iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: X Month of publication: October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10004

www.ijraset.com

Call: ✆08813907089 | E-mail ID: ijraset@gmail.com

Study of Some Bounds on Binary Codes

Rajiv Jain[1], Jaskarn Singh Bhullar[2]
[1,2]*Department of Applied Sciences, MIMIT, Malout Punjab*

Abstract: In this paper, various bounds on maximum number of codeword's for a given size and minimum distance is discussed. Then these bounds are studied with example and various types of upper bounds are calculated for size and distance. The comparison of these bounds have been done and the tighter bounds for $\mathbf{A_q(n,d)}$ is discussed.

***Keywords*: Error Correction, Binary Codes, Bounds, Hamming Bound, Plot kin Bound, Elias Bound**

I. INTRODUCTION

For a given *q*-ary (*n*, *M*, *d*) error correcting code, *n* is the size of code, *d* is the minimum distance between codewords of the code and *M* is the maximum number of codewords in the code. The efficiency of error correcting code is measured by number of codewords *M* in the code and the *d* is the error correcting capability of the code[1, 5]. It is necessary to have maximum number of codewords *M* in code with minimum distance *d* as high as possible for a good error correcting code. But in practice, for a code of given size *n* and minimum distance *d*, it is not always possible to obtain large *M*. So for given *n*, one has to negotiate between number of codewords *M* and Minimum distance *d*.

For *q*> 1, The$A_q(n,d)$ is defined as the largest possible size *M* for which a*q*-ary code with size *n*, codeword'*s* and distance *d* exists.

$$A_q(n,d) = \max\{\, M : \text{an}(n,M,d) \text{ code exists} \,\}$$

So, the bound on maximum number of codewords$A_q(n,d)$plays very important role in construction of codes in the Coding theory. To find $A_q(n,d)$ for given *q*, *n* and *d* is main coding theory problem. In other words, the basic coding theory problem is to find such a code of size n for given minimum distance d, which has maximum number of codewords. Generally it is not easy to find $A_q(n,d)$. To achieve the bounds of$A_q(n,d)$, a few basic theorems are used:

A. For q> 1, $A_q(n,d) \le q^n$for all $1 \le d \le n$

B. $A_q(n,1) = q^n$

C. $A_q(n,n) = q$

II. SOME BASIC UPPER BOUNDS OF $\mathbf{A_q(n,d)}$

In this paper, various basic upper bounds on size(or rate) of linear codes like Singleton bound, SpherePacking bound or Hamming Bound, Plotkin bound, Johnson upper bound, and Elias Upper bound are discussed. Then their bounds on various values of *n* and *d* are computed using their definitions. First the definitions of these upper bounds as follows:

A. Singleton bound

Singletonbound[1, 3, 5]is the one of the basic bound on the number of codewordsfrom the definition of codes. For integers$n \ge d \ge 1$, integer *q* > 1,

$$A_q(n,d) \le q^{n+1-d}$$

For a parameter $[n,k,d]_q$ of linear code, when q is a prime power,then$k + d - 1 \le n$. The codes$[n,k,d]$which satisfy this equality i.e.$k + d - n = 1$, are known as MDS Codes. Reed Solomon codes are good example of Maximum Distance Separable (MDS) codes.

B. Hamming Bound or SpherePacking Bound

For integer *n*,*q* > 1& integer *d*, $1 \le d \le n$, $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

$$A_q(n,d) \le \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

TheSpheres of radius *t*with centre as individualcodewords are disjoint. As there are $u = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$ total vectors in any one of these Spheres. Then maximum number of codewordsMu cannot exceed the numberq^n. The codes$(n,d)_q$, which achieves the

Hamming or SpherePacking bound are known as Perfect codes[1, 5]. The $(23, 12, 7)_2$and $(11, 6, 5)_3$ are perfect codes as they satisfy the Hamming bound.

C. Plotkin Bound

The Plotkin Bound[1, 2, 5] is an improvement of the SpherePacking Bound on $A_q(n, d)$. Plotkin bounds gives more tightly bounds than singleton bounds,SpherePacking bounds or hamming bounds for linear codes. It uses Cauchy Schwarz inequality to prove Plotkin bounds. Plotkin bounds holds for minimum distance d is close to size n.

For integer n,$q > 1$, integer $d$and$r = 1 - \frac{1}{q}$, if $n < d/r$

$$A_q(n, d) \leq \left\lfloor \frac{d}{d - nr} \right\rfloor$$

So, For binary codes, $q = 2$, Plotkin bounds becomes

$$\leq \begin{cases} 2\left\lfloor \frac{d}{2d - n} \right\rfloor & \text{when } d \text{ is even} \quad n < 2d \\ 4d & n = 2d \\ 2\left\lfloor \frac{d+1}{2d+1-n} \right\rfloor & \text{when } d \text{ is odd} \quad n < 2d+1 \\ 4d+4 & n = 2d+1 \end{cases}$$

D. Johnson Upper Bound

The constant weight codes are used to understand Johnson's upper bound[1, 4, 5]on $A_q(n, d)$. If $C$is codewordwith weight w then $A_q(n, d, w)$is defined as themaximum of the number of codewordswith size n and distance $d$of a constant weight w. Then the bounds on $A_q(n, d, w)$ is used to find the upper bounds on $A_q(n, d)$.The following theorems are used to find $A_q(n, d)$:

1) *For Upper bound on$A_q(n, d, w)$:*

i. If $d \leq 2w$, and define $e = \begin{cases} \frac{d}{2} & \text{if } d \text{ is even} \\ \frac{d+1}{2} & \text{if } d \text{ is odd} \end{cases}$

$$A_q(n, d, w) \leq \left\lfloor \frac{n(q-1)}{w} \left\lfloor \frac{(n-1)(q-1)}{w-1} \right\rfloor \ldots \left\lfloor \frac{(n-w+e)(q-1)}{e} \right\rfloor \ldots \right\rfloor \right\rfloor$$

ii. If $d > 2w$, $A_q(n, d, w) = 1$

2) *Johnson Upper bound on $A_q(n, d)$ is defined as*:

Let $t = \left\lfloor \frac{d-1}{2} \right\rfloor$,

If d is odd

$$A_q(n, d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i + \frac{\binom{n}{t+1}(q-1)^{t+1} - \binom{d}{t} A_q(n,d,d)}{A_q(n,d,t+1)}}$$

If d is even

$$A_q(n, d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i + \frac{\binom{n}{t+1}(q-1)^{t+1}}{A_q(n,d,t+1)}}$$

E. Elias Upper Bound

Elias Upper bound is applied for constant weight error correcting codes. For a given n and d, Elias bound is weaker bound than Plotkin's bound, Hamming Bound and Johnson upper bound.[1, 5].

For integer n>1, integer $q > 1$, integer d, $n \geq d \geq 1$, integer $w < r\, n$for$r = 1 - \frac{1}{q}$, &$w^2 - 2rnw + rnd > 0$, then

$$A_q(n, d) \leq \frac{rnd}{w^2 - 2rnw + rnd} \frac{q^n}{H_q(n, w)}$$

Where $H_q(n, w) = \sum_{i=0}^{w} \binom{n}{i} (q-1)^i$

III. AN EXAMPLE

To understand the concept of various upper bounds, we take the examples of bounds on $A_2(8,\ 4)$ are as follows:

A. Singleton Bound

For$q = 2, n = 8, d = 4$

$$A_2(8,4) \leq 2^{8+1-4} = 32$$

B. Hamming Bound or Sphere Packing Bound

For$q = 2, n = 8, d = 4$

$$A_2(8,4) \leq \frac{2^8}{\sum_{i=0}^{\left\lfloor\frac{4-1}{2}\right\rfloor} \binom{8}{i} (2-1)^i} = \frac{2^8}{\sum_{i=0}^{1} \binom{8}{i}} = \frac{2^8}{\binom{8}{0} + \binom{8}{1}} = \frac{2^8}{9} \approx 28$$

C. Plotkin Bound

For$q = 2, n = 8, d = 4$ as here $n = 2d$

$$A_2(8,4) \leq 4\ (4) = 16$$

D. Johnson Bound

For$q = 2, n = 8, d = 4$

Here d is even, therefore For$t = \left\lfloor\frac{4-1}{2}\right\rfloor = 1$

$$A_2(8,4) \leq \frac{2^8}{\sum_{i=0}^{2} \binom{8}{i} (2-1)^i + \frac{\binom{8}{3}(2-1)^{t+1}}{A_2(8,4,3)}} = \frac{2^8}{\sum_{i=0}^{2} \binom{8}{i} + \frac{\binom{8}{3}}{A_2(8,4,3)}} = \frac{256}{9 + \frac{28}{A_2(8,4,2)}}$$

Now, for $q = 2, n = 8, d = 4, w = 2$, As d is even, therefore $e = d/2 = 4$

$$A_2(8,4,2) \leq \left\lfloor \frac{n(q-1)}{w} \left\lfloor \frac{(n-1)(q-1)}{w-1} \right\lfloor \ldots \left\lfloor \frac{(n-w+e)(q-1)}{e} \right\rfloor \ldots \right\rfloor \right\rfloor \right\rfloor$$

$$A_2(8,4,2) \leq \left\lfloor \frac{8}{2} \right\rfloor = 4$$

So, $A_2(8,4) \leq \frac{256}{9+\frac{28}{A_2(8,4,2)}} = \frac{256}{9+\frac{28}{4}} = \frac{256}{16} = 16$

TABLE I
VARIOUS BOUNDS ON $A_2(8,4)$

	Singleton Bound	Sphere Packing or Hamming Bound	Plotkin Bound	Johnson Bound	Elias Bound		
					$w = 1$	$w = 2$	$w = 3$
$A_2(8,\ 4)$	32	28	16	16	50	27	44

E. Elias Bound $q = 2, n = 8, d = 4$

For$r = \frac{1}{2}$, integer$w < \frac{1}{2}\ 8 = 4$,And$w^2 - 8w + 16 > 0$, So $w = 1, 2, 3$ then

$$A_q(n,d) \leq \frac{rnd}{w^2 - 2rnw + rnd} \frac{q^n}{H_q(n,w)}$$

$$\text{So}, A_2(8{,}4) \le \frac{16}{w^2 - 8w + 16}\frac{2^8}{H_2(8,w)}$$

$$\text{Now}, H_q(n,w) = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i$$

$$\text{For } w = 1, H_2(8,1) = \textstyle\sum_{i=0}^{1} \binom{8}{i} (2-1)^i = \sum_{i=0}^{1} \binom{8}{i} = \binom{8}{0} + \binom{8}{1} = 9$$

$$\text{For } w = 2, H_2(8,2) = \textstyle\sum_{i=0}^{2} \binom{8}{i} (2-1)^i = \sum_{i=0}^{2} \binom{8}{i} = \binom{8}{0} + \binom{8}{1} + \binom{8}{2} = 37$$

$$\text{For } w = 3, H_2(8,3) = \textstyle\sum_{i=0}^{3} \binom{8}{i} (2-1)^i = \sum_{i=0}^{3} \binom{8}{i} = \binom{8}{0} + \binom{8}{1} + \binom{8}{2} + \binom{8}{3} = 93$$

$$\text{So, For } w = 1, \quad A_2(8,4) \le \frac{16}{w^2 - 8w + 16}\frac{2^8}{H_2(8,w)} = \frac{16}{9}\frac{2^8}{9} \approx 50$$

$$\text{So, For } w = 2, \quad A_2(8,4) \le \frac{16}{w^2 - 8w + 16}\frac{2^8}{H_2(8,w)} = \frac{16}{4}\frac{2^8}{37} \approx 27$$

$$\text{So, For } w = 3, \quad A_2(8,4) \le \frac{16}{w^2 - 8w + 16}\frac{2^8}{H_2(8,w)} = \frac{16}{1}\frac{2^8}{93} \approx 44$$

IV. CONCLUSION

After applying the above defined upper bounds on $A_q(n,d)$, the following table is obtained. From tableII, it is observed that Plotkin bound is much tighter bound on than Hamming bound and Singleton bound. For n= 8, d=4, Plotkin bound and Johnson bound gives the value 16 which is much tighter than singleton bound and hamming bound which are 32 and 28 respectively. But the drawback of Plotkin bound is that it is valid only for minimum distance *d* near to the size *n*.Due to which Plotkin bound is not defined large values of size of code as compared to minimum distance *d*. Also it can be seen from table II that Johnson bound is much tighter bound that Singleton bound, SpherePacking bound and Plotkin Bound, whereas Elias bound are very weak bound defined on constant weight codes. As for n= 10, d=4, Johnson bound gives the value 51 which is much tighter than singleton bound and hamming bound which are 128 and 93 respectively and Plotkin bound is not defined. Also it can be seen from Table Ithat Elias bound for *w* = 1, 2, 3 are much higher than other bounds discussed here. So it is concluded that for construction of linear binary codes, researcher should keep in mind of Johnson bounds on linear binary codes than other bounds discussed here.

TABLE II
SINGLETON BOUND, SPHERE PACKING BOUND, PLOTKIN BOUND AND JOHNSON BOUNDS ON $A_2(N,D)$

Singleton Bound										
Size → distance ↓	3	4	5	6	7	8	9	10	11	12
3	2	4	8	16	32	64	128	256	512	1024
4	---	2	4	8	16	32	64	128	256	512
5	---	---	2	4	8	16	32	64	128	256
7	---	---	---	---	2	4	8	16	32	64
Sphere Packing Bound										
Size → distance ↓	3	4	5	6	7	8	9	10	11	12
3	2	3	5	9	16	28	51	93	170	315
4	---	3	5	9	16	28	51	93	170	315
5	---	---	2	2	4	6	11	18	30	51
7	---	---	---	---	2	2	3	5	8	13
Plotkin Bound										
Size → distance ↓	3	4	5	6	7	8	9	10	11	12
3	2	2	4	8	16	---	---	---	---	---

4	---	2	2	4	8	16	20	---	---	---
5	---	---	2	2	2	4	6	12	24	---
7	---	---	---	---	2	2	2	2	4	4
Johnson Bound										
Size → distance ↓	3	4	5	6	7	8	9	10	11	12
3	2	2	4	8	16	25	51	83	167	292
4	---	2	2	5	8	16	26	51	89	170

REFERENCES

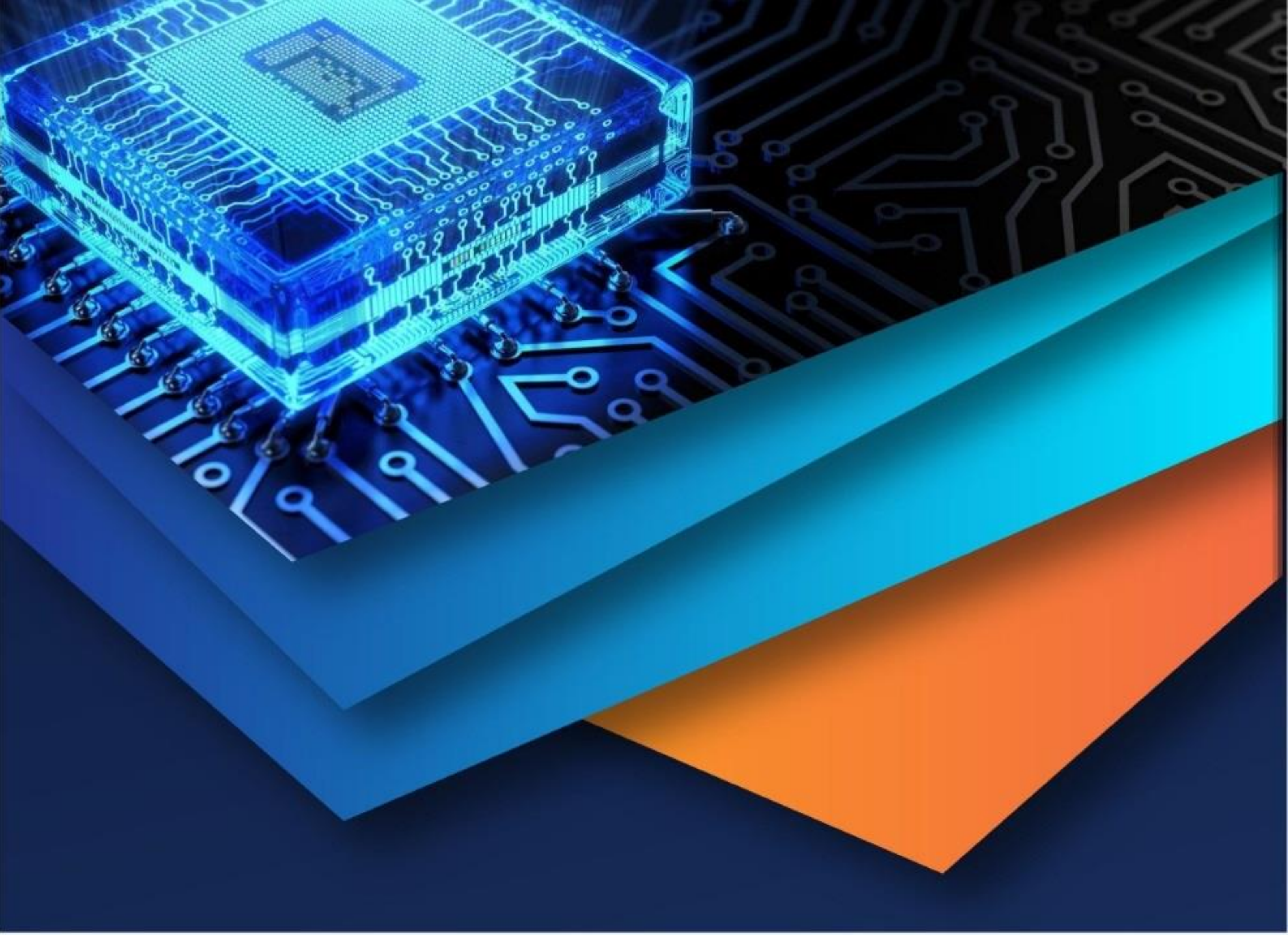
[1] F. J. Mac Williams and N. J. A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, North-Holland, 1977.

[2] M. Plotkin, "Binary codes with specified minimum distance," in IRE Transactions on Information Theory, vol. 6, no. 4, pp. 445-450, September 1960.

[3] R. Singleton, "Maximum distanceq-nary codes," in IEEE Transactions on Information Theory, vol. 10, no. 2, pp. 116-118, April 1964.

[4] S. M. Johnson, "A new upper bound for error-correcting codes" in IRE Transactions on Information Theory, vol. 8, no.3, pp. 203–207, April 1962.

[5] V. Pless, Introduction to the Theory of Error-Correcting Codes. John Wiley &Sons. 1982.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 ✆ (24*7 Support on Whatsapp)