4-9 Linear Code

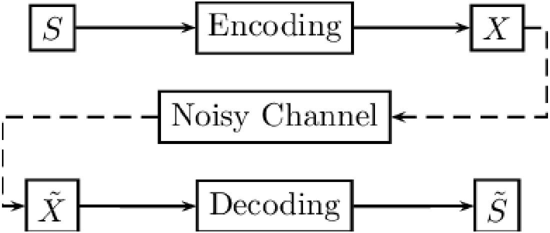
(From the Perspective of Linear Algebra)

Hengfeng Wei

hfwei@nju.edu.cn

May 13, 2019


Welcome to
Linear
Algebra



Q : Where is Cryptography?

$$\boxed{\mathrm{Col}(G_{n\times k}) = C = \mathrm{Nul}(H_{(n-k)\times n})}$$

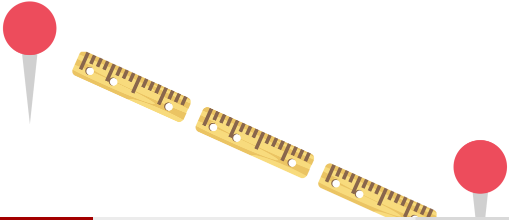
$$\boxed{(n, k, d)}$$

n : length

k : # of information bits

d : distance

$\boxed{\text{Hamming}(7, 4, 3)}$



Definition (Linear Code)

A linear code C of length n is a linear subspace of the vector space $\mathbb{Z}_2^n$ ($\mathbb{F}_q^n$).

$$c_1 \in C, c_2 \in C \implies c_1 + c_2 \in C$$

$$\begin{aligned} d(C) &= \min\left\{ d(c_1, c_2) \mid c_1 \neq c_2, c_1, c_2 \in C \right\} \\ &= \min\left\{ w(c_1 + c_2) \mid c_1 \neq c_2, c_1, c_2 \in C \right\} \\ &= \min\left\{ w(c) \mid c \neq 0, c \in C \right\} \end{aligned}$$

Problem 8.5-19

Let C be a linear code.

Show that either every codeword has even weight or exactly half of them have even weight.

Parity: $w(c_1) + w(c_2)$ *vs.* $w(c_1 + c_2)$

$$C = C_e \cup C_o$$

$$C_e \neq \emptyset \qquad c_o \in C_o$$

$$\boxed{f : x \in C_e \mapsto x + c_o \in C_o}$$

$$C_e \leq C; \quad C = C_e \cup C_o$$

Definition (Linear Code)

An (n, k) linear code C of length n and rank k is a linear subspace with dimension k of the vector space $\mathbb{Z}_2^n$.

Basis: $c_1, c_2, \ldots, c_k \quad (n \times 1)$ column vector

$$c_i = \alpha_1 c_1 + \alpha_2 c_2 + \cdots + \alpha_k c_k$$

$$C = \mathrm{Span}(c_1, c_2, \cdots, c_k)$$

Definition (Generator Matrix)

A matrix $G_{n\times k}$ is a generator matrix for an (n,k) linear code C if

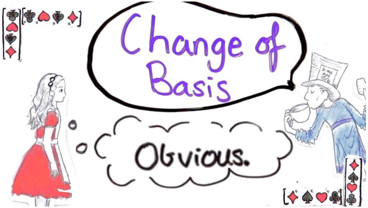
$$C = \mathrm{Col}(G)$$

$$\boxed{G_{n\times k} = \begin{bmatrix} c_1 & c_2 & \cdots & c_k \end{bmatrix}}$$

$$G_{(n\times k)} \cdot d_{k\times 1} = c_{n\times 1} \in C$$

Problem 8.5-7

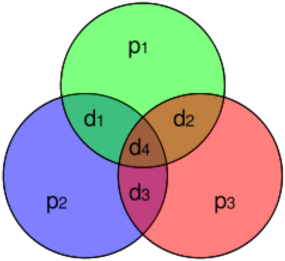
Generator matrices are NOT unique.



Definition (Standard Generator Matrix)

$$G_{n\times k} = \begin{bmatrix} I_k \\ A_{(n-k)\times k} \end{bmatrix}$$

Generator matrix for Hamming code $(7, 4, 3)$



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

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$
G \cdot \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ p_1 = d_1 + d_2 \quad\quad + d_4 \\ p_2 = \quad\quad d_2 + d_3 + d_4 \\ p_3 = d_1 \quad\quad + d_3 + d_4 \end{pmatrix}
$$

Each parity-check bit is a linear combination of some data bits.

$$
\begin{aligned}
d_1 + d_2 \qquad\quad + d_4 + p_1 \qquad\qquad\qquad &= 0 \\
d_2 + d_3 + d_4 \qquad\quad + p_2 \qquad\quad &= 0 \\
d_1 \qquad\quad + d_3 + d_4 \qquad\qquad\qquad\quad + p_3 &= 0
\end{aligned}
$$

$$
\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}
\begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ p_1 \\ p_2 \\ p_3 \end{pmatrix} = 0
$$

Definition (Parity-check Matrix)

A matrix $H_{(n-k) \times n}$ is a parity-check matrix for an (n, k) linear code C if

$$C = \text{Nul}(H)$$

$$\text{rank}(H) = n - k \quad \text{(full row rank)}$$

Each row represents a parity-check equation.

$$H_{(n-k) \times n} \cdot c_{n \times 1} = 0_{(n-k) \times 1}$$

Parity-check matrices are NOT unique.

Elementary Row Operations.

Definition (Standard Parity-check Matrix)

$$H_{(n-k)\times n} = \left[A_{(n-k)\times k} \mid I_{n-k} \right]$$

$$\boxed{\mathrm{Col}(G_{n\times k}) = C = \mathrm{Nul}(H_{(n-k)\times n})}$$

$$G_{n\times k} \cdot d_{k\times 1} = c_{n\times 1} \in \mathrm{Nul}(H_{(n-k)\times n})$$

$$H_{(n-k)\times n} \cdot G_{n\times k} \cdot d_{k\times 1} = 0_{(n-k)\times 1}$$

$$\begin{aligned}
H_{(n-k)\times n} &\cdot G_{n\times k} \\
&= \left[A_{(n-k)\times k} \mid I_{n-k} \right] \cdot \begin{bmatrix} I_k \\ A_{(n-k)\times k} \end{bmatrix} \\
&= A_{(n-k)\times k} \cdot I_k + I_{n-k} \cdot A_{(n-k)\times k} \\
&= A_{(n-k)\times k} + A_{(n-k)\times k} \\
&= 0_{(n-k)\times k}
\end{aligned}$$

$$r = c + e_i$$

$$r = c + (e_i + e_j + \cdots)$$

Definition (Syndrome)

$$\begin{aligned} S(r) &= Hr \\ &= H(c + (e_i + e_j + \cdots)) \\ &= H(e_i + e_j + \cdots) \\ &= He_i + He_j + \cdots \end{aligned}$$

Theorem (Extracting $d(C)$ from H)

If H is the parity-check matrix for a linear code C, then $d(C)$ equals the minimum number of linearly dependent columns of H.

Theorem (Extracting $d(C)$ from H)

If H is the parity-check matrix for a linear code C, then $d(C)$ equals the minimum number of linearly dependent columns of H.

Proof.

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

$$Hc = 0$$

$$\sum_{i=1}^{n} (c_i \cdot H_i) = 0$$

H_i : the i^{th} column of H

□

Theorem (Single Error-detecting Code (Theorem 8.31))

$$
\begin{aligned}
& d(C) \geq 2 \\
& \qquad \iff \forall \{c_i\} \ \textit{linearly independent} \\
& \qquad \iff \textit{no zero column}
\end{aligned}
$$

Theorem (Single Error-correcting Code (Theorem 8.34))

$$
\begin{aligned}
& d(C) \geq 3 \\
& \qquad \iff \forall \{c_i, c_j\} \ \textit{linearly independent} \\
& \qquad \iff \textit{no zero column, no identical columns}
\end{aligned}
$$

Problem 8.5-21

If we are to use an error-correcting linear code to transmit the 128 ASCII characters, what size matrix must be used?

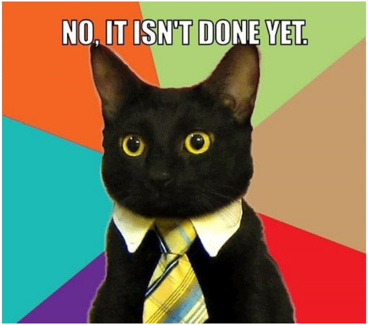
We consider single error-correcting code.

$$H_{(n-k)\times n} = \left[A_{(n-k)\times k} \mid I_{n-k} \right]$$

$$r \triangleq n - k \quad (k = 7)$$

$$k \le 2^r - 1 - r \implies r \ge 4$$

$$H_{4\times 11} : \quad (11, 7) \text{ code}$$



Hamming Code (wiki): General Algorithm

Problem 8.5-21

If we are to use an error-correcting linear code to transmit the 128 ASCII characters, what size matrix must be used? What if we require only error detection?

We consider single error-detecting code.

$$r \triangleq n - k = 1 \text{ is sufficient : } (8, 7) \text{ code}$$

Problem 8.5-23

How many check positions are needed for a single error-correcting code with $k = 20$?

$$r \triangleq n - k \quad (k = 20)$$

$$k \leq 2^r - 1 - r \implies r \geq 5$$

Problem 8.5-22

Find the standard H and G that gives the even parity check bit code with $k = 3$.

$$r \triangleq n - k = 1$$

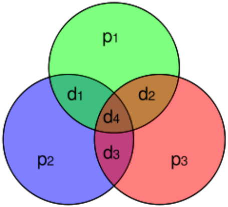
$$d_1 + d_2 + d_3 + p = 0$$

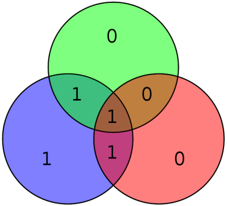
$$H_{(n-k)\times n} = H_{1\times 4} = [1, 1, 1, 1] \qquad G_{n\times k} = G_{4\times 3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

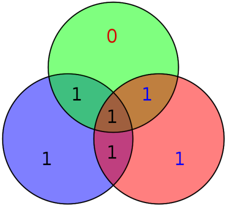
$\textit{Detect}\ d-1$ errors

$\textit{Correct}\ \lfloor \frac{d-1}{2} \rfloor$ errors

Hamming(7, 4, 3)

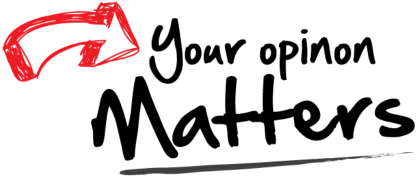






Hamming(7, 4, 3) cannot distinguish
between single-bit errors and two-bit errors.


THANK YOU



Office 302

Mailbox: H016

hfwei@nju.edu.cn