition 2.9: Let $C \subseteq F_q^n$ be a code. The dual code of C is the code $C^\perp$ defined by
$C^\perp := \{x \in F_q^n : \langle x, y \rangle = 0, \forall y \in C\}$,
where for $x = (x_1, ..., x_n)$, $y = (y_1, ..., y_n)$, $\langle x, y \rangle := \sum_{i=1}^{n} x_i y_i$ is the usual bilinear form on $F_q^n \times F_q^n$.
Note that, $C^\perp$ is indeed a linear code.

Definition 2.10: A parity check matrix of a linear code is any generator matrix of its dual.

Definition 2.11: Let A be an alphabet of size $q > 1$ and fix $n, d.$ we define
$A_q(n,d) = \max\{M / \exists an(n, M, d) codeexists.\}$.
An $[n, M, d]$-code for which $M = A_q(n,d)$ is called an optimal code.

Definition 2.12: Let $q > 1$ be a prime power and fix $n, d.$
We define $B_q(n,d) = \max\{q^k / \exists alinear(n, M, d) code.\}$.
A linear $[n, M, d]$ -code for which $q^k = B_q(n,d)$ is called an linear optimal code.

Definition 2.13: The binary entropy function H is defined by $H(x) = x \log_2 \dfrac{1}{x} + (1-x) \log_2 \dfrac{1}{1-x}$.

3. SOME BOUNDS ON CODES

3.1. The Sphere –Covering Lower Bound

Definition 3.1.1: Let A be an alphabet of size q with $q > 1.$ Then for every $u \in A^n$ and every $r \in N$ $(r \geq 0)$, a sphere with centre u and radius r, denoted $S_A(u,r)$, is defined to be the set $\{v \in A^n / d(u,v) \leq r\}$.

The volume of a sphere as above denoted $V_q^n(r)$, is defined to be $|S_A(u,r)|$.

Lemma 3.1.2: For every natural number $r \geq 0$ and alphabet A of size $q > 1$, and for every $u \in A^n$ we have,

$$V_q^n(r) = \begin{cases} \sum_{i=0}^{r} \binom{n}{i} (q-1)^i & 0 \leq r \leq n \\ q^n & r > n \end{cases}$$

Theorem 3.1.3: (Sphere-covering bound) For every natural number $q > 1$, and every $n, d \in N$ such that $1 \leq d \leq n$ it holds that $A_q(n,d) \geq \dfrac{q^n}{V_q^n(d-1)}$.

Proof: Let $C = \{c_1, \ldots, c_M\}$ be an optimal $[n, M, d]$-code over an alphabet of size q. That is, $M = A_q(n,d)$. Since C is optimal, there does not exist any word in A^n of distance at least d from every $c_i \in C$. Thus, for every $x \in A^n$ there exists at least one $c_i \in C$ such that $x \in S_A(c_i, d-1)$.

This implies that, $A^n \subseteq \bigcup_{i=1}^{M} S_A(c_i, d-1)$ and so, $q^n \leq \sum_{i=1}^{M} |S_A(c_i, d-1)| = M.V_q^n(d-1)$.

Since C is optimal, we have $M = A_q(n,d)$ and hence $q^n \leq A_q(n,d).V_q^n(d-1)$, implies that

$$A_q(n,d) \geq \frac{q^n}{V_q^n(d-1)}.$$

3.2. The Hamming (Sphere Packing) Upper Bound

The idea behind the upper bound is that, if we place spheres of radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ around every codeword, then the spheres must be disjoint (otherwise there exists a word that is at distance at most $\left\lfloor \frac{d-1}{2} \right\rfloor$ from two code words and by the triangle inequality there are two code words at distance at most $d-1$ from each other) . The bound is thus derived by computing how many disjoint spheres of this size can be "packed" into the space.

Theorem 3.2.1: (sphere-packing bound): For every natural number $q > 1$ and $n, d \in N$ such that $1 \leq d \leq n$;

$$A_q(n,d) \leq \frac{q^n}{V_q^n\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right)}$$

Proof: Let $C = \{c_1, \ldots, c_M\}$ be an optimal code with $|A| = q$, and let $e = \left\lfloor \frac{d-1}{2} \right\rfloor$. Since $d(C) = d$ the spheres $S_A(c_i, e)$ are all disjoint. Therefore $\bigcup_{i=1}^{M} S_A(c_i, e) \subseteq A^n$, where the union is a disjoint one. Therefore,

$$M \cdot V_q^n\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right) \leq q^n.$$

Using now the fact that $M = A_q(n,d)$ we conclude that, $A_q(n,d) \leq \dfrac{q^n}{V_q^n\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right)}$.

Corollary 3.2.2: For every natural number $q > 1$ and $n, d \in N$ such that $1 \le d \le n$ it holds that,

$$\frac{q^n}{V_q^n(d-1)} \le A_q(n,d) \le \frac{q^n}{V_q^n\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right)}$$

Note that there is huge gap between these two bounds.

Definition 3.2.3: A code C over an alphabet of size q with parameters $[n, M, d]$ is called a perfect code, if

$$M = \frac{q^n}{V_q^n\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right)}$$

Remark 3.2.4: Every perfect code is an optimal code, but not necessarily the other way around.

Proposition 3.2.5: If there exist a perfect code $C \subseteq F_q^n$ with $d(C) = d$ then $|C| = A_q(n,d)$.
Hamming bound is a little odd, since for every pair of values d , $d+1$ where d is odd, the bound does not decrease. This stems from the fact that, for odd d , $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{d}{2} \right\rfloor$. This behavior is not incidental (for binary codes) and a binary code with odd distance can always be extended so that the distance is increased by 1.This does not help with error correction, but does help with error detection.

Theorem 3.2.6: Let d be odd. Then there exists a binary $[n, M, d]$-code if and only if, there exists a binary $(n+1, k, d+1)$-code. Likewise there exists a binary linear $[n, k, d]$-code if and only if, there exists a binary linear $[n+1, k, d+1]$ -code.

3.3. The Singleton Bound and MDS Codes
The parity check matrix H of an (n, k, d) linear code is an n by $n-k$ matrix such that, every $d-1$ rows of H are independent. Since the rows have length $n-k$, we can never have more than $n-k$ independent row vectors. Hence $d-1 \le n-k$ or equivalently $k \le n-d+1$. This establishes the result which is known as the Singleton bound.

Theorem 3.3.1: (Singleton bound) For every natural number $q > 1$ and $n, d \in N$ with $1 \le d \le n$ it holds that $A_q(n,d) \le q^{n-d+1}$. In particular, if C is a linear $[n, k, d]$-code, then $k \le n-d+1$

Proof: Let C be an optimal (n, M, d)-code and so $M = A_q(n,d)$. If we erase the last $d-1$ coordinates from all words in C, we still remain with the same number of words. Now, since we are left with $n-d+1$ coordinates there are at most q^{n-d+1} different words, implying that $A_q(n,d) = M \le q^{n-d+1}$.

Definition 3.3.2: A linear code with parameters $[n, k, d]$ such that $k = n-d+1$ is called a maximum distance separable (MDS) code.

Proposition 3.3.3: The dual code of an MDS code is MDS.
The singleton bound is only of interest for large values of q. In particular, the singleton bound tells us that $k \le n-d+1$ and thus for $d = 3$ it holds that $k \le n-2$. However, by the Hamming bound, we know that for $q = 2$ it really holds that $k \le n - \log n$ and thus the bound given by Singleton is very weak.

Theorem 3.3.4: (Properties of MDS codes)
Let C be a linear code over F_q with parameters $[n,k,d]$. Let G and H be generator and parity-check matrices for C. The following claims are equivalent:

1. C is an MDS code.
2. Every subset of $n-k$ columns in H is linearly independent.
3. Every subset of k columns in G is linearly independent.
4. $C^{\perp}$ is an MDS code.

3.4. The Gilbert -Varshamov Bound
The Gilbert-Varshamov bound is a lower bound for $B_q(n,d)$

Theorem 3.4.1: Let n, k and d be natural numbers such that $2 \le d \le n$ and $1 \le k \le n$.
If $V_q^{n-1}(d-2) < q^{n-k}$ then there exists a linear code (n,k) over F_q with distance at least d.

Proof: If $V_q^{n-1}(d-2) < q^{n-k}$ then there exists a parity check matrix $H \in F_q^{(n-k)\times n}$ for which every $d-1$ columns are linearly independent.

Corollary 3.4.2: Let $q > 1$ be a prime power, and let $n, d \in N$ such that $2 \le d \le n$.
Then $B_q(n,d) \ge \dfrac{q^{n-1}}{V_q^{n-1}(d-2)}$.

Proof: Define $k = n - [\log_q V_q^{n-1}(d-2)+1]$. It follows that,

$$q^{n-k} = q^{[\log_q (V_q^{n-1}(d-2)+1)]} \ge V_q^{n-1}(d-2)+1 > V_q^{n-1}(d-2)$$

Therefore, by the Theorem 3.4.1 there exists a linear $[n,k,d']$-code with $d' \ge d$. It follows that, $B_q(n,d) \ge q^k$. The bound is obtained as

$$q^k = q^{n-[\log_q (V_q^{n-1}(d-2)+1)]} \ge q^{n-1-\log_q (V_q^{n-1}(d-2)+1)} = \frac{q^{n-1}}{V_q^{n-1}(d-2)+1} \ge \frac{q^{n-1}}{V_q^{n-1}(d-2)}.$$

The Gilbert-Varshamov bound asserts the existence of positive rate binary codes only for relative distance $\delta < 1/2$. The Hamming bound on the other hand does not rule out positive rate binary codes even for $\delta > 1/2$, in fact not even for any $\delta < 1$. Thus, there is a qualitative gap between these bounds in terms of identifying the largest possible distance for asymptotically good binary codes.

3.5. The Plotkin Bound

We now present a bound that is much better than the Singleton and Hamming bounds. However it is only relevant for limited parameters. This bound uses the Cauchy-Schwarz inequality. This inequality states that, Let $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$ be sequences of real or complex numbers. Then

$$\left|\sum_{i=1}^{n} a_i b_i\right|^2 \le \sum_{i=1}^{n} |a_i|^2 \sum_{i=1}^{n} |b_i|^2.$$

Theorem 3.5.1: Let C be a $q-ary$ code of length n and minimum distance d. Then if $d > \rho n$,

$$A_q(n,d) \le \frac{d}{d-\rho n}, \quad \text{where } \rho = (q-1)/q$$

Proof: Consider a code C with M codewords in it. Form a list with the M codewords as the rows, and consider a column in this list. Let q_j denote the number of times that the j^{th} symbol in the code alphabet, $0 \le j < q$, appears in this column. Clearly $\sum_{j=0}^{q-1} q_j = M$.

Let the rows of the table be arranged so that the q_0 codewords with the 0^{th} symbol are listed first and call that set of codewords R_0, the q_1 codewords with the 1^{st} symbol are listed second and call that set of codewords R_1, and so forth. Consider the Hamming distance between all $M(M-1)$ pairs of codewords, as perceived by this selected column. For pairs of codewords within a single set R_i, all the symbols are same, so there is no contribution to the Hamming distance. For pairs of codewords drawn from different sets, there is a contribution of 1 to the Hamming distance. Thus, for each of the q_j codewords drawn from set R_j, there is a total contribution of $M - q_j$ to the Hamming distance between the codewords in R_j and all the other sets. Summing these up, the contribution of this column to the sum of the distances between all pairs of codewords is

$$\sum_{j=0}^{q-1} q_j\left(M - q_j\right) = M\sum_{j=0}^{q-1} q_j - \sum_{j=0}^{q-1} q_j^2 = M^2 - \sum_{j=0}^{q-1} q_j^2$$

Now using the Cauchy-Schwartz inequality, we write

$$\sum_{j=0}^{q-1} q_j\left(M - q_j\right) \le M^2 - \frac{1}{q}\left(\sum_{j=0}^{q-1} q_j\right)^2 = M^2\left(1 - \frac{1}{q}\right)$$

Now total this result over all n columns. There are $M(M-1)$ pairs of codewords, each a distance at least d apart. We obtain, $M(M-1)d \le n\left(1 - \frac{1}{q}\right)M^2 = n\rho M^2$.

$$\Rightarrow M \le \frac{d}{d - n\rho}$$

Since this result holds for any code, since the C was arbitrary, it must hold for the code with $A_q(n,d)$ codewords.

Equivalently, $d \le \frac{n\rho M}{M-1}$.

The Plotkin bound provides an upper bound on the distance of a code with given length n and size M.

In order to compare this bound to the Singleton bound, consider the case of $q = 2$ and thus $\rho = 1/2$.

Then, for $d > n/2$ we obtain $A_q(n,d) \le \left\lfloor \frac{d}{d - n/2} \right\rfloor$. Now, if $d = n/2 + 1$ then this bound gives us that $A_q(n,d) \le d = \frac{n}{2} + 1$. The Singleton bound just tells us that $k \le n/2$ and so $A_q(n,d) \le 2^{n/2}$.

Thus, the Plotkin bound is exponentially better than Singleton.

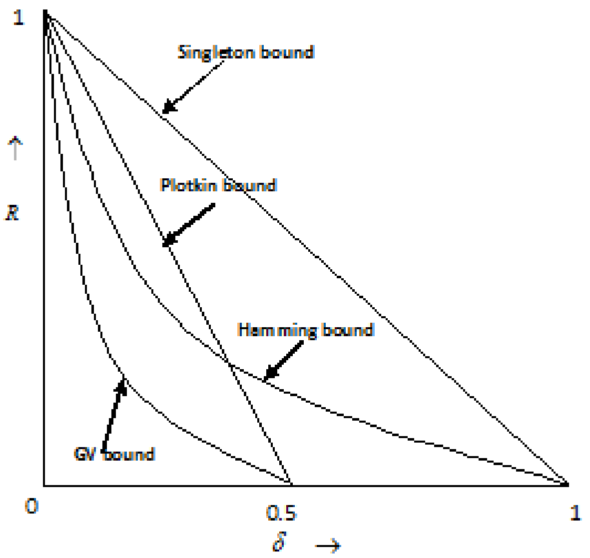

Figure-1: Bounds for binary codes

4. ASYMPTOTIC BOUNDS ON CODES

In this section, we will discuss asymptotic bounds, specifically bounds on codes when $n \to \infty$

Recall that the rate of a code is defined to be $R(C) = \dfrac{\log_q M}{n}$ and the relative distance is $\delta(C) = \dfrac{d-1}{n}$.

4.1. The Asymptotic Singleton Bound

Proposition 4.1.1: Let $\delta = \lim\limits_{n\to\infty} \delta(C)$ and let $R = \lim\limits_{n\to\infty} R(C)$. Then, for every code C it holds that $\delta \le 1 - R$.

Proof: The singleton bound states that, for every (n, M, d)-code, $d \le n - \log_q M + 1$ and equivalently, $d - 1 \le n - \log_q M$. Thus, $\delta(C) = \dfrac{d-1}{n} \le \dfrac{n}{n} - \dfrac{\log_q M}{n} = 1 - R(C) \to 1 - R$.

Note that in this case, there is actually no difference between the regular and asymptotic Singleton bounds.

4.2. The Asymptotic Sphere-Packing Bound

Notations 4.2.1: Let $C = \{C_n\}$ be a family of codes, such that C_n is the concrete code of length n in the family. Then, $\delta = \delta(C) = \lim\limits_{n\to\infty} \delta(C_n)$ and $R = R(C) = \lim\limits_{n\to\infty} R(C_n)$.

The bounds which hold for every n can be written as the bound for C_n, and some hold only for $n \to \infty$ is the bound for C.

Theorem 4.2.2: For every binary code C with asymptotic relative distance $\delta \le \dfrac{1}{2}$ and rate R,

$$R \le 1 - H(\delta/2)$$

Proof: Since $R = \dfrac{\log_q M}{n}$ and so, $n \cdot R = \log_2 M$.

The sphere-packing bound states that, $M \le A_q(n, d) \le \dfrac{q^n}{V_q^n\left(\left\lfloor \dfrac{d-1}{2} \right\rfloor\right)}$

And so, $R_n = \log M \leq \log A_2(n,d)$

$$R_n \leq \log\left(\frac{2^n}{V_2^n\left\lfloor\frac{d-1}{2}\right\rfloor}\right)$$

$$= n - \log V_2^n\left(\left\lfloor\frac{d-1}{2}\right\rfloor\right)$$

$$= n - \log 2^{nH\left(\frac{\delta}{2}\right)}$$

$$= n - nH\left(\frac{\delta}{2}\right)$$

On dividing by n, we obtain $R \leq 1 - H\left(\frac{\delta}{2}\right)$.

4.3. The Asymptotic Gilbert-Varshamov Bound

Theorem 4.3.1: Let n, k and d be such that $R \leq 1 - H(\delta)$ where $R = \frac{k}{n}$ and $\delta = \frac{d-1}{n} \leq \frac{1}{2}$. Then, there exists a binary linear code C_n with rate R and distance at least d.

Proof: If $R \leq 1 - H(\delta)$ then $nR \leq n - nH(\delta)$ and $n - nR \geq nH(\delta)$. Since $nR = k$ we have that $n - k \geq nH(\delta)$. This implies that, $2^{n-k} \geq 2^{nH(\delta)} \geq V_2^n(\delta n) = V_2^n(d-1) > V_2^n(d-2)$
Thus, by the Gilbert-Varshamov bound, there exists a binary linear code with distance at least d.

Corollary 4.3.2: For every n, there exists a binary linear code C_n with asymptotic relative distance and rate that are constant and non-zero.

Proof: Take any δ that is strictly between 0 and 0.5. For example, take $\delta = 1/4$.
Then $H(\delta) = -0.25\log 0.25 - 0.75\log 0.75 \approx 0.81$. This implies that there exists a code with relative distance 0.25 and rate 0.18.

Observe that as $\delta \to 1/2$, $H(\delta) \to 1$ and so $R \to 0$; Conversely, as $\delta \to 0$ we have that $R \to 1$. The above theorem tells us that we can choose anything we like in between these extremes.

4.4. The Asymptotic Plotkin Bound

Definition 4.4.1: Let q be a prime power and $\delta \in R$, with $0 \leq \delta \leq 1$ Then

$$\alpha_q(\delta) := \lim_{n\to\infty} Sup \frac{1}{n}\log_q A_q(n, \delta n)$$

$\alpha_q(\delta)$ is the largest R ,such that there is a sequence of codes over F_q with relative minimum distance converging to δ and information rate converging to R.

Theorem 4.4.2: (Asymptotic Plotkin bound) with $\rho = 1 - 1/q$ we have

$$\begin{cases} \alpha_q(\delta) \leq 1 - \delta/\rho, & if \quad 0 \leq \delta \leq \rho \\ \alpha_q(\delta) = 0, & if \quad \rho \leq \delta \leq 1 \end{cases}$$

Proof: Let C be a (n, M, d)-code over F_q. We can shorten C by considering the subset of C, r -times. Let C' be a code with length $n-r$, minimum distance d, and at least M/q^r -codewords.

Set $n' := \left\lfloor \dfrac{d-1}{\rho} \right\rfloor$ and shorten C, a total of $r = n - n'$ times to obtain a code of length n' with $M' \geq M/q^{n-n'}$ codewords.

The original Plotkin Bound theorem gives us, $\dfrac{M}{q^{n-n'}} \leq M' \leq \dfrac{d}{d-\rho n'} \leq d$, which immediately gives us

$M \leq dq^{n-n'}$.

Therefore we have

$$\alpha_q(\delta) \leq \lim_{n\to\infty} Sup \frac{1}{n} \log_q\left(\delta n q^{n-n'}\right)$$

$$= \lim_{n\to\infty} Sup \left(\frac{\log_q \delta}{n} + \frac{\log_q n}{n} + 1 - \frac{n}{n'} \right)$$

$$\Rightarrow \alpha_q(\delta) = 1 - \delta/\rho \ .$$

Since, $\lim\limits_{n\to\infty} \dfrac{n'}{n} = \lim\limits_{n\to\infty} \left(\dfrac{d-1}{\rho}\right) \Big/ n = \delta \big/ \rho$.

5. CONCLUSION

In this article, we summarize some elementary bounds on codes. By using some simple ideas, we have achieved fairly tight upper and lower bounds on the rate achievable for any value of δ.

ACKNOWLEDGEMENT

The authors would like to thank authorities of Department of Mathematics, Alva's Institute of Engineering and Technology, Moodbidri- 574 225 Karnataka–India and Department of Mathematics, Rani Channamma University, Belgavi- 591156 Karnataka, India for their constant support to make this paper successful.

REFERENCES

1. Berlekamp, E.R,; *Algebraic Coding Theory,* New York; McGraw-Hill, 1968.
2. Cameron, P.J. and van Lint, J.H,; *Designs, Graphs and Codes and their Links*. London Math. Soc. Student Texts, Vol. 22. Cambridge; Cambridge Univ. Press, (1991).
3. F.J.MacWilliams and N. J. Sloane, *The theory of error-correcting codes,* North–Holland, Amsterdam, 1977.
4. R.W. Hamming, *Error detecting and error correcting codes,* Bell system Tech. J.; 29: 147-160, 1950
5. Richard W.Hamming, *Coding and Information theory*, Prentice Hall, Englewood Cliffs, N.J.; 1980.
6. Raymond Hill, *A First Course in Coding Theory,* Oxford Applied Mathematics and Computing Science Series,; Oxford University Press, Oxford, 1986.
7. Rudolf Lidl and Harald Niederreiter, *Introduction to Finite Fields and their Applications,*; Cambridge University Press, Cambridge, 1986.
8. Vera Pless, *The Theory of Error Correcting Codes,*; Wiley Interscience Series in Discrete Mathematics and Optimization.; John Wiley and Sons. New York, 1989 (2nd edition) .
9. Van Lint, J.H,; *Coding Theory,* Springer Lecture Notes, Vol. 201, Berlin-Heidelberg-New York: Springer, 1971.
10. Van Lint, J.H., *Introduction to Coding Theory*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.

Source of Support: Nil, Conflict of interest: None Declared