Summary: In this lecture we study some of the bounds on codes - conditions on their parameters based on the structure of codes. The concept of Hamming spheres is introduced to help arrive at some of these bounds.
References: Ch.1.§10, *Theory of Error-Correcting Codes* by *F.J. MacWilliams and N.J.A Sloane*

Introduction. Linear codes are notated as $[n, k, d]_q$. n represents the number of coordinates in a codeword and k represents the number in coordinates of a message word. d is the minimum Hamming distance between codewords while q is the alphabet over which codewords are constructed. Arbitrary codes are notated as $(n, M, d)_q$ where n, q and d are as before and M represents the number of codewords. The minimum error correcting property of linear codes states that $d \geq 2t + 1$ where t represents the number of correctable errors.

Theorem 1 (Singleton Bound)**.** *The Singleton (upper) bound on the number of codewords, M of an $(n, M, d)_q$ code is given by:*

$$M \leq q^{n-(d-1)}$$

Alternatively expressed for $M = q^k$ codewords,

$$k \leq n - (d - 1)$$

This bound is valid for both linear as well as arbitrary codes.

Proof. Consider a $(n, M, d)_q$ code. By definition of the minimum Hamming distance d, any two codewords c_1 and c_2 would differ in at least d coordinates. Thus, if at most any $d - 1$ coordinates are dropped from all codewords, any two such reduced length vectors would still be distinct. These smaller length vectors would have $n - (d - 1)$ coordinates and thus would be $q^{n-(d-1)}$ in number. For the minimum distance to be d, each of the codewords in the original code should be mapped to a unique smaller length vector. If the number of codewords is more than $q^{n-(d-1)}$, two vectors can be found that map to the same smaller length vector (which are $q^{n-(d-1)}$ in number). This would mean that they differ in less than or equal to $d - 1$ coordinates violating the minimum distance of the code. Thus, for all of the codewords of the original code to be distinct with minimum Hamming distance d,

$$M \leq q^{n-(d-1)}$$

and for $M = q^k$ codewords,

$$k \leq n - (d - 1)$$

□

Definition 1 (Hamming Sphere)**.** *For any vector $v_0 \in \mathbb{F}_q^n$, a Hamming sphere is defined as:*

$$\mathbb{H}_{q,r}(n, v_0) = \{v \in \mathbb{F}_q^n \mid d(v, v_0) \leq r\}$$

It is a set representing all the vectors lying within a Hamming distance r from v_0, the center of the Hamming sphere.

Volume of a Hamming Sphere. The volume of a Hamming sphere counts the number of vectors lying inside it. The volume of a Hamming sphere, $\mathbb{H}_{q,r}(n, v_0)$ is given by:

$$V_q(n, r) = \sum_{j=0}^{r} \binom{n}{j} (q - 1)^j$$

Proof. Consider an n-coordinate vector v_0, the center of the Hamming sphere. The number of ways of choosing all the vectors a distance j away from v_0 is: $\binom{n}{j}$ (ways of choosing j coordinates out of n) times $(q-1)^j$ where any of the other $(q - 1)$ alphabets can now occupy each of these j positions. Thus summing over j till $j = r$ gives the number of vectors lying within a distance r from v_0. □

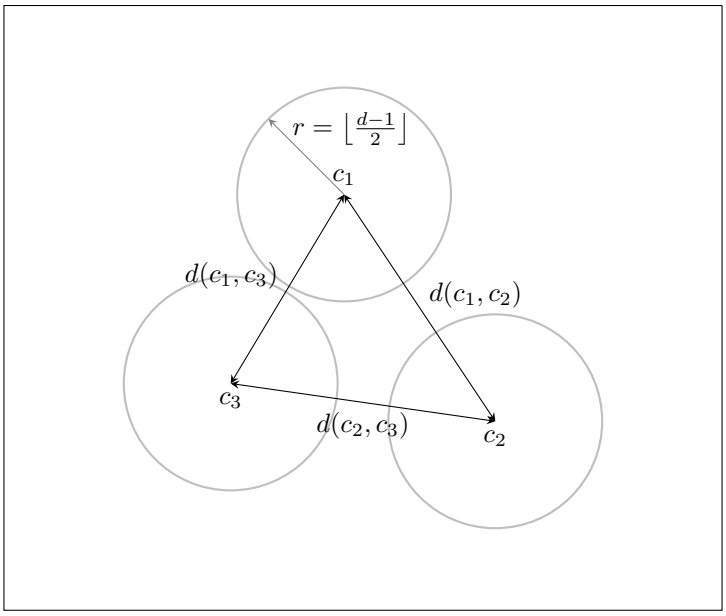

Figure 1: Hamming Bound
$d(c_1, c_3), d(c_1, c_3), d(c_2, c_3) \geq d > 2 \lfloor \frac{d-1}{2} \rfloor$

Let us now look at some bounds on arbitrary codes based on the properties of Hamming spheres.

Theorem 2 (Hamming Bound)**.** *The Hamming bound on the number of codewords of an $(n, M, d)_q$ code is given by:*

$$M \leq \frac{q^n}{\sum_{j=0}^{t} \binom{n}{j} (q-1)^j}$$

Where,

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

The Hamming bound is valid for both linear as well as non-linear codes.

Proof. Consider an $(n, M, d)_q$ code. Construct a Hamming sphere around every codeword of radius $r = \lfloor \frac{d-1}{2} \rfloor$.

Claim. No two such Hamming spheres can have common codewords

Assume that two Hamming spheres surrounding c_1 and c_2 intersect and c is a code common to both of them. From the Triangle Inequality,

$$d \leq d(c_1, c_2) \leq d(c, c_1) + d(c, c_2) \tag{1}$$

However, by assumption that c lies in both spheres,

$$d(c, c_1), d(c, c_2) \leq r = t \tag{2}$$

From (1) and (2),

$$\implies d \leq 2t$$

Which contradicts the minimum error correcting property of the code, $d \geq 2t + 1$.
The total volume (number of codes) enclosed in these M Hamming spheres should be less than the total number of

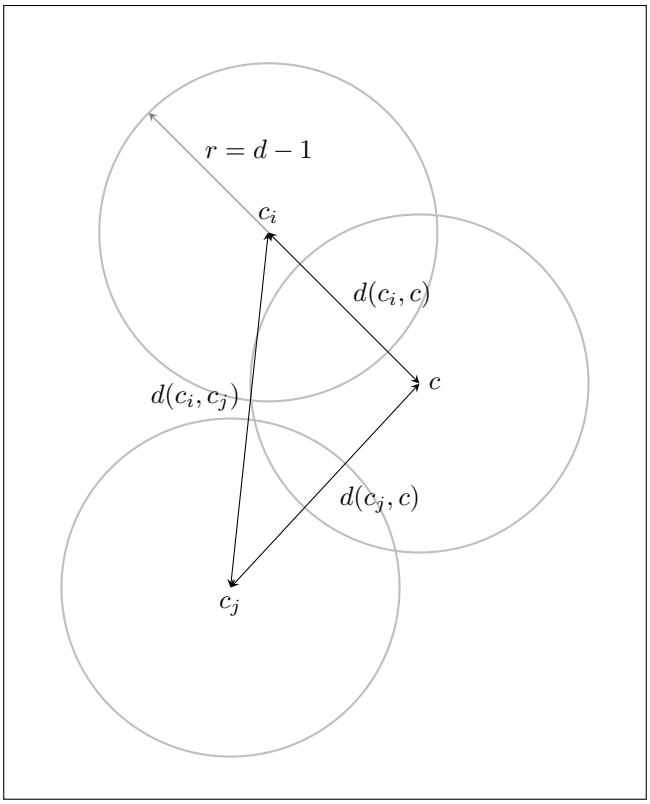

Figure 2: Gilbert Bound
$\exists\, c \in \mathbb{F}_q^n; i, j \ni c \in \mathbb{H}_{q,r}(n, c_i)\ and\ c \in \mathbb{H}_{q,r}(n, c_j)$

available codewords. Thus,

$$M. \sum_{j=0}^{t} \binom{n}{j} (q-1)^j \leq q^n$$

□

While the Hamming and singleton bounds both give upper bounds on the number of codewords, the Gilbert bound provides a lower bound on the maximum number of codewords in a code. Not all codes will satisfy this bound i.e. if it does not have the maximum number of codewords for a given n and d, the bound may not be reached.

Theorem 3 (Gilbert Bound)**.** *Let the maximum number of codewords of a code of length n and minimum distance d be represented as $A_q(n, d)$. The Gilbert (lower) bound on $A_q(n, d)$ is given by:*

$$A_q(n, d) \geq \frac{q^n}{\sum_{j=0}^{d-1} \binom{n}{j} (q-1)^j}$$

Proof. Consider an $(n, M, d)_q$ code. Construct a Hamming sphere around every valid codeword of radius $r = d - 1$.

Claim. These spheres collectively exhaust the codespace for a code with maximum number of codewords given n, d.

Consider those vectors that do not lie inside any of the Hamming spheres around the codewords. If such a vector does exist then it must lie a distance greater than $d - 1$ (or greater than or equal to d) away from every codeword. If this vector is also included in the set of codewords we would now have a new code of the same n and distance d.

Thus a Hamming sphere of the same radius $r = d - 1$ can be constructed around this new codeword. Progressing as above, we can exhaust all the vectors that do not belong to any of the existing Hamming spheres by making it into a codeword and subsequently constructing a Hamming sphere of $r = d - 1$ around it. The resultant code would still have a distance d as all codewords are separated by at least d units. Once all such vectors have been exhausted, converting any other vector into a codeword would reduce the minimum distance of the code as there are no more vectors at a distance greater than or equal to d from all codewords. Thus, this maximal code (with maximum number of codewords) is covered by Hamming spheres that collectively exhaust the code-space with no vectors lying outside any of the spheres.

Claim. Not all of these Hamming spheres are mutually exclusive.

This is a result of the fact that there exist two codewords separated by a distance d. Considering the Hamming spheres around them, the distance between their centers is d which is less than or equal to the sum of their radii, $2(d-1)$. So these two spheres must have at least 1 vector common between them and thus, not all of these Hamming spheres are mutually exclusive.

From the above claims, we can conclude that these Hamming spheres collectively exhaust the volume of the code space and are not all mutually exclusive. This means that the total volume (number) of vectors enclosed within these spheres is larger than the total volume of the code-space, as, in adding the volumes, some codewords would be added more than once. Mathematically,

$$A_q(n,d).\sum_{j=0}^{d-1}\binom{n}{j}(q-1)^j \geq q^n$$

$$\implies A_q(n,d) \geq \frac{q^n}{\sum_{j=0}^{d-1}\binom{n}{j}(q-1)^j}$$

□

Let us now look at an existence criterion for a code with a given n, q and k. The Varshamov bound conditions over the given n and k values to tell if a code of a particular minimum distance d can be generated.

Theorem 4 (Varshamov Bound)**.** *The Varshamov bound on a linear code states that if:*

$$\sum_{j=1}^{d-2}\binom{n-1}{j}(q-1)^j \leq q^{n-k}-1$$

Then, there exists a $[n,k]_q$ linear code with minimum distance at least d.

Proof. The parity check matrix of an $[n,k,d]_q$ linear code, H is of dimension $n-k \times n$.

$$\begin{bmatrix} h_1 & h_2 & h_3 & \dots & h_n \\ \vdots & \vdots & \vdots & & \vdots \end{bmatrix}$$

Let us try to construct a valid H with distance d. This would show existence of a code of minimum distance d. Assume that i of the n columns are in place, such that there are $d-2$ linearly independent columns so far. A new column appended to the end of the parity check matrix can either be a linear combination of these any $d-2$ of these i columns or can be a linearly independent. However for the minimum distance of the appended parity matrix (with $(i+1)$ columns) to be d , the final column should not be a linear combination of any of the $d-1$ independent columns of H. For a binary code, the number of such *invalid* columns is Θ which is less than the number of linear combinations of the i columns is (as some linear combinations may give the same result).

The number of possibilities for the $(i+1)^{th}$ column in total for a binary code is: $2^{n-k}-1$ as each column has $n-k$ elements (number of rows in the parity check matrix), excluding the zero column. Thus, we can construct the $(i+1)^{th}$

column provided the condition $\Theta < 2^{n-k} - 1$ (number of invalid columns $<$ total number of possible columns) holds true and the parity check matrix can be constructed from any of the remaining allowed possibilities. However,

$$\Theta \leq \binom{i}{1} + \binom{i}{2} + \cdots + \binom{i}{d-2} \leq \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{d-2}$$

Thus if

$$\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{d-2} < 2^{n-k} - 1$$

holds good then $\Theta < 2^{n-k} - 1$ would be valid showing a non zero number of possibilities for the $(i+1)^{th}$ column. Correspondingly a parity check matrix can be constructed with minimum Hamming distance at least d (as more independent columns may be found beyond position $(i+1)$, increasing the minimum distance). Extending this to a q-ary linear block code, the Varshamov bound becomes:

$$\sum_{j=1}^{d-2} \binom{n-1}{j} (q-1)^j \leq q^{n-k} - 1$$

For the existence of a linear code with minimum Hamming distance at least d. □