Introduction to Coding Theory **CMU: Spring 2010**

Notes 4: Elementary bounds on codes

January 2010

Lecturer: Venkatesan Guruswami *Scribe: Venkatesan Guruswami*

We now turn to *limitations* of codes, in the form *upper bounds* on the rate of codes as a function of their relative distance. We will typically give concrete bounds on the size of codes, and then infer as corollaries the asymptotic statement for code families relating rate and relative distance. All the bounds apply for general codes and they do not take advantage of linearity. However, for the most sophisticated of our bounds, the linear programming bound, which we discuss in the next set of notes, we will present the proof only for linear codes as it is simpler in this case.

We recall the two bounds we have already seen. The Gilbert-Varshamov bound asserted the existence of (linear) q-ary codes of block length n, distance at least d, and size at least $\frac{q^n}{\mathrm{Vol}_q(n,d-1)}$. Or in asymptotic form, the existence of codes of rate approaching $1 - h_q(\delta)$ and relative distance δ. The Hamming or sphere-packing bound gave an upper bound on the size (or rate) of codes, which is our focus in these notes. The Hamming bound says that a q-ary code of block length n and distance d can have at most $\frac{q^n}{\mathrm{Vol}_q(n,\lfloor (d-1)/2 \rfloor)}$ codewords. Or in asymptotic form, a q-ary code of relative distance δ can have rate at most $1 - h_q(\delta/2) + o(1)$.

As remarked in our discussion on Shannon's theorem for the binary symmetric channel, if the Hamming bound could be attained, that would imply that we can correct *all* (as opposed to most) error patterns of weight pn with rate approaching $1 - h(p)$. Recall that there are perfect codes (such as the Hamming codes) that meet the Hamming bound. However, these codes have very small distance (3 in the case of Hamming codes). A generalization of Hamming codes called binary BCH codes (the acronym stands for the code's independent inventors Hocquenghem (1959) and Bose and Ray-Chaudhuri (1960)) show that when d is a fixed constant and the block length is allowed to grow, the Hamming bound is again tight up to lesser order terms. However, we will improve upon the Hamming bound and show that its asymptotic form (for any relative distance bounded away from zero) cannot be attained for any fixed alphabet. The proof method has some connections to *list decoding*, which will be an important focus topic later in the course.

1 Singleton bound

We begin with the simplest of the bounds:

Theorem 1 *Let C be a code of block length n and minimum distance d over an alphabet of size q. Then $|C| \le q^{n-d+1}$.*

Proof: Suppose not, and $|C| > q^{n-d+1}$. By the pigeonhole principle there must be two codewords $c_1, c_2 \in C$, $c_1 \neq c_2$ that agree on the first $n - d + 1$ locations. But then $\Delta(c_1, c_2) \le d - 1 < d$, contradicting the hypothesis that C has minimum distance d. □

This gives an alphabet-independent asymptotic upper bound on the rate as a function of relative distance.

Corollary 2 *The rate R and relative distance δ of a code satisfy $R \leq 1 - \delta + o(1)$.*

Though really simple, the Singleton bound is tight in general — we will later see an algebraic family of codes called Reed-Solomon codes which achieve the Singleton bound and have dimension $n - d + 1$ and minimum distance d. The family of codes which meet the Singleton bound are called *maximum distance separable* (MDS) codes.

However, Reed-Solomon and other MDS codes will be (necessarily) defined over an alphabet that grows with the block length. For code families over a fixed alphabet such as binary codes, substantial improvements to the Singleton bound are possible. We turn to such bounds next.

2 The Plotkin bound

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. We now prove an upper bound which shows that the relative distance has to be at most 1/2 (and thus the Hamming bound is quite weak for large δ) unless the code has very few codewords (and in particular has vanishing rate).

While the same underlying ideas are involved, the proofs are simpler to present for the binary case, so we will focus on binary codes. We will state the bound for the q-ary case and leave the details as an exercise. Our proofs reduce the task of bounding the size of the code to bounding the number of pairwise far-apart unit vectors in Euclidean space, and then use a geometric argument for the latter task.

We first state the geometric lemma we need.

Lemma 3 *Let $v_1, v_2, \ldots, v_m$ be m unit vectors in $\mathbb{R}^n$.*

1. *Suppose $\langle v_i, v_j \rangle \leq -\epsilon$ for all $1 \leq i < j \leq m$. Then $m \leq 1 + \frac{1}{\epsilon}$.*
2. *Suppose $\langle v_i, v_j \rangle \leq 0$ for all $1 \leq i < j \leq m$. Then $m \leq 2n$.*

Proof: We only prove the first part, and leave the second as an (interesting) exercise. Note that bound of $2n$ is best possible, as we can take n orthonormal vectors and their negations. For the first part, we have

$$0 \leq \langle \sum_{i=1}^{m} v_i, \sum_{i=1}^{m} v_i \rangle = \sum_{i=1}^{m} \|v_i\|^2 + 2 \sum_{1 \leq i < j \leq m} \langle v_i, v_j \rangle \leq m - m(m-1)\epsilon \ ,$$

which gives $m \leq 1 + 1/\epsilon$. □

Using the above, we can prove that a binary code of block length n and distance $d \geq n/2$ cannot have too many codewords.

Theorem 4 *Let C be a binary code C of block length n and distance d.*

1. *If $d > n/2$, then $|C| \leq \frac{2d}{2d-n}$.*
2. *If $d \geq n/2$, then $|C| \leq 2n$.*

Proof: Let $m = |C|$ and let $c_1, c_2, \ldots, c_m \in \{0,1\}^n$ be the codewords of C. By hypothesis $\Delta(c_i, c_j) \geq d$ for $1 \leq i < j \leq m$. We will map the codewords into unit vectors $v_i \in \mathbb{R}^n$, $i = 1, 2, \ldots, m$, such that the angle between every pair of vectors is at least 90 degrees (i.e., their dot product $\langle v_i, v_j \rangle < 0$). These vectors are defined as follows:

$$v_i = \frac{1}{\sqrt{n}}\left((-1)^{c_i[1]}, (-1)^{c_i[2]}, \cdots, (-1)^{c_i[n]}\right) ,$$

where $c_i[\ell]$ is the ℓ'th bit of the codeword c_i. It is easy to check that

$$\langle v_i, v_j \rangle = \frac{1}{n}(n - 2\Delta(c_i, c_j)) \leq \frac{n-2d}{n} .$$

When $d \geq n/2$, these dot products are non-positive, and by the second part of Lemma 3, we can bound $m \leq 2n$.

For the first part, if $2d > n$, then $\langle v_i, v_j \rangle \leq -\frac{2d-n}{n} < 0$, and therefore by the first part of Lemma 3, we can bound

$$m \leq 1 + \frac{n}{2d-n} = \frac{2d}{2d-n} .$$

□

The above shows that a code family of relative distance $\delta \geq 1/2 + \gamma$ can have at most $O(1/\gamma)$ codewords. Thus a code family cannot have relative distance strictly bounded away from 1/2 with a number of codewords that is growing with the block length. In particular, such code families have zero rate. We now prove that this is also the case if the relative distance is 1/2.

We now use a "puncturing" argument, which implies that the complement of the feasible rate vs relative distance region is convex, to derive an upper bound of rate for relative distances $\delta < 1/2$.

Theorem 5 *If a binary code C has block length n and distance $d < n/2$, then $|C| \leq d \cdot 2^{n-2d+2}$.*

Proof: Let $\ell = n - 2d + 1$ and $S = \{1, 2, \ldots, \ell\}$. For each $a \in \{0,1\}^\ell$, define the subcode C_a to be the subcode of C consisting of all codewords which have a in the first ℓ positions, projected on $S^c = \{1, 2, \ldots, n\} \setminus S$. Formally, $C_a = \{c_{|S^c} \mid c_i = a_i \text{ for } 1 \leq i \leq \ell\}$. Each C_a is a binary code of block length $n - \ell = 2d - 1$. Note that since C has distance at least d, so does C_a. By Theorem 4, $|C_a| \leq 2d$. Of course, $|C| = \sum_{a \in \{0,1\}^\ell} |C_a|$. So we conclude $|C| \leq 2d \cdot 2^\ell = d \cdot 2^{n-2d+2}$. □

We record the asymptotic implication of the above upper bound as:

Corollary 6 *The rate R of a binary code of relative distance δ must satisfy $R \leq 1 - 2\delta + o(1)$.*

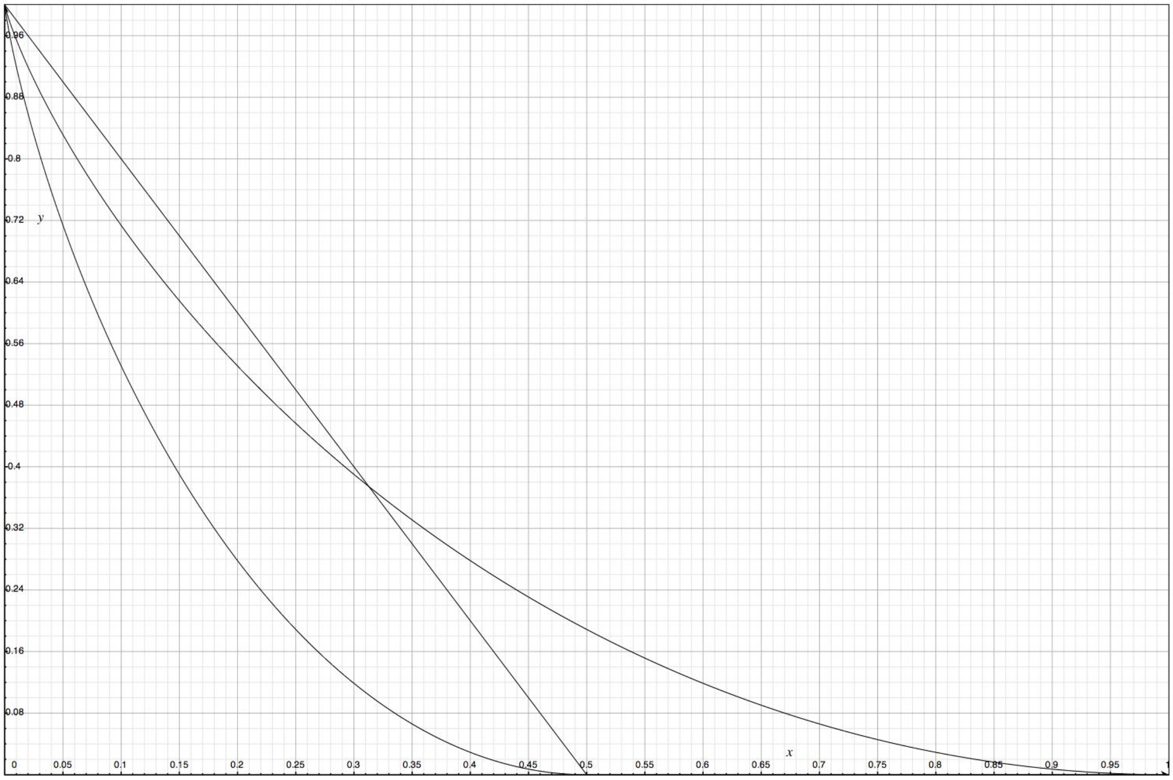
The above arguments can be extended to the q-ary case. The idea is to map q symbols to q unit vectors whose pairwise dot product is exactly $-\frac{1}{q-1}$.

Exercise 1 *Let C be a q-ary code of block length n and minimum distance at least d.*

1. *If $d > (1 - 1/q)n$, then $|C| \leq \frac{qd}{qd-(q-1)n}$.*
2. *When $d < (1 - 1/q)n$, $|C| \leq \frac{q^3 d}{q-1} q^{n-qd/(q-1)}$.*

Deduce that the R of a q-ary code of relative distance δ must satisfy $R \leq 1 - \frac{q}{q-1}\delta + o(1)$.

Here is a plot of the Gilbert-Varshamov lower bound on rate, and the Hamming and Plotkin upper bounds on rate, for binary codes. On the horizontal axis is the relative distance $\delta \in [0, 1]$ and the vertical axis is the rate $R \in [0, 1]$. Any (R, δ) point under the leftmost curve (the Gilbert-Varshamov bound) is achievable, and any (R, δ) point above either the Plotkin bound (the straight line) or the Hamming bound is not achievable. Notice that the Hamming bound is stronger than the Plotkin bound for low distances (or high rates). We now proceed to a bound that improves both the Hamming and Plotkin bounds.



3 Johnson and Elias-Bassalygo bounds

Recall that $A_q(n,d)$ denotes the size of the largest q-ary code of block length n and distance d. We denote by $A_q(n,d,w)$ the size of a largest *constant weight* code of block length n and distance d all of whose codewords have Hamming weight w. We also denote by $A'_q(n,d,w)$ the largest size of a code of block length n and distance d all of whose codewords have Hamming weight *at most* w. For the case $q=2$, we just denote these quantities by $A(n,d)$, $A(n,d,w)$, and $A'(n,d,w)$ respectively.

On your problem set, you are asked to prove the following (just for the binary case).

Exercise 2 *Prove that $A(n,d) \le \frac{2^n}{\binom{n}{w}} A(n,d,w)$. More generally, prove that $A_q(n,d) \le \frac{q^n}{\binom{n}{w}(q-1)^w} A_q(n,d,w)$*

The above gives a method to upper bound the size $A_q(n,d)$ of unrestricted codes via upper bounds on the size $A_q(n,d,w)$ of constant weight codes. Note that when $w < d/2$, $A_q(n,d,w) = 1$, so the Hamming like upper bound $A_q(n,d) \le \frac{q^n}{\binom{n}{w}(q-1)^w}$ is a special case of this. In general the larger the w as a function of d for which we can prove a good upper bound on $A(n,d,w)$ (as either a constant or a polynomial function of n), the better the upper bound on $A_q(n,d)$.

We will now prove such an upper bound, in fact for the more general quantity $A'_q(n,d,w)$. Such a bound, called the *Johnson bound*, is intimately connected to *list decoding*. Proving that $A'_q(n,d,w)$ is small, say at most L which is either a constant or bounded by $n^{O(1)}$, implies that for *every* q-ary code C of block length n and distance d, every Hamming ball of radius w contains at most L codewords of C. In other words, if a codeword is transmitted and at most w errors corrupt it, then one can *list decode* a small list of at most L candidate codewords one of which must equal the original codeword. Of course, for $w < d/2$, we have $L = 1$, and the key here is that one can have $w \gg d/2$ and still ensure a small worst-case *list size* L.

Once we prove the Johnson bound, we will deduce our desired bound on $A_q(n,d)$, called the Elias-Bassalygo bound after their inventors, by appealing to Exercise 2. Our proofs of the Johnson bound will be geometric in nature, relying on Lemma 3. We prove the bounds for binary codes, and leave the extension to larger alphabets as exercises.

3.1 Binary codes

Theorem 7 (Binary Johnson bound) *For integers $1 \le w \le d \le n/2$, if $w \le \frac{1}{2}(n - \sqrt{n(n-2d)})$, then $A'(n,d,w) \le 2n$. (We will often refer to the quantity $\frac{1}{2}(n - \sqrt{n(n-2d)})$ as $J_2(n,d)$, the (binary) Johnson radius.)*

Proof: Let $C = \{c_1, \ldots, c_m\} \subseteq \{0,1\}^n$ be a code such that $\Delta(c_i, c_j) \ge d$ for $i \ne j$, and $\mathrm{wt}(c_i) \le w$ for each $i = 1, 2, \ldots, m$. We will map the codewords c_i into vectors $v_i \in \mathbb{R}^n$ similarly to the proof of the Plotkin bound (Theorem 4), except we won't normalize them to unit vectors here:

$$v_i = \left((-1)^{c_i[1]}, (-1)^{c_i[2]}, \cdots, (-1)^{c_i[n]}\right) ,$$

where $c_i[\ell]$ is the ℓ'th bit of the codeword c_i. Likewise the all 0's vector is mapped to the vector $r \in \mathbb{R}^n$

$$r = (1, 1, \cdots, 1) \; .$$

Let $\alpha > 0$ be a parameter to be picked later. The parameter α will be picked so that all the pairwise dot products $\langle v_i - \alpha r, v_j - \alpha r \rangle$ are nonpositive for $i \neq j$. Now

$$\begin{aligned} \langle v_i - \alpha r, v_j - \alpha r \rangle &= n - 2\Delta(c_i, c_j) + \alpha^2 n + \alpha(2\mathrm{wt}(c_i) - n + 2\mathrm{wt}(c_j) - n) \\ &\leq n - 2d + \alpha^2 n + 2\alpha(2w - n) \; . \end{aligned}$$

The latter quantity is at most 0 provided

$$4w \leq 2n - \left(\alpha n + \frac{n - 2d}{\alpha} \right) \; .$$

The choice $\alpha = \sqrt{n(n-2d)}$ maximizes the right hand side, and leads to the requirement

$$w \leq \frac{n}{2} - \frac{\sqrt{n(n-2d)}}{2}$$

which is met by hypothesis about w. Therefore, for this choice of α, $\langle v_i - \alpha r, v_j - \alpha r \rangle \leq 0$ for $1 \leq i < j \leq m$. are nonpositive for $i \neq j$. Appealing to (the second part of) Lemma 3, we can conclude $m \leq 2n$, and thus $A'(n, d, w) \leq 2n$. $\Box$

Remark 8 *It is possible to improve the upper bound on $A'(n, d, w)$ for $w < J_2(n, d)$ from $2n$ to n by noting that for the choice of parameters $\langle v_i - \alpha r, r \rangle > 0$ for each i. This together with the nonpositive pairwise dot products can be used to improve the geometric upper bound on the number of vectors from $2n$ to n.*

For w slightly less than the Johnson radius $J_2(n, d)$, one can sharpen the upper bound on $A'(n, d, w)$ to a constant independent of n.

Exercise 3 *Prove that when $w \leq \frac{n}{2} - \frac{\sqrt{n(n-2d+2d/L)}}{2}$, $A'(n, d, w) \leq L$.*
*(**Hint**: Follow the above proof, and pick parameters so that the first part of Lemma 3 can be used.)*

Together with Exercise 2, we thus have the following upper bound, called the Elias-Bassalygo bound, on the size (rate) of codes of certain distance (relative distance).

Theorem 9 *For integers $1 \leq d \leq n/2$,*

$$A(n, d) \leq \frac{n 2^{n+1}}{\binom{n}{J_2(n,d)}}$$

where $J_2(n, d) = (n - \sqrt{n(n-2d)})/2$.
Thus a binary code family of relative distance δ has rate at most

$$1 - h\Big(\frac{1-\sqrt{1-2\delta}}{2}\Big) + o(1) \ .$$

3.2 Statement for larger alphabets

As with the Plotkin bound, we leave the extension of the Johnson and Elias-Bassalygo bounds to larger alphabets exercises. The hint is to map q symbols into appropriate vectors in $\mathbb{R}^q$ so that large distance between codewords translates into small dot product between their associated vectors.

Exercise 4 *For all integers $q \geq 2$ and $1 \leq d \leq (1-1/q)n$, $A'_q(n,d,w) \leq n(q-1)$ provided*

$$w < J_q(n,d) = n\Big(1-\frac{1}{q}\Big)\left(1-\sqrt{1-\frac{qd}{(q-1)n}}\right) \ .$$

Further, if

$$w \leq n\Big(1-\frac{1}{q}\Big)\left(1-\sqrt{1-\frac{qd(1-\epsilon)}{(q-1)n}}\right)$$

then $A'_q(n,d,w) \leq 1/\epsilon$.

Together with Exercise 2, this gives the Elias-Bassalygo upper bound for q-ary codes:

Theorem 10 *A q-ary code family of relative distance δ has rate at most*

$$1 - h_q\left((1-1/q)\Big(1-\sqrt{1-\frac{q\delta}{q-1}}\Big)\right) + o(1) \ .$$

3.3 Alphabet oblivious bound for Johnson radius

When discussing list decoding of codes such as Reed-Solomon codes which are defined over an alphabet size that grows with the block length, it will be useful to have the following ”alphabet oblivious” version of the Johnson bound. (This version is also a simpler and often good enough approximation to the q-ary Johnson radius when q is somewhat large.)

Theorem 11 *Let $C \subseteq \Sigma^n$ be a code of block length n and distance d. Then the following hold:*

1. *Every Hamming ball of radius at most*

$$J(n,d) = n - \sqrt{n(n-d)}$$

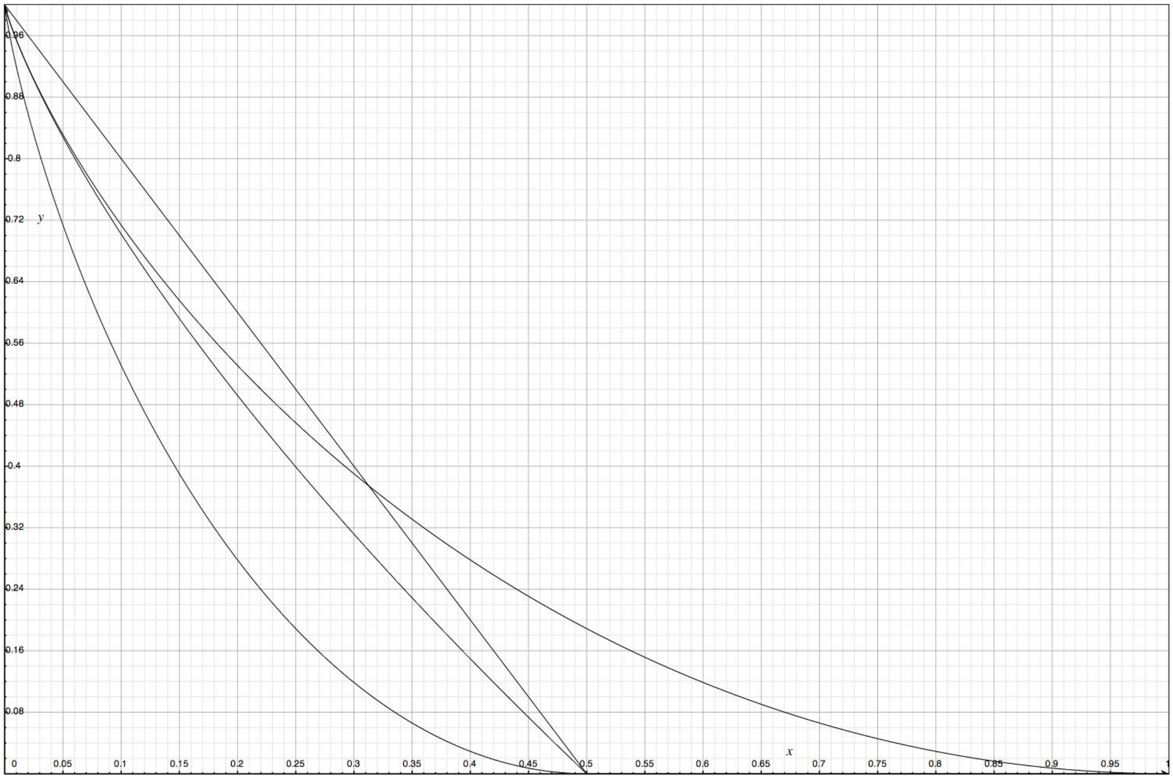
   in Σ^n has at most $O(n|\Sigma|)$ codewords of C.

2. *Every Hamming ball of radius at most* $n - \sqrt{n(n-d+d\epsilon)}$ *in* Σ^n *has at most* $1/\epsilon$ *codewords of* C.

The above statement follows from Exercise 4 by verifying that for every $q \geq 2$ and $0 \leq x \leq 1 - 1/q$,

$$1 - \sqrt{1-x} \leq (1-1/q)\sqrt{1 - \frac{qx}{q-1}}\ .$$

We conclude with a plot that adds the Elias-Bassalygo upper bound to the earlier plot. Note that this bound improves on both the Hamming and Plotkin bounds, but for small distances the difference between the Hamming the Elias-Bassalygo bounds is small.


0.96
0.88
0.8
0.72
y
0.64
0.56
0.48
0.4
0.32
0.24
0.16
0.08
x
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5
0.55
0.6
0.65
0.7
0.75
0.8
0.85
0.9
0.95
1