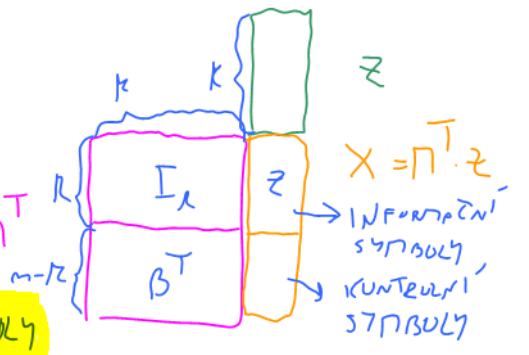
SAMOOPRAVNÉ KÓDY - LINEÁRNÍ KÓDY

- Připomenutí z minula:
  - LINEÁRNÍ KÓD je podprostor vektorového prostoru $\mathbb{K}^n$ kde $\mathbb{K}$ je konečné těleso (a zároveň $\mathbb{K}$ tvoří abecedu Σ)
    - s parametry n, k, d, q se značí $[n, k, d]_q$
    - víme, že každé konečné těleso $\mathbb{K}$ obsahuje Galoisovo těleso $\mathbb{F}_q$
  - $\forall x, y, z \in \mathbb{K}^n : d(x, y) = d(x+z, y+z) = d(x-y, 0)$
  - $\Rightarrow$ minimální vzdálenost d se rovná $\min\{d(x-y,0) = \min\{d(x,0)\}$ $x, y \in C$, $x \neq y$; $x \in C$, $x \neq 0$
    - $\Rightarrow$ ke zjištění d není třeba zkoumat všechny dvojice, stačí počítat nenulové složky kódových slov
- Výhoda lineárních kódů - úsporný popis - namísto všech q^k prvků kódu stačí uvést k prvků nějaké jeho báze
  - GENERUJÍCÍ MATICE kódu C = matice $\Pi \in \mathbb{F}^{k \times n}$ jejíž řádky tvoří bázi kódu C
- V prostoru $\mathbb{F}_q^n$ definujeme SKALÁRNÍ SOUČIN $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$ pro $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$
  - není skalárním součinem podle klasické definice, protože neplatí $\langle x, x \rangle = 0 \Leftrightarrow x = 0$ (například pro $x = (1,1,0,0)$ nad $\mathbb{F}_2$)
- DUÁLNÍM KÓDEM k lineárnímu kódu C je jeho ortogonální doplněk

  $C^\perp = \{x \in \mathbb{F}_q^n : \langle x, y \rangle = 0$ pro každé $y \in C\}$
  - z povahy našeho skalárního součinu nemusí být $C \cap C^\perp = \{0\}$
  - platí $\dim(C^\perp) + \dim(C) = n$ a $(C^\perp)^\perp = C$
  - generující matice $\Pi^\perp$ kódu $C^\perp$ se nazývá KONTROLNÍ MATICÍ
    - řádky kontrolní matice určují lineární rovnice, které musí každé slovo z C splňovat (a naopak každý vektor z $\mathbb{F}_q^n$, který je splňuje, je kódovým slovem v C
    - neboli $C = \{x \in \mathbb{F}_q^n : \Pi^\perp \cdot x = 0\}$

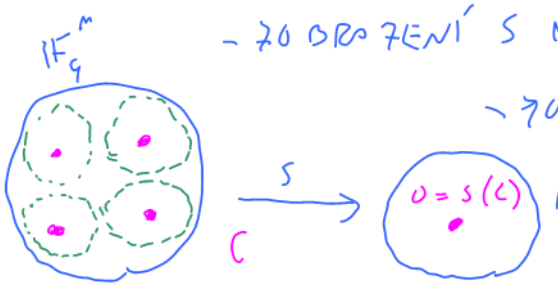
- MĚJME LINEÁRNÍ KÓD C S PARAMETRY $[m, k, d]_q$

- KÓDOVÁNÍ LINEÁRNÍMI KÓDY:
  - ZE VSTUPNÍHO SLOVA $z \in \mathbb{F}_q^k$ CHCEME VYTVOŘIT KÓDOVÉ SLOVO $x \in C \subseteq \mathbb{F}_q^m$
  - NECHŤ $\Pi \in \mathbb{F}_q^{k \times m}$ JE GENERUJÍCÍ MATICE KÓDU C
  - PRO KAŽDÝ LINEÁRNÍ KÓD EXISTUJE EKVIVALENTNÍ KÓD, JEHOŽ GENERUJÍCÍ MATICE MÁ TVAR $\left[\begin{array}{c|c} I_k & B \end{array}\right]_k$ (TZV. STANDARDNÍ FORMA)
    - STAČÍ GENERUJÍCÍ MATICI UPRAVIT GAUSSOVOU ELIMINAČNÍ METODOU A PŘÍPADNĚ PERMUTOVAT SLOUPCE
  - $\Rightarrow$ BUĎ MATICE Π JE VE STANDARDNÍ FORMĚ
  - JAKO KÓDOVÉ SLOVO ZVOLÍME $x = \Pi^T z \in C$
    - $\Rightarrow x$ MÁ NA PRVNÍCH k SOUŘADNICÍCH SLOVO z (TZV. INFORMAČNÍ SYMBOLY) A NA ZBYLÝCH $m-k$ SOUŘADNICÍCH OBSAHUJE TZV. KONTROLNÍ SYMBOLY



- DEKÓDOVÁNÍ LINEÁRNÍMI KÓDY:
  - U LINEÁRNÍCH KÓDŮ EXISTUJE METODA, JAK EFEKTIVNĚJI DEKÓDOVAT
  - TUTO METODU SI NYNÍ POPÍŠEME
  - PO ODESLÁNÍ $x \in C$ BYLO PŘIJATO $y \in \mathbb{F}_q^m$
  - PŘÍJEMCE ZNÁ POUZE y A CHCE NAJÍT KÓDOVÉ SLOVO, KTERÉ JE NEJBLÍŽ
  - NECHŤ $\Pi^\perp$ JE KONTROLNÍ MATICE KÓDU C
    - JE-LI GENERUJÍCÍ MATICÍ KÓDU C MATICE $\Pi = \left[\begin{array}{c|c} I_k & B \end{array}\right]_k$, PAK $\Pi^\perp = \left[\begin{array}{c|c} -B^T & I_{m-k} \end{array}\right]_{m-k}$, PROTOŽE PAK $\Pi^\perp \cdot \Pi^T = -B^T I_k + I_{m-k} B^T = 0$
  - JAKO SYNDROM SLOVA $y \in \mathbb{F}_q^m$ NAZVEME SOUČIN $\Pi^\perp \cdot y$
  - PROTOŽE $C = \{x \in \mathbb{F}_q^m : \Pi^\perp x = 0\}$, TAK MÁME URČENÉ LINEÁRNÍ ZOBRAZENÍ $s : \mathbb{F}_q^m \to \mathbb{F}_q^{m-k}$ SPLŇUJÍCÍ $C = \ker(s)$
    - JÁDRO ZOBRAZENÍ s
  - ZOBRAZENÍ s NAZVEME SYNDROM
  - ZOBRAZENÍ s JE NA, PROTOŽE PLATÍ:

$$\underbrace{\dim(\ker(s))}_{=\dim(C)=k} + \dim(\underbrace{\mathrm{Im}(s)}_{\text{OBRAZ } s}) = \underbrace{\dim(\mathbb{F}_q^m)}_{=m}$$



- **LEMMA 13.1:**
ZOBRAZENÍ s JE PROSTÉ NA $B(0,t)$, KDE $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

- **DK:**
- MĚJME $y, y' \in B(0,t)$, $y \neq y'$
- POTOM $d(y,y') \leq d(0,y) + d(0,y') \leq 2t$
HAMMINGOVA VZDÁLENOST; Δ-NEROVNOST; $y, y' \in B(0,t)$; s JE LINEÁRNÍ
- SPOREM - NECHŤ $s(y) = s(y')$, POTOM $0 = s(y) - s(y') = s(y - y')$
- $C = \ker(s) \Rightarrow y - y' \in C$
- DÁLE PRO KAŽDÉ $x \in C \setminus \{0\}$ PLATÍ $d(x,0) \geq d \geq 2t+1$ A
$d(0, y-y') = d(y,y') \leq 2t$
d = MIN. VZDÁLENOST; $t = \left\lfloor \frac{d-1}{2} \right\rfloor$
$\Rightarrow y - y' = 0$ A TEDY $y = y'$ $\Rightarrow$ SPOR ⊠

- POUŽIJE LEMMA 13.1 TEDY K $s|_{B(0,t)}$ EXISTUJE INVERZNÍ ZOBRAZENÍ
↳ s OMEZENÉ NA $B(0,t)$

s^{-1}: $s(B(0,t)) \longrightarrow B(0,t)$
- s^{-1} NENÍ LINEÁRNÍ, ALE JDE POPSAT TABULKOU S q^{n-k} ŘÁDKY Z $B(0,t)$
- V TÉTO TABULCE JE PRO KAŽDÝ SYNDROM SLOVA ULOŽENO NĚJAKÉ SLOVO S MINIMÁLNÍ VÁHOU A S DANÝM SYNDROMEM
- NYNÍ VÍME, ŽE PLATÍ:
1) PRO $y \in B(x,t)$ MÁME $s(y-x) \overset{s \text{ LIN.}}{=} s(y) - \underbrace{s(x)}_{=0, \text{ PROTOŽE } x \in C = \ker(s)} = s(y)$
- NEBOLI y A VZNIKLÁ CHYBA $y - x$ MAJÍ STEJNÝ SYNDROM
2) PRO $y \in B(x,t)$ MÁME $y - x \in B(0,t)$ A TEDY $y - x = s^{-1}(s(y-x))$
- NEBOLI VZNIKLOU CHYBU JDE URČIT POUZE S
$s^{-1} \circ s$ JE IDENTITOU NA $B(0,t)$
3) $x = y - (y-x) \overset{2)}{=} y - s^{-1}(s(y-x)) \overset{1)}{=} y - s^{-1}(s(y))$ - NEZÁVISÍ NA x
- PRO DANÉ y POUZE SYNDROMU $s(y)$ DOKÁŽEME URČIT KÓDOVÉ SLOVO x, ZE KTERÉHO VZNIKLO, NASTALO-LI $\leq t$ CHYB

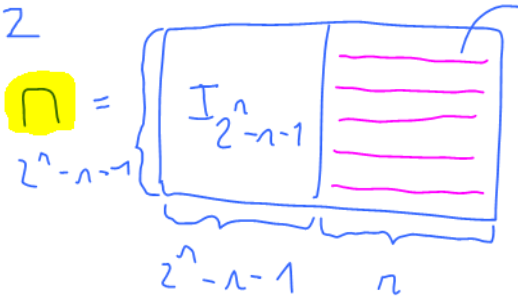
- JAK TEDY DEKÓDOVAT:
- PRO PŘIJATÉ SLOVO $y \in \mathbb{F}_q^n$ SPOČÍTAT $x = y - s^{-1}(\pi^{\perp}(y))$, KDE $\pi^{\perp}$ JE KONTROLNÍ MATICE A ZOBRAZENÍ s^{-1} MÁME PŘEDPOČÍTANÉ JAKO TABULKU
- NASTALO-LI $\leq t$ CHYB, JE x KÓDOVÉ SLOVO, ZE KTERÉHO y VZNIKLO

- **TVRZENÍ 13.2**:

VZDÁLENOST d KÓDU C = MINIMÁLNÍ POČET LINEÁRNĚ ZÁVISLÝCH SLOUPCŮ KONTROLNÍ MATICE H^T

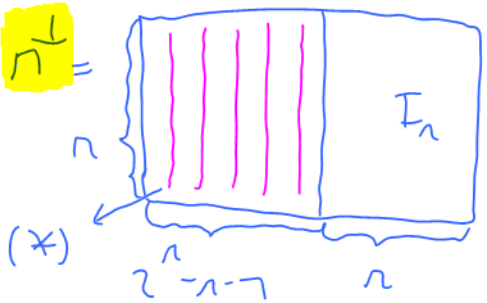
- **DK**:
  - VÍME, ŽE d = MINIMÁLNÍ POČET NENULOVÝCH SYMBOLŮ V NENULOVÉM SLOVĚ x Z C
  - $x \in C \Leftrightarrow H^T x = 0$ A TEDY SLOUPCE H^T VYBRANÉ NENULOVÝMI SLOŽKAMI x JSOU LINEÁRNĚ ZÁVISLÉ ⊠

- **HAMMINGOVY KÓDY**:
  - PŘÍKLAD LINEÁRNÍCH KÓDŮ, KTERÉ JSOU DOKONCE PERFEKTNÍ
  - JEJICH NEVÝHODOU JE, ŽE NEDOKÁŽÍ OPRAVIT PŘÍLIŠ MNOHO CHYB
  - NAD TĚLESEM $\mathbb{F}_2$ (TEDY $q=2$)
  - PŘIROZENÉ PARAMETR $n \geq 2$
  - GENERUJÍCÍ MATICE G =



VŠECHNY NENULOVÉ VEKTORY Z $\mathbb{F}_2^n$ RŮZNÉ OD VEKTORŮ KANONICKÉ BÁZE (*)

⇒ KONTROLNÍ MATICÍ H^T =



- SLOUPCE = NENULOVÉ VEKTORY Z $\mathbb{F}_2^n$
- DVA VEKTORY Z $\mathbb{F}_2^n \setminus \{0\}$ JSOU LINEÁRNĚ ZÁVISLÉ $\Leftrightarrow$ JSOU TOTOŽNÉ ⇒ ⇒ MINIMÁLNÍ POČET LINEÁRNĚ ZÁVISLÝCH SLOUPCŮ V H^T JE 3 A PODLE **TVRZENÍ 13.2** JE VZDÁLENOST KÓDU 3 (PRO $n \geq 2$)

⇒ TEDY SE O KÓD S PARAMETRY $[2^n-1, 2^n-n-1, 3]_2$ (3: OPRAVÍ SE 1 CHYBA)

- **PŘÍKLAD**:
  - PRO $n=3$ DOSTÁVÁME KÓD S PARAMETRY $[7,4,3]_2$
  - JEDNÁ SE O KÓD SESTAVENÝ Z FANOVY ROVINY PŘI ÚKOLU PUČÍTKA A DOPLŇKŮ

- HAMMINGOVY KÓDY JSOU PERFEKTNÍ:

- STAČÍ UKÁZAT, ŽE HAMMINGŮV ODHAD $|C| \leq \frac{q^n}{V(t)}$ JE TĚSNÝ

- $t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$

- $V(t) = V(1) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i = 1 + (2^n - 1) = \underline{\underline{2^n}}$

- $\frac{q^n}{V(1)} = \frac{2^{2^n-1}}{2^n} = \underline{\underline{2^{2^n-n-1}}}$

- $|C| = 2^k = \underline{\underline{2^{2^n-n-1}}}$ ⇒ HAMMINGŮV ODHAD JE SKUTEČNĚ PRO HAMMINGOVY KÓDY TĚSNÝ

↓ VOLBA PRVKŮ BÁZE

- DÁ SE I LÉPE REPREZENTOVAT FUNKCE s^{-1}:

- TABULKA REPREZENTUJÍCÍ s^{-1} MÁ POUZE $2^{n-k} = 2^{2^n-1-(2^n-n-1)} = 2^n = n+1$ PRVKŮ
- VE SKUTEČNOSTI TABULKU VŮBEC NEPOTŘEBUJEME
- ZPERMUTUJEME-LI SLOUPCE P PODLE $\Pi^{\perp}$ PAK, ABY i-TÝ SLOUPEC BYL BINÁRNÍM ZÁPISEM ČÍSLA i, PAK $s(y)$ UDÁVÁ POZICI, NA NÍŽ NASTALA CHYBA

$$\Pi^{\perp} = \begin{pmatrix} 0 & 0 & 0 & & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 1 & \cdots & \vdots \\ 0 & 1 & 0 & & \vdots \\ 1 & 0 & 1 & & 1 \end{pmatrix}$$

BINÁRNĚ 1 2 3 4 ...

- PROTOŽE $d=3$, PAK STAČÍ UVAŽOVAT JEN ≤ 1 CHYBU
- PRO $y = x = (0, \ldots, 0, 1, 0, \ldots, 0)^T$ JE $s(y) = i$-TÝ SLOUPEC $\Pi^{\perp}$ = BINÁRNÍ ZÁPIS i
- NASTALA-LI ≤ 1 CHYBA, PAK VÍME, ŽE PŘIJATÉ SLOVO y A CHYBA $y - x$ MAJÍ STEJNÝ SYNDROM

⇒ LZE DEKÓDOVAT NÁSLEDOVNĚ:

- JE-LI $s(y) = 0$, PAK $x = y$
- JINAK JE $s(y)$ BINÁRNÍM ZÁPISEM ČÍSLA i A PAK x = SLOVO VZNIKLÉ Z y VYNĚNOU BITU, KTERÝ JE V y NA POZICI i