LINEAR CODES

T. Important parameters (n, M, d) to calculate d you need to calculate Hamming humber of codewords distance of every pair of codewords $O(n^2)$

IT ENCODE:

TIP DF CODING

Upon recieving W. You need to find CEC with

minimum Hamming distance

win H(c,w)

DEFINITION:

A code C over alphabet q (qis a power of prime)
is linear if two conditions hold:

 $T. \forall x, y \in C \quad x+y \in C$

1. $t \times_{i} y \in X_{i-1} \times_{i-1} \times_{i-$

Ex2.1

(= {00000,00000, 10000, 10000, 10000, 10000, 10000} C-3dimensional

Decide whether C is linear.

T. J

 \int_{0}^{∞}

Code C is a subspace of [\{0,13\,\text{t},\)] | m-dimensional space What is the dimension of C? | vectors

How large is \{-dimensional subspace? 2\\\ (\frac{2}{9}\) for alphabet of \(\frac{1}{9}\) of size \(\frac{1}{9}\) |

for linear codes instead of \((n,M,d)\) we

for linear codes instead of (n, 17, d) we often write (n, 2, d)
& site of code subspace.

ADVANTAGE I. How to calculate minimum distance of?

$$\frac{1}{H(c_{n}, c_{n})} = H(c_{n} + \omega_{1} c_{n} + \omega)$$

$$H(c_{n} + c_{n}, c_{n} + c_{n})$$

FIND the codeword of the smallest weight (number of noursers)

ENCODING

Generating matrix G= 2 bo of code C. Since M=2 we can associate each message with m; { {0,13}} to encode message in calalate

$$m_5 = 101$$

$$C_1 = (001) \cdot 6 = (0.0 + 0.1 + 1.1 0, 00)$$

WE DO NOT NEED ENCODING TABLE! STORING G IS EMOUGH

Algorithm to find normal form of 6:

1) start with an arbitron G

- 1,) start with an arbitry G
- 2.) Do hollowing operations until normal form is found:
 - a.) permutation of vows
 - 6.) multiplication of a now by nonzero scalar | Change Co, addition of nows

 - d.) multiplication of columns by non-zero scalar of the ode for equivalent
 - $G = \begin{pmatrix} 10010 \\ 10010 \end{pmatrix} = \begin{pmatrix} 10010 \\ 10010 \\ 10010 \end{pmatrix} = \begin{pmatrix} 10010 \\ 10010 \\ 10010 \\ 10010 \end{pmatrix} = \begin{pmatrix} 100100 \\ 10010 \\ 1$
 - $= \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

Codes with G in normal form are called systemic

DECODING

Standard array de coding

(ose+
$$u = {u+c|c\in C}$$

fu, v ∈ {0,13 h coset a and coset v are either identical or orisjoint.

Coset leader is an element of a coset with the smallest weight. (= \ 000000, 1011 \ 0, 01011 \ 11101} C+ M / S () 00000 00000 11101 0/011. 11100 01010 (0111 00001 900 00010 000100 (0100. 01001 111 () 00100 10010 0111 11001 0 6 6 0 0 0000 11000 11110 101011 10000 10000 00110 11 011 01101 10001 000011 01000 11110 0001 · filio 1 00011 10101 01000 01000/4 01011010 11110 0001 10011 01110 00/01 11000 0 (100) 0 1 100 (| 0 | 0 (000) 00 (1)

Decoding Procedure:

2.) Find w in standard giveny
3.) Call coset leader of a coset w belongs to Iw.
4.) decode w as w+lw

Example

W= 11110 in avery lw= 01000

So I decode as 10110

SYNDROME DECODING

Dual CODE C - of C

Scalar product

 $\overrightarrow{X} \cdot \overrightarrow{D} = \left(X_0 \cdot D_0 + X_1 \cdot M_1 + \dots + X_{m_1} \cdot D_{m_1} \right)$

X and of ave perpendianlar

 $i \left\{ \vec{x} \cdot \vec{k} = 0 \right\}$

C = { W | W < {0,13° & W · C = 0, 4 C < C}}

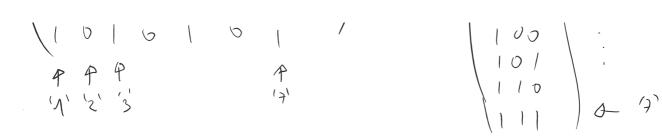
if dimension of C is & then dimension of C is N-E

 $G = (T_r A)$

evror in the channel is characterized by an evror vector (= 50,73

There is a one to one correspondence between

Cryptography 2019 Page 9



for every vector with '1' in E-th position
Soudhowe is 1/2';
Example: