Linearis kodok

mit jelent?

definicio: $C \subset \mathbb{F}_q^n$ linearis, ha C egy alter $\mathbb{F}_q^n$-ben. Ekkor $k = \dim(C)$ a kod dimenzioja.
Specialisan $|C| = q^k$. Ekkor C egy (n, k) kod.

linearis kodoknal

Singleton-korlat: $k \leq n - d + 1$
kodsuly: $w(C) = d(C)$
Hamming-korlat: $C \subset \mathbb{F}_q^n$ egy linearis (n, k) kod, amely t hibat tud javitani.
Ekkor

$$\sum_{i=0}^{n} \binom{n}{i} (q-1)^i \leq q^{m-k}$$

1.

Legyen V egy vektorter. $W \subset V$ egy linearis alter, ha
1 $V \neq \emptyset$
2 $w_1, w_2 \in W,\ a, b \in \underbrace{\mathbb{K}}_{\mathbb{K}=\mathbb{R} \vee \mathbb{C}} \Longrightarrow a \cdot w_1 + b \cdot w_2 \in W$
3 $O \in W$

a

$$(c_1, c_2, c_3) \to (c_1, c_2, c_3, c_1 + c_2 + c_3) \quad c_1, c_2, c_3 \in \mathbb{F}_2$$

1

$$(0, 0, 0) \to (0, 0, 0, 0)$$

2

$$a(u_1, u_2, u_3, u_1 + u_2 + u_3) + b(v_1, v_2, v_3, v_1 + v_2 + v_3) = (a \cdot u_1 + b \cdot v_1, a \cdot u_2 + b \cdot v_2 a \cdot c_3 + b \cdot c_3, c_1 + c_2 + c_3)$$

inkabb engedjuk el

b

$$(c_1, c_2) \to (c_1, c_2, c_1 + c_2, \max\{c_1, c_2\})$$

$$C \neq \emptyset$$
$$(0, 0) \to (0, 0, 0, 0)$$
$$a \cdot (u_1, u_2, u_1 + u_2, \max\{u_1, u_2\}) + b(v_1, v_2, v_1 + v_2, \max\{v_1, v_2\}) = (..., a \cdot \max\{u_1, u_2\} + b \cdot \max\{v_1, v_2\}) =$$
$$= (1, 1, 0, 1) + (1, 0, 1, 1) = (0, 1, 1, 0) \Longrightarrow \text{ellentmondas}$$

2.

C linearis (n, k) kod $\Longrightarrow$ C alter $\Longrightarrow$ $c_1, ..., c_n \in C$ szavak, melyek generaljak a C alteret.

$$< c_1, ..., c_k >= \left\{a_1 \cdot c_1 + a_2 \cdot c_2 + ... + a_n \cdot c_n \in \mathbb{F}_q\right\} = C$$

Generator matrix:
C egy linearis (n, k) kod $c_1, ..., c_k$ generatorokkal.
Ekkor C egy generatormatrixa $G = (c_1, ..., c_k) \in \mathbb{F}_q^{n \times k}$

n-szeres ismetles kod: $G = (1, 1, ..., 1)^T = 1^T \in \mathbb{F}_q^{n \times 1}$
paritasbites kod: $G = \binom{I}{1} \in \mathbb{F}_n^{(k+1) \times k}$

Egy $u \to G_u$ kodolas szisztematikus, ha a kodszavak utolso $n - k$ elemet elhagyva a kodolando szot kapjuk.
$G = \binom{I}{B}, B \in \mathbb{F}_q^{(n-k) \times k}$

pelda

$$(c_1, c_2) \to (c_1, c_2, c_1 + c_2)$$

ez egy paritasbites kodolas

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

$$G \cdot c = \begin{pmatrix} c_1 \\ c_2 \\ c_1 + c_2 \end{pmatrix}$$

Ellenorzo matrix: C egy (n, k) kod. C egy ellenorzo matrix. $H \in \mathbb{F}_q^{(n-k) \times n}$
$H_c = 0$ pontosan akkor ha $c \in C$

n-szeres ismetles kod: $H = (I_{n-1}, -1) \in \mathbb{F}_q^{(n-1) \times n}$

paritasbites: $H = 1 = (1, ..., 1) \in \mathbb{F}_q^{1 \times (k+1)}$

Minimalis tavolsag: C egy (n, k) kod, $H \in \mathbb{F}_q^{(n-k) \times n}$ a C kod ellenorzo matrixa.
Pontosan d a kod minamalis tavolsaga, ha a H minden $\leq d - 1$ oszlopa linearisan fuggetlen.
Van H-nak d opszlopa, esek linearisan osszefuggoek

Legyen C egy (n, k) kod, $G \in \mathbb{F}_q^{n \times k}$ a C generatormatrixa, $H \in \mathbb{F}_q^{(n-k) \times n}$ pontosan akkor az ellenorzomatrixa ha $HG = O \in \mathbb{F}_q^{(n-k) \times k}$ rank $H = n - k$

Legyen C egy (n, k) kod, $G \in \mathbb{F}_q^{n \times k}$ a C generatormatrixa. TFH: $u \to G_u$ kodolas szisztematikus, azaz $G = \binom{I_u}{B} \in \mathbb{F}_q^{n \times k}, B \in \mathbb{F}_q^{(n-k) \times k}$. Ekkor $H = (-B, I_{n-k})$

3.

a.

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$n = 7, k = 4 \Longrightarrow (7,4) \text{ kod}$$

$$B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$H = (-B, I_{n-k}) = \begin{pmatrix} -1 & -1 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 & 1 & 0 \\ -1 & -1 & -1 & 0 & 0 & 0 & 1 \end{pmatrix} \Longrightarrow H \text{ minden } 1 \leq d-1 \text{ oszlopa linearisan fuggetlen}$$

b.

$$G_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$n = 7, k = 3 \Longrightarrow (7,3) \text{ kod}$$

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$H = (-B, I_{n-k}) = \begin{pmatrix} -1 & -1 & -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & -1 & -1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \Longrightarrow H \text{ minden } 1 \leq d-1 \text{ oszlopa linearisan fuggetlen}$$

4

a

$$(c_1, c_2, c_3) \to (c_1, c_2, c_3, c_1 + c_2 + c_3)$$

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

$$H = [-1, -1, -1, 1]$$

hany darab linearisan fuggetlen oszlopa van legfeljebb?

$$d = 2,$$
$$t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{2-1}{2} \right\rfloor = 0$$
$$k \stackrel{?}{=} n - d + 1$$
$$3 = 4 - 2 + 1$$
$$3 = 3 \Longrightarrow \text{MDS}$$

Hamming korlat:

$$\sum_{i=1}^{t} \binom{n}{i} (q-1)^i \leq q^{n-k} \Longrightarrow \sum_{i=0}^{0} \binom{4}{i} (2-1)^i \stackrel{?}{=} 2^{4-3} = \binom{4}{0} (1)^0 = 2^1 \Longrightarrow 1 \neq 2 \Longrightarrow \text{nem perfekt kod}$$

c

$$(c_1, c_2, c_3) \to (c_1, c_2, c_3, 2c_1 + 3c_2, c_1 + 4c_3) \in \mathbb{F}_5$$
$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 3 & 0 \\ 1 & 0 & 4 \end{pmatrix}$$
$$H = \begin{pmatrix} -2 & -3 & 0 & 1 & 0 \\ -1 & 0 & -4 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 0 & 1 & 0 \\ 4 & 0 & 1 & 0 & 1 \end{pmatrix} \Longrightarrow d \leq 2$$
$$k \stackrel{?}{=} n - d + 1 \Longrightarrow 3 \neq 4 \Longrightarrow \text{nem MDS}$$
$$\text{nem perfekt}$$