$C$ je $(M, n, d)$-kód: kódová slova délky $n$ (nad abecedou s $q$ znaky)
$|C| = M$
$\forall u \neq w \in C \quad dist(u, w) \geq d$
↑ #souřadnic i kde $u_i \neq w_i$

& definice plyne: 1) $C$ je odolné na $d-1$ chyb
nastala žádná chyba
stalo se $1-(d-1)$ chyb
alespoň $d$ chyb

2) $t := \lfloor \frac{d-1}{2} \rfloor$ pokud nastane $\leq t$ chyb
tak $\exists$ právě jedno $w \in C$ t.ž. se od přijatého slova liší $\leq t$ souřadnicích

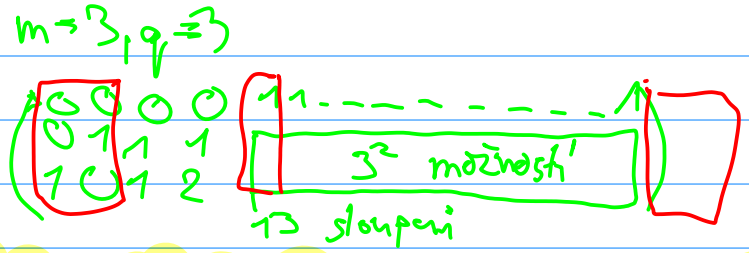
**Lineární kód** ≡ $q$ je mocnina prvočísla, $\mathbb{F}_q$ $q$-prvkové těleso
$C \subseteq (\mathbb{F}_q)^n$ je lineární podprostor

$G$ matice generující $C$, $H$ kontrolní matice generuje jádro $G$

Hammingovy kódy pro $m \in \mathbb{N}$, $q$ mocnina prvočísla

$H = \begin{bmatrix} | & | & \cdots & | \\ \text{sloupce } H & & & \end{bmatrix}$ } $m$

všechny nenulové vektory z $\mathbb{F}_q^m$ t.ž. 1. nenulová souřadnice je $= 1$




každé 2 sloupce $s_1 \neq s_2$ z $H$ jsou LN

kdyby $\exists \alpha, \beta \; \alpha s_1 + \beta s_2 = 0$ $(\alpha, \beta) \neq (0, 0)$ kdyby $\alpha = 0$ tak $\beta s_2 = 0$ ✓

$\alpha \neq 0, \beta \neq 0$ pokud by 1. nenulová $s_1 =: i_1$
1. nenulová $s_2 =: i_2$
$i_1 \neq i_2$, BÚNO $i_1 < i_2$ tak v $(\alpha s_1 + \beta s_2)_{i_1} = \alpha (s_1)_{i_1}$ ✓

$\alpha s_1 + \beta s_2 = 0 \iff \alpha s_1 = (-\beta) s_2$

$\Rightarrow [\underbrace{\alpha \cdot (-\beta)^{-1}}_{=1}] \cdot s_1 = s_2 \quad \Rightarrow s_1 = s_2$ ↯

---

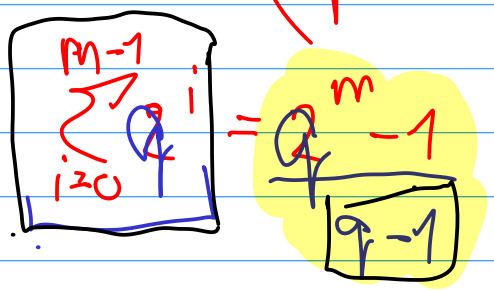
$\Leftarrow$ $G$ je matice popisující $\ker H$ a generuje kód

pro $n = \frac{q^m - 1}{q-1}$ ($q^{n-m} \mid n, 2$)

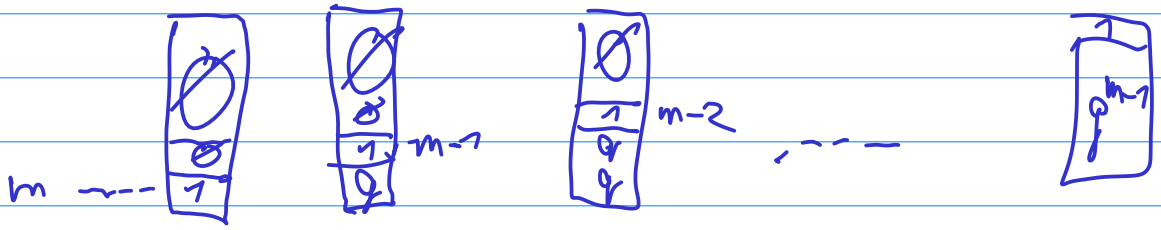
pro $n = \#$ nenulových $v \in \mathbb{F}^m$ t.ž. 1. nenulová souřadnice $= 1$

$(n-1)! \gg (q^m - 1)$

Př.: $q = 2$




všechny $\neq \emptyset$ vektory z $\mathbb{F}^m$ začíst ekvivalenci $v \sim w$ pokud se liší pouze 1. nenulovou souřadnicí




---

Věta (Hammingova): mějme $(M, n, d)$-kód nad abecedou s $q$ symboly

$t := \lfloor \frac{d-1}{2} \rfloor$. Potom platí

$\Updownarrow$ $d \geq 2t+1$

$$M \cdot \left( \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \right) \leq q^n$$

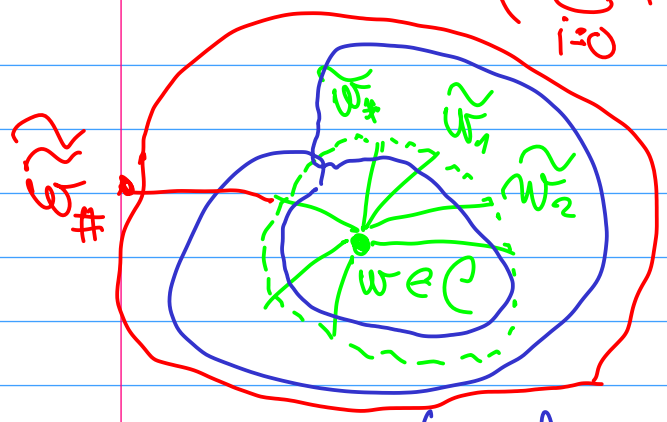
Def: $(M, n, d)$-kód nad abecedou s $q$ znaky je PERFEKTNÍ

NASTÁVÁ ROVNOST

Hammingovy kódy jsou perfektní

$$q^{n-m} \cdot \underbrace{(1 + n(q-1))}_{1 + (q^m - 1)} = q^n$$

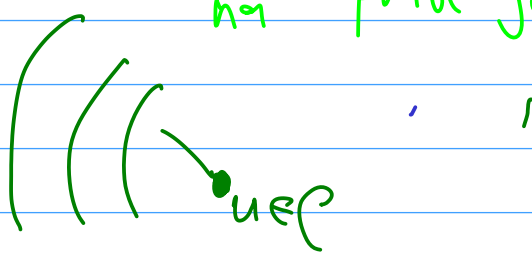
Dk(věta): $M \cdot \left( \sum_{i=0}^{t} \binom{n}{i}(q-1)^i \right) \leq q^n$




$\tilde{w}_i$ se liší od $w$ na právě jedném místě

#slov lišících se od $w$ na $\leq t$ místech:

- $n(q-1)$
- $\binom{n}{2}(q-1)^2$
- ⋮
- $\binom{n}{t}(q-1)^t$




#slov lišících se od $u$ na $\leq t$ místech:

- $n(q-1)$
- $\binom{n}{2}(q-1)^2$
- ⋮
- $\binom{n}{t}(q-1)^t$

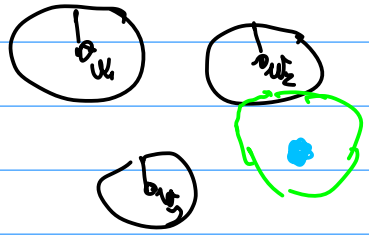
koule okolo $u$ a $w$ jsou disjunktní

$$\sum_{w \in C} |B(w,t)| = \sum_{w \in C} \left(1 + n(q-1) + \dots + \binom{n}{t}(q-1)^t\right)$$

$$= M \cdot \left( \sum_{i=0}^{t} \binom{n}{i}(q-1)^i \right) \leq q^n \quad \text{(HM)}$$

DCV: pokud $(M, n, 3)$-kód nad $\mathbb{Z}_2$ je perfektní, pak $n = 2^m - 1$ pro nějaké $m \in \mathbb{N}$

$n \neq 2^m - 1$



**Def:** $C_1, C_2 \subseteq \mathbb{F}^n$ **lineární** kódy nad $\mathbb{F}$.

Řekneme, že $C_1$ je ekvivalentní $C_2$ pokud

$\exists \Pi \in S_n$ t.ž. $(\alpha_1 \alpha_2 \dots \alpha_n) \in C_1$

$\Leftrightarrow$

$(\alpha_{\Pi(1)} \alpha_{\Pi(2)} \dots \alpha_{\Pi(n)}) \in C_2$

**Def:** Lineární kód $C \subseteq \mathbb{F}^n$ dimenze $k$ ($\text{rank}(G) = k$, $|C| = q^k$) je systematický pokud

$\forall \alpha_1, \dots, \alpha_k \in \mathbb{F}$ $\exists$ právě jedna volba

$\alpha_{k+1} \dots \alpha_n \in \mathbb{F}$ t.ž.

$\alpha_1 \alpha_2 \dots \alpha_k \alpha_{k+1} \dots \alpha_n \in C$

$G = ($  $)$

**Věta:** systematický L. kód $\Rightarrow$ $G = \left[\begin{array}{c|c} 1 & \\ & \\ & F \end{array}\right]$ $H = \left[\begin{array}{c|c} -F & \\ & 1 \end{array}\right]$

**Dcv:** pokud $C \subseteq \mathbb{F}^n$ je lineární kód, $\exists$ systematický kód $C_S \subseteq \mathbb{F}^n$ t.ž. $C \Leftrightarrow C_S$