Bounds for codes (Chap. 13)

Let's understand more about the tradeoffs in trying to make (n,m,d) q-ary codes and $[n,k,d]$ $\mathbb{F}_q$-linear codes

have both $\begin{cases} d \text{ large} & \text{(for error-correction)} \\ m \text{ or } k \text{ large relative to } n & \left(\text{for high } q\text{-ary rate } \frac{\log_q(m)}{n} \text{ or } \frac{k}{n}\right) \end{cases}$

We will give

- 3 general upper bounds on m in (n,m,d) relative to d and n
  (Hamming §13.1, Singleton §13.3, Plotkin bounds) notice Garrett
- 1 lower bound for k in $[n,k,d]$ relative to d and n
  (Gilbert-Varshamov §13.2 bound)

Hamming's sphere-packing bound (§13.1)

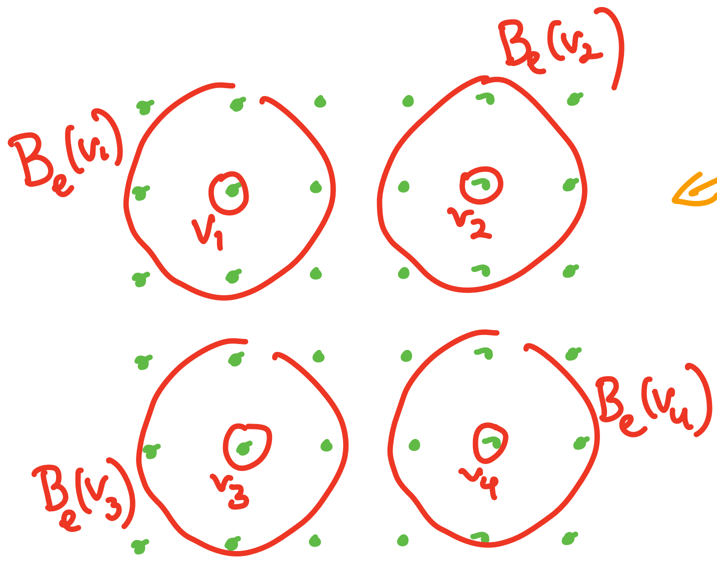
THEOREM In any $(n, m, 2e+1)$ q-ary code, corrects up to e errors

$$m \le \frac{q^n}{1+(q-1)\binom{n}{1}+(q-1)^2\binom{n}{2}+\dots+(q-1)^e\binom{n}{e}}$$

proof: In order for $\mathcal{C} \subset \Sigma^n$ to correct e errors, the $m = |\mathcal{C}|$ different Hamming balls of radius e around codewords $v \in \mathcal{C}$

$$B_e(v) := \{ w \in \Sigma^n : d(v,w) \le e \}$$

must all be disjoint inside Σ^n.



just a cartoon — not what Hamming balls really look like!

Note that each of these $B_e(v)$ has the same number of words from Σ^n: since $q = |\Sigma|$,

$$\#B_e(v) = \overset{v \text{ itself}}{1} + \overbrace{\binom{n}{1}(q-1)^1}^{\text{words distance 1 from } v} + \overbrace{\binom{n}{2}(q-1)^2}^{\text{words distance 2 from } v} + \dots + \overbrace{\binom{n}{e}(q-1)^e}^{\text{words distance } e \text{ from } v}$$

pick 1 letter of v to change — pick its new value — pick 2 letters of v to change — pick their new values — ... etc

Disjointness inside Σ^n implies

$$\# \Sigma^n \geq \sum_{v \in \mathcal{C}} \#B_e(v) = |\mathcal{C}| \cdot \#B_e(v)$$

$$q^n \geq m \cdot \left(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \dots + \binom{n}{e}(q-1)^e\right)$$

Now divide by the sum in parentheses. ∎

EXAMPLE If I want a $(10, m, 7)$ binary code, (corrects 3 errors)
how many words does Hamming bound limit me to?

$$m \leq \frac{2^{10}}{1 + \binom{10}{1}(2-1)^1 + \binom{10}{2}(2-1)^2 + \binom{10}{3}(2-1)^3} = \frac{1024}{1+10+45+120} = \frac{1024}{176} < 6$$

so $m \leq 5$. Not very many codewords!

When $\mathcal{C}$ achieves equality in the Hamming bound, the balls $B_e(v)$ for $v \in \mathcal{C}$ disjointly cover Σ^n, and $\mathcal{C}$ is called a perfect (e-)code.

This is quite rare, but some exist.

EXAMPLE Hamming's $[n, k, 3]$ $\mathbb{F}_q$-linear codes are perfect 1-codes

$$n = \frac{q^r-1}{q-1}, \quad k = \frac{q^r-1}{q-1} - r = n-r, \quad 3 \leftarrow \text{so } e=1$$

since $m = q^k = q^{n-r}$ ← equality!

while Hamming's bound said

$$m \le \frac{q^n}{1+\binom{n}{1}(q-1)} = \frac{q^n}{1+n(q-1)} = \frac{q^n}{1+(q^r-1)} = \frac{q^n}{q^r} = q^{n-r}$$

EXAMPLE M. Golay wrote down 4 very special linear codes in 1948, called the Golay codes:

used in Voyager 1979–81 Jupiter & Saturn fly-bys

G_{24} is $[24, 12, 8]$ and $\mathbb{F}_2$-linear

G_{23} is $[23, 12, 7]$ $\mathbb{F}_2$-linear a perfect 3-code

G_{12} is $[12, 6, 6]$ $\mathbb{F}_3$-linear

G_{11} is $[11, 6, 5]$ $\mathbb{F}_3$-linear a perfect 2-code

(See John Baez cool blog post on syllabus!)

It was actually proven in 1973 by Tietäväinen that there are no other $\mathbb{F}_q$-linear perfect codes, up to permuting the coordinates in $(\mathbb{F}_q)^n$

[Except for some degenerate exceptions:

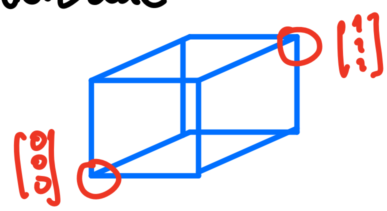
$C = \{\underline{0}\} \subset (\mathbb{F}_q)^n$ is always $[n, 0, n]$

and perfect but useless!

$C = \{\underline{0}, \underline{1}\} \subset (\mathbb{F}_2)^n$ is always $[n, 1, n]$

binary repetition code

and a perfect e-code if $n = 2e+1$ is odd]



So for linear perfect codes other than binary repetition, the error-correction $e \leq 3$, not very large.

There do exist other non-linear perfect codes.

The Singleton bound (§13.3)

THEOREM:
In any (n,m,d) q-ary code, $m \leq q^{n-(d-1)}$.
So in any $[n,k,d]$ $\mathbb{F}_q$-linear code, $k \leq n-(d-1)$.

---

proof: Let $\mathcal{C} = \{v = (v_1, \ldots, v_n) : v \in \mathcal{C}\} \subset \Sigma^n$ be such an (n,m,d) q-ary code and consider $\hat{\mathcal{C}} = \{ \hat{v} = \underbrace{(v_1, \ldots, v_{n-(d-1)})}_{\text{truncations of the words in } \mathcal{C} \text{ to their 1st } n-(d-1) \text{ positions}} : v \in \mathcal{C}\} \subset \Sigma^{n-(d-1)}$.

We claim that the shorter words $\hat{v}, \hat{v}'$ are all distinct in $\hat{\mathcal{C}}$: if $\hat{v} = \hat{v}'$ then their corresponding words v, v' in $\mathcal{C}$ would have $d(v,v') \leq d-1 < d = d(\mathcal{C})$, a contradiction.

Hence $|\mathcal{C}| = |\hat{\mathcal{C}}| \leq |\Sigma^{n-(d-1)}| = q^{n-(d-1)}$ ∎

EXAMPLE Suppose as before, I want a $(10, m, 7)$ binary code. How severely does Singleton's bound limit $m = |\mathcal{C}|$?

$$m \le 2^{10-(7-1)} = 2^4 = 16,$$

so not as stringent as Hamming's bound $m \le 5$.

(But in other cases, Singleton's bound can be more stringent than Hamming's)

DEF'N: If $\mathcal{C}$ is an (n, m, d) code achieving equality $m = q^{n-(d-1)}$ in Singleton's bound, it is called a maximum distance separable code. (or MDS code)

EXAMPLES

(1) Repetition codes are always $(n, \underset{q}{\underset{\parallel}{m}}, \underset{n}{\underset{\parallel}{d}})$ MDS q-ary codes

$$\mathcal{C} = \left\{ \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}, \ldots, \begin{bmatrix} q-1 \\ q-1 \\ \vdots \\ q-1 \end{bmatrix} \right\} \qquad \text{(or } [n, 1, n] \ \mathbb{F}_q\text{-linear)}$$

since $m = q^{n-(d-1)}$,

$$\underset{q}{\underset{\parallel}{m}} = \underset{q}{\underset{\parallel}{q^{n-(n-1)}}}$$

(2) MDS codes with $d=n-1$ have $m = q^{n-(n-1-1)} = q^2$

and relate to $q \times q$ Latin squares (Sestinas! Sudoku!) for $n=3$

pairs of mutually orthogonal $q \times q$ Latin squares for $n=4$

also called Graeco-Latin Squares

triples of — " ——— for $n=5$

The $n=3$ case...

DEF'N: A $q \times q$ Latin square has each of the q letters of Σ appearing exactly once in each row and in each column.

$q=4$ A 4×4 Latin square

rows \ columns	0	1	2	3
0	0	1	2	3
1	3	0	1	2
2	2	3	0	1
3	1	2	3	0

$\Longleftrightarrow$ $\mathcal{C} =$

row	column	entry
0	0	0
0	1	1
0	2	2
0	3	3
1	0	3
1	1	0
1	2	1
1	3	2
2	0	2
2	1	3
2	2	0
2	3	1
3	0	1
3	1	2
3	2	3
3	3	0

$\subset \Sigma^3 = \{0,1,2,3\}^3$

$(\overset{n}{3}, \overset{m}{q^2}, \overset{d}{2})$ MDS q-ary code

	1	2	3	4	5	6	7	8	9
A	9	2	6	1	7	8	4	3	5
B	8	5	1	9	4	3	2	7	6
C	4	7	3	6	5	2	9	8	1
D	2	1	9	4	6	7	3	5	8
E	7	3	4	8	9	5	6	1	2
F	6	8	5	2	3	1	7	4	9
G	5	6	8	7	2	4	1	9	3
H	3	4	2	5	1	9	8	6	7
I	1	9	7	3	8	6	5	2	4

Sudokus are 9x9 Latin Squares with even more structure

Sestina
by Elizabeth Bishop

September rain falls on the house.
In the failing light, the old grandmother
sits in the kitchen with the child
beside the Little Marvel Stove,
reading the jokes from the almanac,
laughing and talking to hide her tears.

She thinks that her equinoctial tears
and the rain that beats on the roof of the house
were both foretold by the almanac,
but only known to a grandmother.
The iron kettle sings on the stove.
She cuts some bread and says to the child,

It's time for tea now; but the child
is watching the teakettle's small hard tears
dance like mad on the hot black stove,
the way the rain must dance on the house.
Tidying up, the old grandmother
hangs up the clever almanac

on its string. Birdlike, the almanac
hovers half open above the child,
hovers above the old grandmother
and her teacup full of dark brown tears.
She shivers and says she thinks the house
feels chilly, and puts more wood in the stove.

It was to be, says the Marvel Stove.
I know what I know, says the almanac.
With crayons the child draws a rigid house
and a winding pathway. Then the child
puts in a man with buttons like tears
and shows it proudly to the grandmother.

But secretly, while the grandmother
busies herself about the stove,
the little moons fall down like tears
from between the pages of the almanac
into the flower bed the child
has carefully placed in the front of the house.

Time to plant tears, says the almanac.
The grandmother sings to the marvelous stove
and the child draws another inscrutable house.

The line-ending words in the six main stanzas of a sestina repeat in a 6x6 Latin square pattern:

A B C D E F
F A E B D C
C F D A B E
E C B F A D
D E A C F B
B D F E C A

The Plotkin bound (Roman §4.5, not in Garrett)

This one is only relevant when d is pretty large as a fraction of n (= block length), but is believed to be a very tight bound on m.

THEOREM: If $\mathcal{C}$ is an (n,m,d) q-ary code and $d > \left(1-\frac{1}{q}\right)\cdot n$, then $m \leq \dfrac{d}{d-\left(1-\frac{1}{q}\right)n}$.

EXAMPLE Let's compare what it says about $(\underset{n}{10}, m, \underset{d}{7})$ binary codes to our previous $(q=2)$

$m \leq 5$ from Hamming's bound
($m \leq 16$ from Singleton's bound.)

Check Plotkin applies, since the hypothesis is satisfied:

$$7 = d \overset{\checkmark}{>} \left(1-\tfrac{1}{2}\right)n = \left(1-\tfrac{1}{2}\right)10 = 5$$

Plotkin says $m \leq \dfrac{d}{d-\left(1-\frac{1}{q}\right)n} = \dfrac{7}{7-\left(1-\frac{1}{2}\right)10} = \dfrac{7}{7-5} = \dfrac{7}{2}$

so $m \leq 3$, much better than Hamming!

(skipped in lecture)

proof of Plotkin's bound: Let's compare some lower and upper bounds on this sum:

$$S := \sum_{v \in \mathcal{C}} \sum_{\substack{v' \in \mathcal{C}: \\ v' \neq v}} \underbrace{d(v,v')}_{\geq d}$$

$\geq d$ by definition of $d = d(\mathcal{C})$

so $$S \geq \sum_{v \in \mathcal{C}} \sum_{\substack{v' \in \mathcal{C}: \\ v' \neq v}} d = d \, \# \{ (v,v') \in \mathcal{C} : v' \neq v \}$$

$$= d \cdot m(m-1)$$

choices for v | choices for v'

On the other hand,

$$S = \sum_{v \in \mathcal{C}} \sum_{\substack{v' \in \mathcal{C}: \\ v' \neq v}} \sum_{i=1}^{n} \begin{cases} 1 & \text{if } v_i' \neq v_i \\ 0 & \text{if } v_i' = v_i \end{cases}$$

interchange order of sums

$$= \sum_{i=1}^{n} \sum_{v \in \mathcal{C}} \sum_{\substack{v' \in \mathcal{C}: \\ v' \neq v}} \begin{cases} 1 & \text{if } v_i' \neq v_i \\ 0 & \text{if } v_i' = v_i \end{cases}$$

$$= \sum_{i=1}^{n} \sum_{v \in \mathcal{C}} \# \{ v' \in \mathcal{C} : v_i' \neq v_i \}$$

classify v according to $v_i = j$

$$S = \sum_{i=1}^{n} \sum_{j=0}^{q-1} \sum_{\substack{v \in \mathcal{C}: \\ v_i = j}} \# \{ v' \in \mathcal{C} : v_i' \neq j \}$$

If we let $k_{ij} := \#\{v \in \mathcal{C} : v_i = j\}$ for all positions $i = 1, 2, \dots, n$ and letters $j = 0, 1, \dots, q-1$

then we can rewrite the innermost sum:

$$S = \sum_{i=1}^{n} \sum_{j=0}^{q-1} \underbrace{k_{ij}}_{\substack{\text{choices}\\ \text{for } v \in \mathcal{C}\\ \text{with } v_i = j}} \, (\underbrace{m - k_{ij}}_{\substack{\text{choices for } v' \in \mathcal{C}\\ \text{with } v'_i \neq j}})$$

$$= \sum_{i=1}^{n} \left[m \sum_{j=0}^{q-1} k_{ij} - \sum_{j=0}^{q-1} k_{ij}^2 \right]$$

since $x_0 = k_{i,0}$, $x_1 = k_{i,1}$, $\vdots$, $x_{q-1} = k_{i,q-1}$ satisfy $x_0 + x_1 + \dots + x_{q-1} = m$

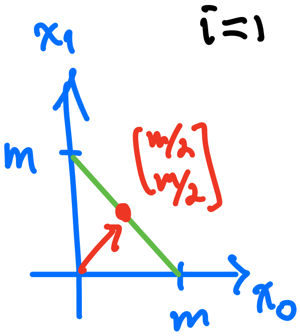
$$= \sum_{i=1}^{n} \left[m \cdot m - \sum_{j=0}^{q-1} k_{ij}^2 \right]$$

since the minimum of $\|x\|^2 = \sum_{j=0}^{q-1} x_j^2$ on the set $x_0 + x_1 + \dots + x_{q-1} = m$ occurs when

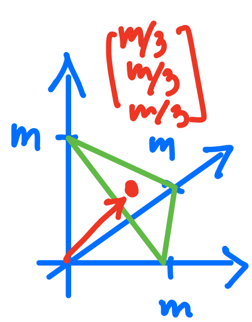
$$x_0 = x_1 = \dots = x_{q-1} = \frac{m}{q}$$

(e.g. via calculus)

$$\leq \sum_{i=1}^{n} \left[m^2 - \sum_{j=0}^{q-1} \left(\frac{m}{q}\right)^2 \right]$$



$q=2$



$q=3$

Thus $S \leq n\left(m^2 - \dfrac{m^2}{q}\right)$

Comparing the two bounds on S,

$$dm(m-1) \leq S \leq n\left(m^2 - \frac{m^2}{q}\right)$$

so
$$d(m-1) \leq nm\left(1-\frac{1}{q}\right)$$
$$dm - d \leq nm\left(1-\frac{1}{q}\right)$$
$$dm - nm\left(1-\frac{1}{q}\right) \leq d$$
$$m\big(\underbrace{d-\left(1-\tfrac{1}{q}\right)n}_{>0 \text{ by hypothesis}}\big) \leq d$$

$$\Longrightarrow \quad m \leq \frac{d}{d-\left(1-\frac{1}{q}\right)n} \qquad \blacksquare$$

Gilbert-Varshamov Bound (§13.2)

This only works for linear codes, but it's a lower bound on k in $[n,k,d]$ (or $m=q^k$), so it works in the opposite direction to the other bounds, providing existence of codes.

THEOREM: There exists an $[n,k,d]$ $\mathbb{F}_q$-linear code $\mathcal{C}$ whenever

$$q^{n-k} > 1 + (q-1)\binom{n-1}{1} + (q-1)^2\binom{n-1}{2} + \dots + (q-1)^{d-2}\binom{n-1}{d-2},$$

or equivalently by taking $\log_q(-)$, whenever

$$k < n - \log_q\left(1 + (q-1)\binom{n-1}{1} + (q-1)^2\binom{n-1}{2} + \dots + (q-1)^{d-2}\binom{n-1}{d-2}\right).$$

---

proof: Let's try to build such a $\mathcal{C}$ by choosing n column vectors in $(\mathbb{F}_q)^{n-k}$ for the generator matrix H of its dual code $\mathcal{C}^\perp$, having no $d-1$ of its columns dependent ($\Rightarrow d(\mathcal{C}) \geq d$):

$$H = {\scriptstyle n-k}\left\{\begin{bmatrix} | & | & & | & | \\ u_1 & u_2 & \cdots & u_{n-1} & u_n \\ | & | & & | & | \end{bmatrix}\right.$$

imagine we have already chosen all of the first $n-1$ columns

Now we must chose this last column u_n in $(\mathbb{F}_q)^{n-k}$ avoiding all $\mathbb{F}_q$-linear combinations of $d-2$ or fewer previously chosen columns.

Thus u_n must avoid at most this many vectors in $(\mathbb{F}_q)^{n-k}$:

$$1 + \binom{n-1}{1}(q-1) + \binom{n-1}{2}(q-1)^2 + \dots + \binom{n-1}{d-2}(q-1)^{d-2}$$

... etc.

avoid $\underline{0}$

pick a column u_i $i=1,2,\dots,n-1$

pick a nonzero coefficient $c \in (\mathbb{F}_q)^\times$ to avoid cu_i

pick columns $\{u_i, u_j\}$

pick nonzero coefficients $c_i, c_j \in (\mathbb{F}_q)^\times$ to avoid $c_iu_i + c_ju_j$

As long as $|(\mathbb{F}_q)^{n-k}| = q^{n-k}$ is bigger than the above sum, we can pick u_n.

And at any of the earlier stages picking u_1, then u_2, etc, one needs similar inequalities, but they are all less stringent. $\blacksquare$

EXAMPLE: How small do we need to make k to build a $[10, k, 7]$ $\mathbb{F}_2$-linear code? Gilbert-Varshamov tells us how once we make sure

$$k < 10 - \log_2\left(1 + \binom{9}{1}(2-1)^1 + \binom{9}{2}(2-1)^2 + \dots + \binom{9}{5}(2-1)^5\right) \approx 1.42$$

$5 = 7-2$
$= d-2$

So it only works to build $\mathcal{C}$ if $k \leq 1$,

e.g. the $[10, 1, 10]$ $\mathbb{F}_2$-repetition code

$$\mathcal{C} = \{\underline{0}, \underline{1}\} \subset (\mathbb{F}_2)^{10}$$

This may seem a bit disappointing, but we shouldn't have been surprised:

Plotkin told us $m \leq 3$ for any $(10, m, 7)$ 2-ary code,

$\Rightarrow 2^k < 3$ for any $[10, k, 7]$ $\mathbb{F}_2$-linear code

$\Rightarrow k < \log_2(3) \approx 1.58$

i.e. $k \leq 1$