Math 846 Presentation
Parameters of a code, Hamming code
Instructor: Pro. Paul Terwilliger

Ruocheng Yang

May 2023

Introduction.

Math Model: Sender $\xrightarrow{x}$ code (error correction) $\xrightarrow{C}$ channel $\xrightarrow{v=c+\varepsilon}$ decode $\xrightarrow{C}$ Receiver $\xrightarrow{x}$

$x \in \mathbb{F}_q^k$ information; $x \to C \subseteq$ codeword with error correction capability

ε: error vector

Definitions: def 1: $\mathbb{F}_q^n$, n-dim v.s. over $\mathbb{F}_q$, nonempty subset C in $\mathbb{F}_q^n$ called a q-element code, n: length of code, vectors in C called code words

- $K = |C|$, $1 \le K \le q^n$, number of code words
- $k = \log_q K$, information bits ($k \in \mathbb{R}$, $0 \le k \le n$)
- $\frac{k}{n}$: efficiency or information rate

We need a def. to compare the capability of error correction

def 2. $\vec{a} = (a_1, \cdots a_n)$ $\vec{b} = (b_1 \cdots b_n) \in \mathbb{F}_q^n$

- Hamming weight of $\vec{a}$ $w_H(a) = \#\{i \mid 1 \le i \le n, a_i \neq 0\}$
- Hamming distance $d_H(a,b) = \#\{i \mid 1 \le i \le n, a_i \neq b_i\} = w_H(a-b)$

Easy to check this is a distance. (omit H)

def 3. Assume C is code with length n and q-element $C \subseteq \mathbb{F}_q^n$ nonempty $K = |C| \ge 2$ minimal Hamming distance = minimal distance of C

$$d \triangleq d(C) = \min\{d(c,c') \mid c, c' \in C, c \neq c'\}$$

Easy but fundamental:

Thm. If d is the minimal distance of C, then C can examine $\le d-1$ elements errors, also can do error correction $\le \left[\frac{d-1}{2}\right]$ elements.

Proof. triangle inequality.

- Assume the sending code $c \in C$, errors $\le d-1$ i.e. $1 \le w(\varepsilon) \le d-1$, so accept $v = c + \varepsilon \neq C$

$\Rightarrow d(c,v) = w(v-c) = w(\varepsilon) \le d-1$. Also for $c' \neq C$, $d(c,c') \ge d$, so $v \neq c'$, v is not a code ✓

- Assume $1 \le w(\varepsilon) \le \left[\frac{d-1}{2}\right]$, so $d(c,v) = w(\varepsilon) \le \left[\frac{d-1}{2}\right]$, and for $c' \neq C$,

$$d(c',v) \geq d(c,c') - d(c,v)$$
$$\geq d - \left[\frac{d-1}{2}\right] > \left[\frac{d-1}{2}\right]$$

so c is a unique closest code for v, $v \to c$ ✓ correct.

#

Parameters. For fixed $\mathbb{F}_q$, $C \subseteq \mathbb{F}_q^n$ has three parameters.

- Length n
- Number of codes $K = |C|$ (or use information bits $k = \log_q K$), $0 \leq k \leq n$
- Minimal distance $d = d(C)$, $1 \leq d \leq n$

We represent the error code as $(n, K, d)_q$ or $[n, k, d]_q$ or q-ary....

Topics: • Good codes i.e. $\frac{k}{n}$ and d big enough
• Good decoding

For ①, n, k, d are restricting each other.

$\frac{k}{n} = \max = 1$, $k = n$, $K = q^n$, $C = \mathbb{F}_q^n$ $d = 1$

$d = \max = n$, $\max |C| = q$, $K \leq q$, $k \in 1$, $\frac{k}{n} \leq \frac{1}{n}$

So a good way to ask this is fixing two of them.

eg. get the Hamming bound. Hard to create good codes.

For ②, it is from application save time to code and decode eg. Thm above

✓ ✗

So we need Combinatorics, Algebra even Geometry

Classification. For $\mathbb{F}_q^n$, classify q-ary codes i.e. same n, k, d.

def⁴ (equivalence)

- Permutation. $\sigma \in S_n$ $\sigma(c) = (c_{\sigma(1)}, c_{\sigma(2)} \cdots c_{\sigma(n)}) \in \mathbb{F}_q^n$ $\sigma(C) = \{\sigma(c) | c \in C\}$ ✓
  (component)
- Element Permutation. $f: \mathbb{F}_q \to \mathbb{F}_q$ bijection, $f(0) = 0$

  $f(c) = (f(c_1) \cdots f(c_n))$ $f(C) = \{f(c), c \in C\}$ ✓
- Parallel transport $C \subseteq \mathbb{F}_q^n$, $v \in \mathbb{F}_q^n$, $C' = C + v = \{c + v | c \in C\}$ ✓

Some bounds of error-correcting codes

Thm. (Hamming bound) For $(n, K, d)_q$ we have

$$q^n \geq K \sum_{i=0}^{[\frac{d-1}{2}]} (q-1)^i \binom{n}{i}$$

Proof. Counting vectors in the "balls".

For any $r \in \mathbb{N}$, $v = (v_1, v_2, \cdots v_n) \in \mathbb{F}_q^n$, define $S_q(v, r) = \{u \in \mathbb{F}_q^n \mid d(u, v) \leq r\}$

- Numer of vectors in this balls.

For $i \geq 0$, if $d(u,v) = i$, then u and v have i distinct components, fix v. $\binom{n}{i}$ to choose i components.
Since on these i components, $u_j \neq v_j$, so every component has $q-1$ choices, other components are same.

So there are $(q-1)^i \cdot \binom{n}{i} - u$ satisfying $d(u,v) = i$.

$$\text{So } |S_q(v, r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Now we assume $\exists$ (n, K, d) q-ary C, name $\ell = [\frac{d-1}{2}]$, focus on $S_q(c, \ell)$, there are K balls.
For distinct balls $S_q(c_1, \ell)$ & $S_q(c_2, \ell)$, these not interect each other since if $u \in S_q(c_1, \ell) \cap S_q(c_2, \ell)$, then $d(u, c_1) \leq \ell$, $d(u, c_2) \leq \ell$

$$\Rightarrow d(c_1, c_2) \leq d(c_1, u) + d(c_2, u) \leq 2\ell = 2\left[\frac{d-1}{2}\right] \leq d-1$$

But $d(c_1, c_2) \geq d$.

So all the sum of elements $= K \cdot \sum_{i=0}^{r} \binom{n}{i} (q-1)^i \leq \#(\mathbb{F}_q^n) = q^n$.

#

def 5. perfect code (equality) i.e. q-ary C $(n, K, 2\ell+1) \Rightarrow q^n = K \cdot \sum_{i=0}^{\ell} (q-1)^i \binom{n}{i}$

Good: K balls $S_q(c, \ell)$ fill the entire space.

1973. Van Lint & Tietäväinen decide all of the perfect codes. (there is a survey)

Remark. Another bounds: • Singleton bound : $K \leq q^{n-d+1}$ $(n \geq k+d-1)$

$\Downarrow$

Good ✓ MDS (Maximal Distance Separable) code

For binary codes, Plotkin bound : $K \leq \begin{cases} 2[\frac{d}{2d-n}] & K \text{ even} \\ 2[\frac{d}{2d-n}] - 1 & K \text{ odd} \end{cases}$

Indeed, finding good codes is a combinatorial problem, since C is just a subset of $\mathbb{F}_q^n$.
So consider C to be a linear subspace of $\mathbb{F}_q^n$.

Remark: For Singleton bound, we can create the set $C_a = \{(c_1, c_2, \cdots c_{n-1}) \mid (c_1, c_2, \cdots c_{n-1}, a) \in C\}$, $d(C_a) \geq d(C) = d$.

For q codes C_a ($a \in \mathbb{F}_q$), all numbers $\Rightarrow |C| = K = \sum_{a \in \mathbb{F}_q} |C_a|$. $\exists\, a \in \mathbb{F}_q$ s.t. $|C_a| \geq K/q$, so $\exists$ ($n-1, \geq K/q, \geq d$) q-ary code. Keep doing this, we know $\exists$ q-ary code C' with parameters $(d, \geq K/q^{n-d}, d)$.

$\Rightarrow q \geq |C'| \geq K/q^{n-d}$, so $K \leq q^{n-d+1}$

MDS code is related to polynomial code. See references for details.

Linear codes

Parity Check matrix & Generator matrix

def 6. (linear codes) Linear subspace of $\mathbb{F}_p^n$ over $\mathbb{F}_p$ i.e. $\forall\, c, c' \in C \Rightarrow a, a' \in \mathbb{F}_p$, $ac + a'c' \in C$

$k = \dim_{\mathbb{F}_q} C$, $K = |C| = q^k$, $d(C) = \min d(c, c')$

Lemma. $d(C) = \min\{w(c) \mid 0 \neq c \in C\}$

Proof. $0 \in C$.

Tools in LA. $\mathbb{F}_q$-basis of C $\{v_1, v_2, \cdots v_k\}$, $v_i = (a_{i1}, \cdots a_{in})$ $(\forall\, 1 \leq i \leq k$ $a_{ij} \in \mathbb{F}_q$ $\forall\, 1 \leq j \leq n$

Each code can be uniquely written by $C = b_1 v_1 + \cdots + b_k v_k$ $(b_i \in \mathbb{F}_q)$

$= (b_1, b_2, \cdots, b_k)\, G$

$\operatorname{rank}(G) = k$, $G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} a_1 \cdots a_m \\ \vdots \\ a_{k1} \cdots a_{kn} \end{pmatrix}$

↓ generator matrix, not unique, depends on basis.

error-coding: $\varphi: \mathbb{F}_q^k \longrightarrow C \subseteq \mathbb{F}_q^n$

$(b_1, \cdots b_k) \longmapsto (b_1, \cdots b_k)\, G$

q^k messages

On the other hand, k-dim sub v.s. must be all solutions of homogeneous linear equations

e.g. $\begin{cases} b_{11}x_1 + b_{12}x_2 + \cdots + b_{1n}x_n = 0 \\ \vdots \\ b_{n-k,1}x_1 + b_{n-k,2}x_2 + \cdots + b_{n-k,n}x_n = 0 \end{cases}$

$H = (b_{ij})_{1 \leq i \leq n-k,\ 1 \leq j \leq n}$ $\operatorname{rank}(H) = n-k$

↓ parity check matrix

From def, $\forall\, v \in \mathbb{F}_q^n$, $v \in C \Leftrightarrow vH^T = 0$, so we can use H to check $v \in C$ or not.

H can also determine the minimal distance of the linear code.

$H=(u_1,u_2,\cdots u_n)$ $\quad u_i=\begin{pmatrix} b_{1i} \\ b_{2i} \\ \vdots \\ b_{n-k,i} \end{pmatrix}$ $\quad (1\le i\le n)$

Lem. q-ary $[n,k]$ code C, if $d-1$ vectors in u_i is $\mathbb{F}_q$ linear independent, and $\exists$ d vectors $\mathbb{F}_q$ linear dependent, C has minimal distance d.

Proof. $c=(c_1,c_2,\cdots c_n)$ $\quad w_H(c)=l$

$$c=0 \Leftrightarrow 0=Hc^T=(u_1,u_2,\cdots u_n)\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}=c_{j_1}u_{j_1}+\cdots+c_{j_l}u_{j_l}$$

weight l codes in C give l $\mathbb{F}_q$-linear dependent vectors in H. So min distance $=\min_{v_j}\#(l.d.$

H can also be used to error-correcting.

Exercise. $\exists$ a linear code C' equivalent to code C, s.t. C' has the generator matrix in form $G'=[I_k \mid P]$, $P\in\mathbb{F}_{q\ k\times(n-k)}$ and C' has parity check matrix $[-P^T \mid I_{n-k}]$.

Useful.

Error Correction Decoding Algorithm for Linear Codes.

Assume C is a q-ary $[n,k,d]$ code, $l=[\frac{d-1}{2}]$, and C has $H=(u_1,u_2\cdots u_n)$ u_i has length $n-k$ on $\mathbb{F}_q$. If some errors happen, i.e. receive a vector $y=c+\varepsilon$ and $w(\varepsilon)\le l$ (error positions $\le l$).

- Compute $v=Hy^T$.
  This is a length $n-k$ vector on $\mathbb{F}_q$, called the parity checking vector.
- If $v=0$, then $\varepsilon=0$, $y=c$ ✓
- If $v\neq 0$, then v can be represented by $\le l$ vectors via linear combinations using $u_1,\cdots u_n$
  i.e. $v=a_{i_1}u_{i_1}+\cdots+a_{i_t}u_{i_t}$ $\quad (1\le i_1<i_2<\cdots<i_t\le n)$,
  and $1\le t\le l$, $a_{i_1},a_{i_2}\cdots a_{i_t}\in\mathbb{F}_q\setminus\{0\}$, and
  $\varepsilon=(\varepsilon_1,\varepsilon_2,\cdots\varepsilon_n)$
  $\varepsilon_{i_1}=a_{i_1}$, $\varepsilon_{i_2}=a_{i_2}\cdots\varepsilon_{i_t}=a_{i_t}$, and when $i\neq i_1,i_2,\cdots i_t$, $\varepsilon_i=0$. So $c=y-\varepsilon$
  i.e. There are t errors, and errors are $i_1,i_2,\cdots i_t$, values are $a_{i_1},a_{i_2},\cdots a_{i_t}$.

Extended code.

Exercise. Assume C is a $[n,k,d]$-binary code, $d\in\{1,3,5,7,\cdots\}$, then the extended code

$$C'=\{(c_1,c_2,\cdots c_n,c_{n+1})\in\mathbb{F}_2^{n+1} \mid (c_1,c_2,\cdots c_n)\in C,\ c_1+c_2+\cdots+c_n+c_{n+1}=0\}$$

is a $[n+1,k,d+1]$-binary code.

Hamming Code (perfect linear code, also Golay code)

Assume $m \geq 2$, $\mathbb{F}_q^m$ has $q^m - 1$ nonzero vectors, and $v_1, v_2 \in \mathbb{F}_q^m$ are linear dependent $\Leftrightarrow$ $\exists\, a \in \mathbb{F}_q^n$ s.t. $a v_2 = v_1$. Projective equivalence each class has $q-1$ vectors $\Rightarrow$ $\frac{q^m-1}{q-1}$ classes.

Choose a representitive vector from each class $u_1, u_2, \cdots u_n$, $n = \frac{q^m-1}{q-1}$, length of u_i is m.

linear

$$H_m = (u_1, u_2, \cdots u_n)$$

def.7 (Hamming code) q-any code with parity check matrix H_m.

Thm. Parameters of $[n,k,d]$ Hamming code is $\left[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3\right]$, and perfect.

Proof. $(1,0,\cdots 0), (0,1,\cdots 0) \cdots (0,0,\cdots 1) \in$ different equivalent classes, two of them are linear independent so $\operatorname{rank}(H) = m$. So $n = \frac{q^m-1}{q-1}$; #{equivalent class}, $k = n - m = \frac{q^m-1}{q-1} - m$

So each column in H belongs to different equivalent classes, any two columns are linear independent

$\Rightarrow$ Sum of two columns nonzero, so must be equivalent to one column vector in H, so these three l.d.

$\Rightarrow d = 3$, $\sum_{i=0}^{q} (q-1)^i \binom{n}{i} = 1 + (q-1)n = 1 + q^m - 1 = q^m = q^{n-k}$ ✓

Ex. $[7,4,3]$-code binary Hamming code. When $q=2$, H_m is a matrix with $2^m - 1$ m-length nonzero vectors.

So $[n,k,3] = [2^m - 1, 2^m - 1 - m, 3]$ $(m \geq 2)$

For $m=3$,

$$H_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} = (I_3 \,|\, P)$$

So from this we get the generator matrix

$$G_3 = (P^T \,|\, I_4) = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

This is equivalent to example before.

Also, Golay code is a good perfect code. (Later)

1973, as before said, for every nontrivial q-ary perfect code, n, k, d must be same as Hamming code or Golay code.

But $[n,k,d]$ only invariant under equivalent classes, not "perfect invariants". Generally we have codes with same parameters but not equivalent.

So we need something specific.

eg. MacWilliams identity & weight polynomial

[References].

[1] Algebraic Combinatorics. Eiichi Bannai, Etsuko Bannai
Tatsuro Ito, Rie Tanaka

[2] Introduction to Coding Theory. Van Lint

[3] Coding Theory. Van Lint