

Exploring Bounds

Tyler Friedman

April 18, 2015

1 Introduction

An interesting problem in coding theory is determining the maximum number of codewords in a code with certain parameters. For an n -dimensional code, we are interested in the maximum number of codewords such that the code has minimum distance d . Formally, we use the notation $A_q(n, d)$ and $B_q(n, d)$ to define the maximum of number of codewords in a code over \mathbb{F}_q of length n and minimum distance d for an arbitrary (linear or non-linear) code and linear code, respectively.

For arbitrary n and d , it is difficult to find $A_q(n, d)$ and $B_q(n, d)$ exactly. In lecture, we have considered upper bounds—Sphere Packing, Singleton, and Greisner—as well as lower bounds—Gilbert and Varshamov—on these values. The purpose of this paper is to take a survey of other well-known bounds in the literature that we have not discussed. In the first part of the paper, we will consider the Plotkin Upper bound, the Elias Upper bound, and the Linear Programming Upper Bound. In the second part of the paper, we will consider asymptotic versions of Singleton, Plotkin, Hamming, and Elias. (I am very certain that I won't get to discuss all of these bounds, but I am currently unsure how much space each discussion will take up so I've listed all that I am considering.) For each bound, we will consider its proof as well as related examples. Lastly, in the final part we will consider lexicodes, an interesting subset of linear codes that meet the Gilbert Bound.

Some implementation specific details: for the Linear Programming bound, I will introduce basic linear programming concepts and as well as the Krawtchouk polynomials. For the Asymptotic Hamming bound I will introduce the Hilbert entropy function.

2 Upper Bounds

2.1 Plotkin Upper Bound

The Plotkin Bound is an upper bound that often improves upon the Sphere Packing Bound on $A_q(n, d)$.

Theorem 1 (Plotkin). *Let C be an (n, M, d) code over \mathbb{F}_q such that $rn < d$ where $r = 1 - q^{-1}$. Then*

$$A_q(n, d) \leq \left\lfloor \frac{d}{d - rn} \right\rfloor \quad (1)$$

Before proving this bound, it is important to note that it is only valid when d is sufficiently close to n . For large q , this can be a considerable limiting factor. Consider that our restriction is $n < 2d$ for $q = 2$, $n < \frac{3}{2}d$ for $q = 3$, $n < \frac{4}{3}d$ for $q = 4$, etc.

Proof. Let

$$S = \sum_{x \in \mathcal{C}} \sum_{y \in \mathcal{C}} d(x, y) \quad (2)$$

Note that for $x, y \in \mathcal{C}$, $d(x, y) = 0$ for $x = y$, and $d \leq d(x, y)$ for $x \neq y$. This implies that

$$M(M - 1)d \leq S \quad (3)$$

This comes directly from equation 2. We have M possible codewords to consider for x in the outer summation, $M - 1$ distinct codewords from x to consider in the inner summation for y , and the distance between x and y will always be greater than or equal to the minimum distance d .

Next, let \mathcal{M} be the $M \times n$ matrix whose rows are the codewords of \mathcal{C} . For $1 \leq i \leq n$, let $n_{i,\alpha}$ be the number of times $\alpha \in \mathbb{F}_q$ occurs in column i of \mathcal{M} . Note that $\sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha} = M$ for $1 \leq i \leq n$. This is simply because there are M total elements of \mathbb{F}_q in each column, so the sum over all $n_{i,\alpha}$ must necessarily be M .

I claim that we can rewrite S as a double sum over these $n_{i,\alpha}$ values. Specifically,

$$S = \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha} (M - n_{i,\alpha}). \quad (4)$$

Note that $n_{i,\alpha} (M - n_{i,\alpha})$ is multiplying the number of times α occurs in column i by the number of times it doesn't occur in column i . In other words, we're counting the number of times two elements of the same column are not equivalent, exactly the condition that constitutes our Hamming distance. By summing over all α and then all columns, we arrive at the same value generated by 2.

Next, simplify:

$$\begin{aligned} \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha} (M - n_{i,\alpha}) &= M \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha} - \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha}^2 \\ &= nM^2 - \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha}^2 \end{aligned} \quad (5)$$

Recall the Cauchy-Schwarz inequality, which states that $(\sum_{i=1}^n x_i y_i)^2 \leq (\sum_{i=1}^n x_i^2) (\sum_{i=1}^n y_i^2)$. For our purposes, this means that $\left(\sum_{\alpha \in \mathbb{F}_q} 1 \cdot n_{i,\alpha}\right)^2 \leq q \left(\sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha}^2\right)$.

Using this inequality, we obtain

$$S \leq nM^2 - \sum_{i=1}^n q^{-1} \left(\sum_{\alpha \in \mathbb{F}_q} 1 \cdot n_{i,\alpha} \right)^2 = nM^2 - \frac{nM^2}{q} = nrM^2. \quad (6)$$

Combining 3 and 6, we get $M(M-1)d \leq nrM^2$, which simplifies to

$$M \leq \left\lfloor \frac{d}{d - rn} \right\rfloor. \quad (7)$$

□

It is interesting to see exactly how the Sphere Packing and Plotkin bounds compare for specific values of n and d . For the following examples we will assume $q = 2$. Also, recall that if d is even, $A_2(n, d) = A_2(n-1, d-1)$.

Example 2.1.1. $(n, d) = (7, 4)$.

Applying the Sphere Packing bound, we have $A_2(7, 4) = A_2(6, 3) \leq \frac{2^6}{1+6}$, giving us $A_2(7, 4) \leq 9$.

Applying the Plotkin bound, we have $A_2(7, 4) \leq \frac{4}{4 - \frac{1}{2} \cdot 7} = 8$.

Example 2.1.2. $(n, d) = (9, 6)$.

Applying Sphere Packing, we have $A_2(9, 6) = A_2(8, 5) \leq \frac{2^8}{1+8+28}$, giving us $A_2(n, d) \leq 6$.

Applying the Plotkin bound, we have $A_2(9, 6) \leq \frac{6}{6 - \frac{1}{2} \cdot 9} = 4$.

It is also interesting to consider a more broader picture of what is going on here. Below is a graph comparing rates of codes versus the Sphere Packing and Plotkin bounds that we can calculate for those values for different values of q .

balls

3 Asymptotic Bounds

We now wish to consider these $A_q(n, d)$ values as n goes to infinity. To do so, we must more formally define two terms.

In class, we have considered the *rate* of a linear code, k/n , as one measure of the goodness of a code. That is, the rate tells us how much information relative to redundancy that our codewords provide. The concept of rate can be generalized to non-linear codes as well. For a possibly nonlinear code over \mathbb{F}_q with M codewords, the *rate* is defined to be $n^{-1} \log_q M$. Notice that for an $[n, k, d]$ linear code, $M = q^k$ and hence the rate is k/n as we expect.

A second notion of goodness that we have discussed, but I think not formally defined, is the *relative distance* of a code. For a linear or nonlinear code of length n has minimum distance d , this value is the ratio d/n .

Consequently, for our asymptotic bounds, we are interested in the largest possible rate for a family of codes over \mathbb{F}_q of lengths going to infinity with relative distances approaching some constant δ . In other words, we consider the equation:

$$\alpha_q(\delta) = \limsup_{n \rightarrow \infty} n^{-1} \log_q A_q(n, \delta n) \quad (8)$$

[What does this imply?]

3.1 Asymptotic Singleton Bound

Recall the Singleton Bound from lecture:

Theorem 2. For $d \leq n$, $A_q(n, d) \leq q^{n-d+1}$.

[explain what this means, what are the implications]

Theorem 3. If $0 \leq \delta \leq 1$, then $\alpha_q(\delta) \leq 1 - \delta$.

This theorem follows directly from the Singleton bound.

Proof.

$$\begin{aligned} \alpha_q(\delta) &= \limsup_{n \rightarrow \infty} n^{-1} \log_q A_q(n, \delta n) \\ &\leq \limsup_{n \rightarrow \infty} n^{-1} \log_q q^{n-\delta n+1} \\ &\leq \limsup_{n \rightarrow \infty} \frac{n - \delta n + 1}{n} \\ &\leq 1 - \delta \end{aligned} \quad (9)$$

□

3.2 Asymptotic Plotkin Bound

Asymptotic singleton, include 2 examples Asymptotic plotkin, some examples draw graph Asymptotic hamming define hilbert, prove 135,136, define $v_q(n,a)$, black box 2.10.3, prove 2.10.5

Table of common $A_q(n, d)$ values Recall basic theory: thm 2.1.2, 2.1.6

Sections

Elias talk about importance define it prove two lemmas that do the heavy lifting easy proof to finish it off work out some examples

Linear Programming Bound talk about importance define it prove it work out some examples

Note existence of two lower bounds, say we talked about them in class