Linear Block Codes as Vector Spaces:

Defn: A (linear) block code C over a field F_q of q symbols of length n and q^k codewords is a q-ary linear (n,k) code iff its q^k codewords form a k-dimensional vector subspace of the vector space of all the n-tuples F_q^n.

The number n is said to be the length of the code and the number k is the dimension of the code. The rate of the code is $R = k/n$.

In short: n-dimensional vector space

k-dimensional vector-subspace

A code is a k-dimensional vector subspace of an n-dimensional vector subspace over a field F_q.

Ex: $q=2$ $\quad n=6$ $\quad k=3$

$F_2 = \{0,1\}$ $\quad V = \{000000, 000001, \ldots\ldots 111111\}$

V: all 6-tuples, $2^6 = 64$ tuples; V: vector space.

dimension of V is $n=6$

Now consider a subspace of V with dimension 3 $\quad k=3$

(26)

The basis vectors of the subspace are chosen of

$B = \{100011, 010101, 001110\}$

then the span of B is our subspace

i.e, code

$C = span(B)$ $C = \{000000, 100011, 010101, 001110,$

$100011+010101, 100011+001110,$

$010101+001110\}$

The code C is shown of $C(6,3)$ $\Rightarrow n \Rightarrow k$

$C = \{000000, 100011, 010101, 001110$

$110110, 101101, 011011\}$

Generator Matrix:

Given a linear code C (subspace)

let B be the set of basis vectors of the subspace (= code)

The matrix whose rows are the basis vectors is called the generator matrix of the code

i.e,

$$B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix}_{k \times n}$$

Ex°: For the $C(6,3)$ code the generator matrix is given of

(n = 6, k = 3)

$$G = \begin{bmatrix} 100011 \\ 010101 \\ 001110 \end{bmatrix}$$

3×6 → number of basis vector in vector space

↓ number of basis vectors in subspace

Remark: Rows of a Generator matrix are linearly independent

Code: Row span of Generator matrix is a code.

Codebook is the same of the code.

Ex°: $G = \begin{bmatrix} 1000 \\ 0111 \end{bmatrix}_{2\times4}$ Find the code generated by G.

S/n°:

$$C = \{0000, 1000, 0111, 1111\}$$

$C(4,2)$ (n = 4, k = 2)

$C(n,k)$

Code rate is $R = \frac{k}{n} = \frac{2}{4} = 0.5$

Codeword: Each vector (tuple) of the codebook is referred to of the codeword.

- For a linear code, the sum of any two codewords is also a codeword. More generally, any linear combination of codewords is a codeword.

Encoding:

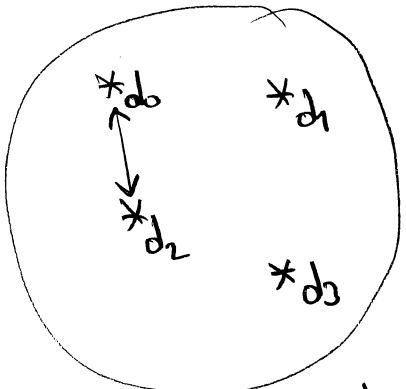
n-dimensional vector space has 2^n tuples

k-dimensional subspace has 2^k tuples

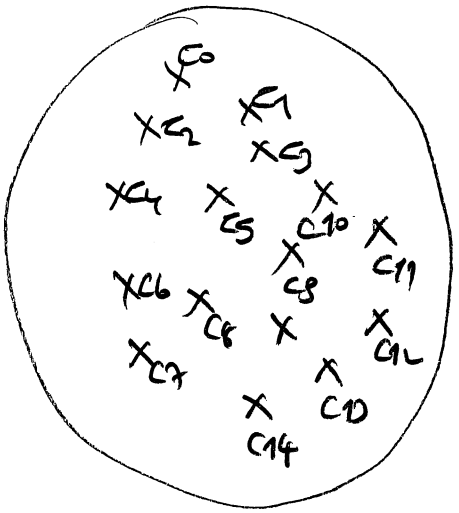
$C(n,k)$ $\quad k<n$

Ex: $n=4 \quad k=2$

$2^k = 2^2 = 4$



Assume we want to transmit 4 data words (each has 2 bits)



n=4 dimensional vector space.

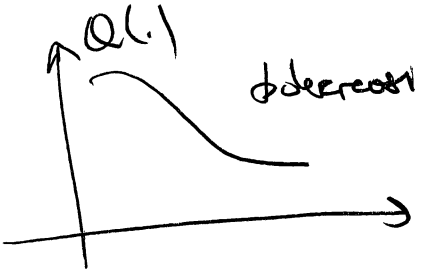
Assume that we wanna transmit information words

$d_0, \ldots d_3$

(25)

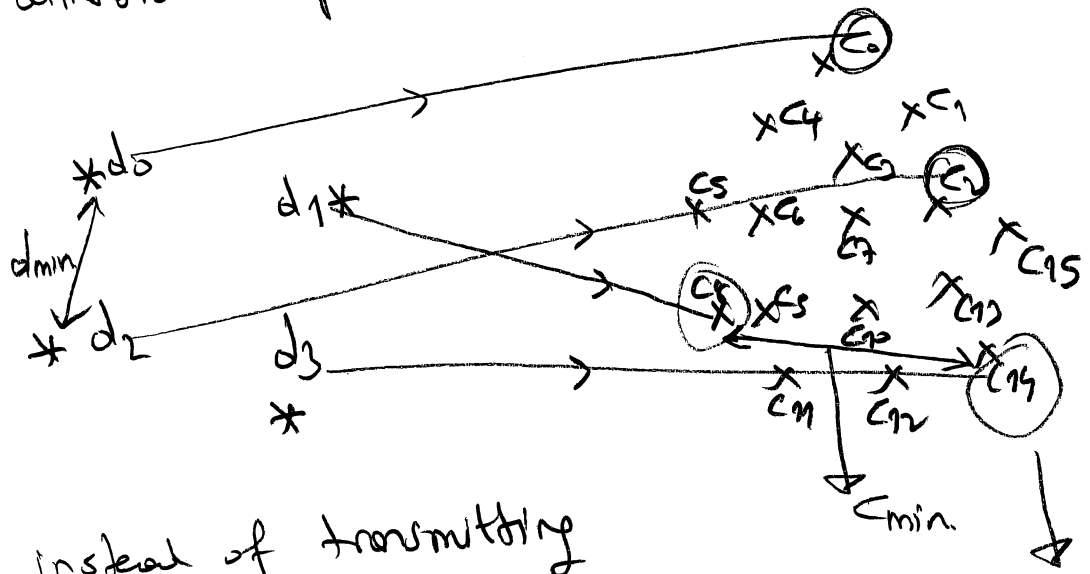
At the receiver the prob of error is related to d_{min} among codewords.

i.e, $P_e = Q\left(\sqrt{\frac{d_{min}^2}{2N_0}}\right)$



To reduce P_e
we should increase d_{min}.

to achieve this, lets make a mapping from k-dimensional space to n-dimensional space, but use a subspace of n-dimensional space. We only 4 vectors from n-dimensional space



instead of transmitting $d_0, \ldots d_3$, transmit c_0, c_2, c_8, c_{14}

since $c_{min} > d_{min}$

we have a less prob. of transmission error

since $P_e' = Q\left(\sqrt{\frac{c_{min}^2}{2N_0}}\right) < P_e = \left(\sqrt{\frac{d_{min}^2}{2N_0}}\right)$

This is the principle of coding.

(30)

Encoding Operations

Assume that we have $C(n,k)$

for example $k=2$ $n=4$

$k=2$ means we encode datawords of length 2

$n=4$ " the codewords are of length 4

let $G=\begin{bmatrix}1000\\0001\end{bmatrix}_{2\times4}$ $k=2, n=4$ $G=[\cdot]_{k\times4}$

let the information words (data words)

to be encodes of

$d_0=[00]$

$d_1=(11)$

Code is found of

$C=\{\underbrace{0000}_{c_0}, \underbrace{1000}_{c_1}, \underbrace{0001}_{c_2}, \underbrace{1001}_{c_3}\}$

$d_0 * \rightarrow$ $*c_0$ $*c_1$

$d_1 * \rightarrow$ $*c_2$ $*c_3$

how to make the mapping?

The mapping is done using

$c = d\,G$ → generator matrix

c ↓ codeword mapped to d

d ↓ dataword

For our example

$$c_0 = d_0 G \longrightarrow c_0 = [0\ 0]\begin{bmatrix}1000\\0001\end{bmatrix} = 0\times1000 + 0\times0001$$

$$\Rightarrow c_0 = [0000]$$

$$c_1 = d_1 G \longrightarrow c_1 = [1\ 1]\begin{bmatrix}1000\\0001\end{bmatrix}$$

$$= [1\times1000 + 1\times0001]$$

$$= [1001]$$

$\overline{d}_0\ (00) \rightarrow$ *c_0 (0000)

$\overline{d}_1\ (11) \rightarrow$ *c_1 (1001), *c_2 (0001), *c_3 (1000)

In general:

Let $\overline{d}_{1\times k} = [d_0\ d_1 \cdots d_{k-1}]_{1\times k}$ → dataword

$\overline{c}_{1\times n} = \overline{d}_{1\times k}\ G_{k\times n}$ → encoding operation.

$G = \begin{bmatrix}\overline{g}_0\\\overline{g}_1\\\vdots\\\overline{g}_{k-1}\end{bmatrix}$ → rows are basis vectors

(32)

$$\bar{c} = \bar{d} \times G$$

$$= \underbrace{[d_0\ d_1 \cdots d_{k-1}]}_{1\times k} \times \underbrace{\begin{bmatrix} \bar{g}_0 \\ \bar{g}_1 \\ \vdots \\ \bar{g}_{k-1} \end{bmatrix}}_{k\times n}$$

$$\bar{c} = d_0 \bar{g}_0 + d_1 \bar{g}_1 + \cdots d_{k-1} \bar{g}_{k-1}$$

Linear combination of $\bar{g}_0, \bar{g}_1, \cdots \bar{g}_{k-1}$ according to ~~dataword~~ bits (symbols)

$$\bar{c} = (c_0\ c_1 \cdots c_{n-1})_{1\times n}$$

$$(c_0\ c_1 \cdots c_{n-1})_{1\times n} = d_0 \bar{g}_0 + d_1 \bar{g}_1 + \cdots + d_{k-1} \bar{g}_{k-1}$$

each $\bar{g}_i$ has dimension $1\times n$.

Ex^e Generator matrix of a linear code is given of

$$G = \begin{bmatrix} 100011 \\ 010101 \\ 001110 \end{bmatrix} \Rightarrow G = \begin{bmatrix} \bar{g}_0 \\ \bar{g}_1 \\ \bar{g}_2 \end{bmatrix}$$

encode a) $\bar{d}_1 = (101)$ b) $d_2 = (111)$

Sln: $\bar{c}_1 = \bar{d}_1 G \rightarrow c_1 = (101)\begin{pmatrix} \bar{g}_0 \\ \bar{g}_1 \\ \bar{g}_2 \end{pmatrix}$

$$= \bar{g}_0 + \bar{g}_2$$

$$= (100011) + (001110) \rightarrow c_1 = (101101)$$

(30)

$$\overline{C_2} = \overline{d_2} \times G \rightarrow \overline{C_2} = (111)\begin{pmatrix} \overline{P_3} \\ \overline{P_1} \\ \overline{P_2} \end{pmatrix}$$

$$= \overline{P_3} + \overline{P_1} + \overline{P_2}$$

$$= (100011 + 010101 + 001110)$$

$$= (111000)$$

Dual Code's

A code is nothing but a subspace of a vector space. Then a dual-space also exists.

If $\dim(V)=n$ & $\dim(C)=k$

V ↓ vector space

C ↓ subspace (code)

the $\dim(C^{\perp})=n-k$.

$C^{\perp}$ ↓ dual space

- Let C be a code and G be the generator matrix of this code, c_i is a codeword of C, c_d is the dual code of C if $c.c_d=0$ $\forall c, c_d$.

The generator matrix of the dual code is denoted by H. H is called parity-check matrix of C.

Theorem: Let C be an (n,k) linear code over F_p and let H be a parity check matrix of C.

A vector $\bar{v}$ is a codeword iff

$$\bar{v}H^T=0$$

That is, the codewords in C are in the (left) nullspace of H.

(35)

Proof:

$$H=\begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_{n-k} \end{bmatrix}_{(n-k)\times n} \longrightarrow \text{each row is a basis vector in dual subspace}$$

let $\bar{v}$ be a code word. $\bar{v}=[v_1\ v_2 \dots v_n]$

$$\bar{v}H^T = [\bar{v}] \begin{bmatrix} h_1^T & h_2^T & \dots & h_{n-k}^T \end{bmatrix}_{n\times(n-k)}$$

$$= \underbrace{\bar{v}.h_1^T}_{=0} + \underbrace{\bar{v}.h_2}_{=0} + \dots \underbrace{\bar{v}h_{n-k}^T}_{=0}$$

since $\bar{v}\in C$ & $h_i \in C_d$ $\quad \bar{v}h_i^T=0$ ——

Let G be the generator matrix of C & H be the generator matrix of the dual code C_d i.e, parity check matrix of C

then $GH^T=0$

Proof:

$$G=\begin{bmatrix} \bar{g}_1 \\ \vdots \\ \bar{g}_k \end{bmatrix}_{k\times n} \qquad H=\begin{bmatrix} \bar{h}_1 \\ \vdots \\ \bar{h}_{n-k} \end{bmatrix}_{n-k\times n}$$

↓ dimension of the code is k

↓ dimension of the dual code is $n-k$

$$GH^T=\begin{bmatrix} \bar{g}_1 \\ \bar{g}_k \end{bmatrix}\underbrace{\begin{bmatrix} \bar{h}_1^T & \dots & \bar{h}_{n-k}^T \end{bmatrix}}_{H^T}_{k\times(n-k)} = \underbrace{\bar{g}_1H^T}_{=0} + \underbrace{g_2H^T}_{=0} + \dots \underbrace{\bar{g}_kH^T}_{=0}$$

(36)

Ex°

$G = \begin{bmatrix} 1101 \\ 0110 \end{bmatrix}$ → Generator matrix of a code is given

$k=?,\ n=?$ Find Code generated by G

Find dual Code

Find generator matrix of the dual code.

S/n°

$G = [\ ]_{k \times n}$ $k=2$ $n=4$

$G = \begin{bmatrix} 1101 \\ 0110 \end{bmatrix} \rightarrow C = \{0000, 1101, 0110, 1011\}$

↓ Code generated by G

To find dual code, let $\bar{c}_d \in C_d$

$\bar{c}_d = (a\ b\ c\ d)$

Then for each $\bar{c} \in C$ $\quad \bar{c} \cdot \bar{c}_d = 0$

$(0\ b\ c\ d)(0000) = 0$

$(a\ b\ c\ d)(1101) = 0 \rightarrow a+b+d=0$

$(a\ b\ c\ d)(0110) = 0 \rightarrow b+c=0 \longrightarrow$ $b=0\ c=0$ or $b=1\ c=1$

$(a\ b\ c\ d)(1011) = 0 \rightarrow a+c+d=0$

let $b=0\ c=0$ then $a+d=0$

let $b=1\ c=1$ then $a+d+1=0$

$b=0\ c=0$ $\quad a+d=0$

↙ $a=d=0$ → $a=d=1$

$b=1\ c=1 \rightarrow a+d+1=0$

$a+d=1$

↙ $a=1\ d=0$ / $a=0\ d=1$

(37) Then the dual code is found as

a	b	c	d	
0	0	0	0	} → dual code
1	0	0	1	
1	1	1	0	
0	1	1	1	

$C_d = \{0000, 1001, 1110, 0111\}$

The generator matrix of C_d can be chosen as

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

it can be shown that $GH^T = 0$

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1+1+1+1 & 0+1+1 \end{bmatrix}$$

$$= [0 \quad 0]$$

$C(n,k)$ → contains 2^k codewords

$C_d(n, n-k)$ → contains 2^{n-k} codewords

Systematic form of Generator matrix.

For (n,k) code let G be the generator matrix

If G can be put into the form

$$G=[I_k \; P] \quad \text{or} \quad G=[P \; I_k]$$

then G is said to be systematic generator matrix.

To put any G into systematic form, elementary row operations are performed.

Note: Every generator matrix may not be put into systematic form using only elementary row-operations.

Ex: $G=\left[\begin{array}{ccc|cc} 1&0&1&0&0\\ 0&1&0&0&1\\ 0&1&1&1&0 \end{array}\right]$ put G into systematic form

Sln:

G $\xrightarrow{\text{row3}\leftarrow\text{row2}+\text{row3}}$ $\left[\begin{array}{ccc|cc} 1&0&1&0&0\\ 0&1&0&0&1\\ 0&0&1&1&1 \end{array}\right]$

$\left[\begin{array}{ccc|cc} 1&0&1&0&0\\ 0&1&0&0&1\\ 0&0&1&1&1 \end{array}\right]$ $\xrightarrow{\text{row1}\leftarrow\text{row1}+\text{row3}}$ $\left[\begin{array}{ccc|cc} 1&0&0&1&1\\ 0&1&0&0&1\\ 0&0&1&1&1 \end{array}\right]$

Hence, systematic form of G is

$$G=\underbrace{\left[\begin{array}{ccc|cc} 1&0&0&1&1\\ 0&1&0&0&1\\ 0&0&1&1&1 \end{array}\right]}_{I \quad P}$$

Ex³ $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$ put G into systematic form

Sln: G cannot be put into systematic form using only elementary row operations.

Definitions

Two linear codes which are the same except for a permutation of the components of the codewords are said to be equivalent codes.

Let G be the generator matrix of a linear code using elementary row operations and column permutations on G to obtain G'

Then G' is the generator matrix of the equivalent code.

Note: G can be put into systematic form using elementary row operations and column permutations. In this case the final matrix G' is the generator matrix of an equivalent code.

Error correction capability of a code and it's equivalent is the same.

Ex3 Let $G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

and column 2 $\longleftrightarrow$ column 4

gives $G' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

The code generated by G is

$C = \{0000, 1000, 0001, 1001\}$

The code generated by G' is

$C_{ep} = \{0000, 1000, 0100, 1100\}$

Ex2 $G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \rightarrow C = \{0000, 1001, 0101, 0011, 1101, 1010, 0110, 1111\}$

$G' = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \rightarrow C_{ep} = \{1100, 0101, 0110, 1001, 1010, 0011, 1111, 0000\}$

(40)

If Generator matrix is in systematic form

i.e, $G = [\underbrace{I}_{k\times k} \quad \underbrace{P}_{k\times(n-k)}]_{k\times n}$

Then the encoded word (codeword) becomes of

$$\bar{C} = \bar{d}G \rightarrow \bar{C} = \bar{d}[I \quad P]$$

$$\rightarrow \bar{c} = [\bar{d}I \quad \bar{d}P]$$

$$\rightarrow \bar{c} = [\bar{d} \quad \underbrace{\bar{d}P}_{=\bar{p}}]$$

↓ small $\bar{p}$

$$\bar{c} = [\bar{d} \quad \bar{p}]$$

↓ dataword → parity word

Definition: Hamming Distance

Let $\bar{c}_i$ & $\bar{c}_j$ be codewords

$$\bar{c}_i = (c_{i1} \; c_{i2} \cdots c_{in})$$
$$\bar{c}_j = (c_{j1} \; c_{j2} \cdots c_{jn})$$

Let $w(c_{ir}, c_{kr}) = \begin{cases} 1 & \text{if } c_{ir} \neq c_{kr} \quad r = 1, \ldots n \\ 0 & \text{otherwise} \end{cases}$

$$d_H(\bar{c}_i, \bar{c}_j) = \sum_{r=1}^{n} w(c_{ir}, c_{kr})$$

↓ Hamming distance between $\bar{c}_i$ & $\bar{c}_j$

i.e, Hamming distance is nothing but total number of different symbols between two codewords.

Minimum Distance of a Codes

The minimum Hamming distance between any pairs of codewords is called the minimum distance of the code.

i.e, $C \rightarrow$ code

$$d_{min}(C) = \min_{\bar{c}_i, \bar{c}_j \in C} d_H(\bar{c}_i, \bar{c}_j)$$

Hamming Weights

Hamming Weight of a codeword is

$$d_H(\bar{c}) = d_H(\bar{c}, \bar{0}) \quad \bar{0} \rightarrow \text{all zero codewords}$$

i.e, number of nonzero ~~terms~~

Remark: The minimum distance of a linear code is the minimum Hamming weight of all the codewords.

Remark: Equivalent codes have the same minimum distance

(42)

— A code with minimum distance d_{min} can detect all error patterns of weight less than or equal to $(d_{min}-1)$.

— A code with minimum distance d_{min} can correct all error patterns of weight less than or equal to $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$

Ex: Generator matrix of a linear code is given as $G=\begin{bmatrix} 1&0&1&0&0 \\ 0&1&0&0&1 \\ 0&1&1&1&0 \end{bmatrix}$

a) Find all the codewords b) Find $d_{min}(C)$?

c) Hamming weight of each codeword?

d) Error detection and correction capability?

Sln:

a) $G=\underbrace{\begin{bmatrix} 1&0&1&0&0 \\ 0&1&0&0&1 \\ 0&1&1&1&0 \end{bmatrix}}_{3\times 4} \rightarrow C=\{0000, 10100, 01001, 01110, 11101, 11010, 00111, 10011\}$

b) $d_{min}(C)=2$

c) $C=\{0000, 10100, 01001, 01110, 11101, 11010, 00111, 10011\}$
$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$
$0 \quad 2 \quad 2 \quad 3 \quad 4 \quad 3 \quad 3 \quad 3$

d) $d_{min}=2 \rightarrow 2-1=1$ error can be detected

$\left\lfloor \frac{2-1}{2} \right\rfloor = 0$ error can be corrected.

(43)

Exercise:

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]_{4\times 7}$$

a) Find $d_{min}(C)$

b) Assume that the following operations are performed on G

row 2 $\longleftrightarrow$ row 3

column 5 $\longleftrightarrow$ column 6

Let G_b be the resulting matrix of the equivalent code C_{ep}

fin $d_{min}(C_{ep})$

Property: $G \rightarrow$ generator matrix of a linear code

$H \rightarrow$ parity check matrix

The minimum distance is the smallest number of columns of H when summed give zero

Ex: $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$ Find H & find $d_{min}(C)$ using H

Sln: $G = [I \; P]$ $H = [-P^T \; I]$ $P = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$

3×5

(44)

$$G=\begin{bmatrix} 1&0&0&1&1 \\ 0&1&0&1&0 \\ 0&0&1&0&1 \end{bmatrix} \rightarrow H=\left[\begin{array}{ccc|cc} 1&1&0&1&0 \\ 1&0&1&0&1 \end{array}\right]$$

G: I | P (3×5; k, n)

H: P^T | I (2×5)

$$H=\begin{bmatrix} 1&1&0&1&0 \\ 1&0&1&0&1 \end{bmatrix}$$

↓ ↓ ↓

their sum gives zero

Hence $d_{min}(C)=3$

(45)

Properties of Linear Codes:

① If $\bar{c}_i$ & $\bar{c}_j \in C$ then $\bar{c}_i + \bar{c}_j \in C$

② If $k \in F_q$ → field $k\bar{c} \in C$ If $\bar{c} \in C$

③ The all zero codeword $\bar{0}$ i.e $(0 \cdots 0)$ is always a codeword.

Some simple Bounds on Block Codes:

Theorem: For $C(n,k)$ linear code, the minimum distance d_{min} is bounded by

$$d_{min} \leq n-k+1$$

which is called Singleton bound.

Proof: $H = [\quad]_{(n-k)\times n}$ → The rows are linearly independent

Row rank of $H = (n-k)$

Row Rank = Column Rank = Matrix Rank

$\text{rank}(H) = n-k$. Any collection of $(n-k+1)$ columns must therefore be linearly dependent.

Thus the minimum distance cannot be larger than $n-k+1$

A code for which $d_{min} = n - k + 1$ is called maximum distance separable (MDS) code.

Definition:

The vectors at Hamming distances $\leq t$ away from a word form a sphere called Hamming sphere of radius t.

The number of words in a Hamming sphere up to radius t for a code of length n over an alphabet of q symbols is denoted $V_q(n,t)$, where

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

For binary case

$$V_2(n,t) = \sum_{j=0}^{t} \binom{n}{j}$$

Theorem: The Hamming Bound:

A t-random error correcting code (q-ary) C must have redundancy r satisfying

$$r \geq \log_q V_q(n,t) \qquad r = n - k$$

$$C(n,k)$$

For binary code $r = n - k$.

$$r \geq \log_2 V_2(n,t) \rightarrow V_2(n,t) \leq 2^r$$

$$\sum_{j=0}^{t} \binom{n}{j} \leq 2^{n-k}$$

↓ Hamming bound for a t-error correcting linear code.

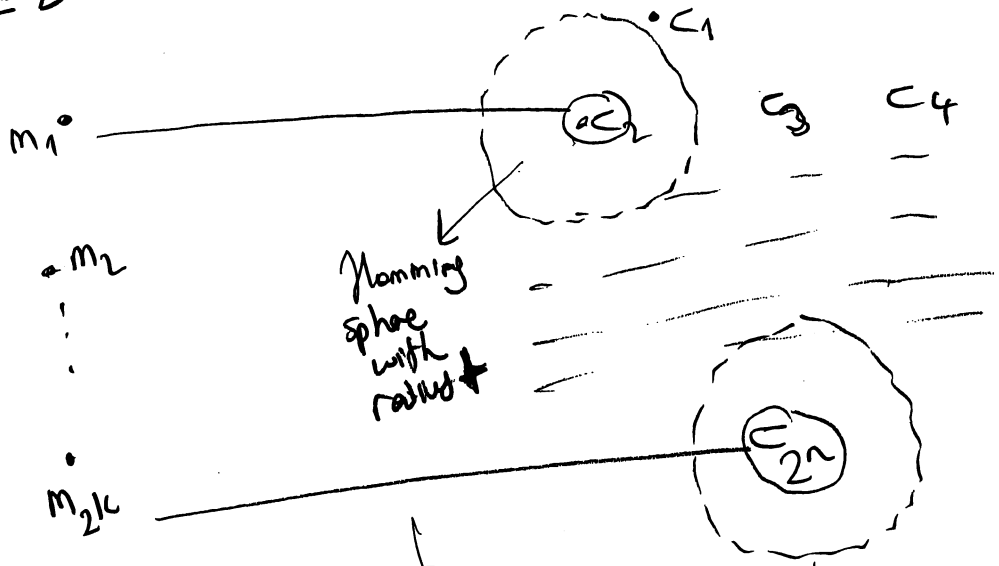
Proof: For (n,k) code

$k \rightarrow$ information word length (dataword)

$n \rightarrow$ codeword length

$2^n \rightarrow$ total number of codewords

$M = 2^k \rightarrow$ total number of dataword



↓ mapping

↓ Hamming sphere with radius t

Total number of Hamming spheres in subspace (code) equals to M

(48)

The total number of vectors (words) in M Hamming sphere is $M V_2(n,t)$ which is smaller or equal to the total number of vectors in vector space which is 2^n

$$M V_2(n,t) \leq 2^n \quad \rightarrow \text{binary code}$$

$$2^k \sum_{j=0}^{t} \binom{n}{j} \leq 2^n$$

$$\Rightarrow \sum_{j=0}^{t} \binom{n}{j} \leq 2^{n-k}$$

$$\Rightarrow \sum_{j=0}^{t} \binom{n}{j} \leq 2^r$$

Ex° $C(4,2) \rightarrow$ a linear code (binary code)

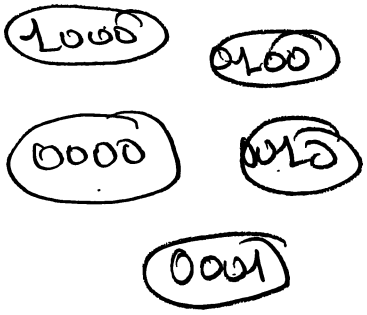
Find $V(4,1)$ $\quad V_2(n,t)$

$n = 4, \; t = 1$

i.e, number of vectors in a Hamming sphere.

S/n° Without using formula lets find the number of vectors by inspection

(4) Since all zero vector is also a word (vector) lets put it to the center of the sphere



The number of vectors is 5

Using formula

$$V_2(4,1) = \sum_{j=0}^{t=1} \binom{4}{j}$$

$$= \binom{4}{0} + \binom{4}{1}$$

$$= 1 + 4$$

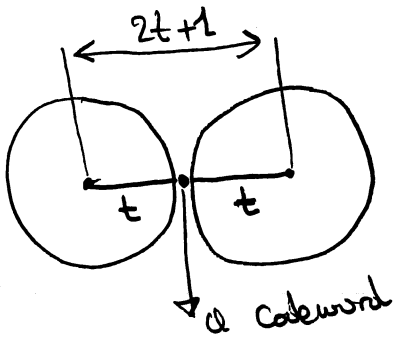
$$= 5$$

Ex3 For $c(4,2)$ find $V_2(4,2)$

Ex4 $d_{min} = 5$ error correcting capability

Sln: $t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$

$= 2$



(50) Ex°

$t = 3$ → error correcting capability

$d_{min} = ?$

Sln:

$d_{min} \geq 2t+1 \rightarrow d_{min} \geq 7$

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

d_{min} can be 7
8

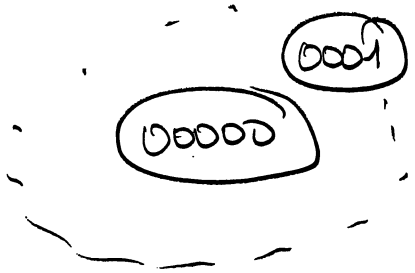
but d_{min} cannot be 9 or greater than 9.

Ex°

Find the number of words with Hamming weight less than or equal to $t=3$ for $C(5,3)$ code

Sln:

The first is 0 codeword



number of words with Hamming weight 1

total number of vectors is

$$\sum_{j=0}^{3} \binom{5}{j} = \binom{5}{0} + \binom{5}{1} + \cdots \binom{5}{3}$$

$\binom{5}{0} = 1$ indicates 0 word

$\binom{5}{3}$ number of words with Hamming weight 3

(51)

Ex°

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{2\times 4}$$

Show all Hamming spheres around codewords.

error correcting capability ?

How decoding is performed

Sln° Will be solved during class