Coding Theory: Bounds

- Sphere Packing Bound

- Sphere Packing Bound

  There are many bounds on $(n, k, d)_q$ linear codes, we will see two more: the Gilbert bound and the Singleton bound.

- Sphere Packing Bound

  There are many bounds on $(n, k, d)_q$ linear codes, we will see two more: the Gilbert bound and the Singleton bound.

Recall: $A_q(n, d)$ = number of codewords in a code over $\mathbb{F}_q$ of length n and minimum distance at least d.
$B_q(n, d)$ = number of codewords in a linear code over $\mathbb{F}_q$ of length n and minimum distance at least d.

The Gilbert Bound

Recall that the Sphere Packing Bound is an upper bound on $A_q(n, d)$:

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

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

The Gilbert Bound is a lower bound.

The Gilbert Bound

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

The Sphere Packing Bound:

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

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

Covering radius

Recall:

Packing radius = The largest radius of spheres centered at codewords so that the spheres are pairwise disjoint.

Covering radius

Recall:

Packing radius = The largest radius of spheres centered at codewords so that the spheres are pairwise disjoint.

When codes are not perfect, in order to fill $\mathbb{F}_q^n$ with spheres centered at codewords, the spheres must have radius larger than $t = \lfloor \frac{d-1}{2} \rfloor$. Then not all spheres will be pairwise disjoint.

Covering radius

$\rho = \rho(\mathcal{C})$ is the smallest integer s such that $\mathbb{F}_q^n$ is the union of the spheres of radius s centered at the codewords of $\mathcal{C}$.

Packing radius = The largest radius of spheres centered at codewords so that the spheres are pairwise disjoint.

Covering radius

$\rho = \rho(\mathcal{C})$ is the smallest integer s such that $\mathbb{F}_q^n$ is the union of the spheres of radius s centered at the codewords of $\mathcal{C}$.

Packing radius = The largest radius of spheres centered at codewords so that the spheres are pairwise disjoint.

A code $\mathcal{C}$ is perfect if and only if its covering radius equals its packing radius ($t = \rho(\mathcal{C})$).

- Otherwise, the covering radius is larger than the packing radius ($t \leq \rho(\mathcal{C})$).

Covering radius

$\rho = \rho(\mathcal{C})$ is the smallest integer s such that $\mathbb{F}_q^n$ is the union of the spheres of radius s centered at the codewords of $\mathcal{C}$.

The covering radius $\rho(\mathcal{C})$ of a code $\mathcal{C}$, linear or not, is at most $d-1$.

Suppose by contradiction that $\rho(\mathcal{C}) \geq d$.
Then spheres of radius $d-1$ are not covering $\mathbb{F}_q^n$, and there must be at least one vector $\mathbf{x}$ which is in none of these spheres.
Create a new code $\mathcal{C}' = \mathcal{C} \cup \{\mathbf{x}\}$.
Then $|\mathcal{C}'| = |\mathcal{C}| + 1$, and the minimum Hamming distance of $\mathcal{C}'$ is still d, since $\mathbf{x}$ is at distance at least d from all other codewords.
Iterate with $\mathcal{C}'$ instead of $\mathcal{C}$.

The Gilbert Bound

$B_q(n,d) \geq \frac{q^n}{\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i}$.

For $\mathcal{C}$ a linear code with $B_q(n,d)$ codewords:

- The covering radius of $\mathcal{C}$ is at most $d-1$.
- The spheres of radius $d-1$ about the codewords cover $\mathbb{F}_q^n$ by definition.
- A sphere of radius $d-1$ centered at a codeword contains $\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i$ vectors.
- The $B_q(n,d)$ spheres must fill the space.

$$\frac{q^n}{\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i} \le B_q(n,d) \le \frac{q^n}{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i},\ t = \lfloor \frac{d-1}{2} \rfloor$$

$$\frac{q^n}{\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i} \leq B_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i},\ t = \lfloor\frac{d-1}{2}\rfloor$$

For $q = 2$:

$$\frac{2^n}{\sum_{i=0}^{d-1}\binom{n}{i}} \leq B_2(n,d) \leq \frac{2^n}{\sum_{i=0}^{t}\binom{n}{i}},\ t = \lfloor\frac{d-1}{2}\rfloor$$

For $q = 2$ and $n = 5$:

$$\frac{2^5}{\sum_{i=0}^{d-1} \binom{5}{i}} \leq B_2(5, d) \leq \frac{2^5}{\sum_{i=0}^{t} \binom{5}{i}}, \ t = \lfloor \frac{d-1}{2} \rfloor$$

For $q=2$ and $n=5$:

$$\frac{2^5}{\sum_{i=0}^{d-1}\binom{5}{i}} \leq B_2(5,d) \leq \frac{2^5}{\sum_{i=0}^{t}\binom{5}{i}},\ t=\lfloor\frac{d-1}{2}\rfloor$$

$d=2$: $\frac{2^5}{1+5} \approx 5.3 \leq B_2(5,2) \leq 2^5 = 32$ $B_2(5,2)=8,16,32$

$d=3$: $\frac{2^5}{1+5+10} = 2 \leq B_2(5,3) \leq \frac{2^5}{1+5} \approx 5.3$ $B_2(5,3)=2,4$

$d=4$: $\frac{2^5}{1+5+10+10} \approx 1.23 \leq B_2(5,4) \leq \frac{2^5}{1+5} \approx 5.3$
$B_2(5,4)=2,4$

Exercise. Is there a binary code with parameters $(5, 2, 2)$?

Exercise. Is there a binary code with parameters $(5,2,2)$?

The bounds tell us:

$$d=2\colon\ \frac{2^5}{1+5} \approx 5.3 \le B_2(5,2) \le 2^5 = 32$$

So for $n=5$ and $d=2$, we need at least 6 codewords (in fact 8 for a linear code), so no, such a code ($k=2$ means 4 codewords) does not exist.

Exercise. Is there a binary code with parameters $(5, 2, 2)$?

The bounds tell us:

$$d = 2\colon\ \frac{2^5}{1+5} \approx 5.3 \leq B_2(5, 2) \leq 2^5 = 32$$

So for $n = 5$ and $d = 2$, we need at least 6 codewords (in fact 8 for a linear code), so no, such a code ($k = 2$ means 4 codewords) does not exist.

Fitting the parameters does not guarantee the existence.

The Singleton Bound

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

We want to prove that $k \leq n - d + 1 \iff d \leq n - (k-1)$.

Project all the codewords on the first $k-1$ coordinates. Since there are q^k different codewords, by the pigeon-hole principle, at least two of them should agree on these $k-1$ coordinates.

These then disagree on at most the remaining $n-(k-1)$ coordinates. Hence the minimum distance d of the code is $d \leq n - (k-1)$.

The Singleton Bound

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

We want to prove that $k \leq n - d + 1 \iff d \leq n - (k - 1)$.

Consider the $(4, 2, 3)$ tetracode over $\mathbb{F}_3$.
We have

$$k = 2 \leq n - d + 1 = 4 - 3 + 1$$

Maximum Distance Separable (MDS) codes

Codes whose parameters are meeting the Singleton bound.

MDS Codes

So far?

MDS $\iff k = n - d + 1$

$(n, k, d_H)_q$	k/n	name	MDS
$(n, 1, n)_q$	$\frac{1}{n}$	repetition	yes
$(n, n-1, 2)_q$	$\frac{n-1}{n}$	parity check	yes
$(\frac{q^r-1}{q-1}, n-r, 3)_q$	$\frac{n-r}{n}$	Hamming	
$(24, 12, 8)_2$	$\frac{1}{2} = 0.5$	$\mathcal{G}_{24}$	no
$(23, 12, 7)_2$	$\frac{12}{23} \approx 0.52$	$\mathcal{G}_{23}$	no
$(12, 6, 6)_3$	$\frac{1}{2} = 0.5$	$\mathcal{G}_{12}$	no
$(11, 6, 5)_3$	$\frac{6}{11} \approx 0.545$	$\mathcal{G}_{11}$	no
$(2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r})_2$		$\mathcal{R}(r, m)$	

MDS Codes

So far?

MDS $\iff k = n - d + 1$

$(n,k,d_H)_q$	k/n	name	MDS
$(n,1,n)_q$	$\frac{1}{n}$	repetition	yes
$(n,n-1,2)_q$	$\frac{n-1}{n}$	parity check	yes
$(\frac{q^r-1}{q-1}, n-r, 3)_q$	$\frac{n-r}{n}$	Hamming	
$(24,12,8)_2$	$\frac{1}{2} = 0.5$	$\mathcal{G}_{24}$	no
$(23,12,7)_2$	$\frac{12}{23} \approx 0.52$	$\mathcal{G}_{23}$	no
$(12,6,6)_3$	$\frac{1}{2} = 0.5$	$\mathcal{G}_{12}$	no
$(11,6,5)_3$	$\frac{6}{11} \approx 0.545$	$\mathcal{G}_{11}$	no
$(2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r})_2$		$\mathcal{R}(r,m)$	

To find more MDS codes, we need more alphabets (than $\mathbb{F}_p$, $\mathbb{F}_4$).

Gilbert Bound

Singleton Bound

Maximum distance separable (MDS)