

SAPUOPRAVNÉ KÓDY:

- PŘENOS DAT X PŘES KOMUNIKAČNÍ KANÁL, PŘI PŘENOSU MŮŽE DOJÍT K CHYBĚ A NA VÝSTUP MŮŽE BÝT PŘIJATO $\gamma \neq X$
- CÍLE: 1) PŘENĚST CO NEJVÍCE DAT
2) UPRAVIT CO NEJVÍCE CHYB
- APLIKACE - KOMUNIKACE, UKLÁDÁNÍ DAT, ...



ŘÁKLAOVNÍ TERMINOLOGIE:

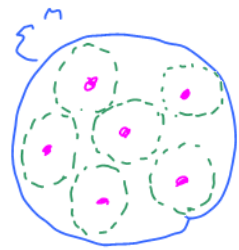
- **ABECEDA \Sigma** = KONKRETNÍ MNOŽINA SYMBOLŮ
- **SLONO DĚLKY m** = USPOŘÁVANÁ m-TICE SYMBOLŮ
- Σ^m = MNOŽINA SLON DĚLKY m NAD ABECEDOU \Sigma
- **HANNINGOVA VZÁLEENOST** SLON $X = (x_1, \dots, x_m), \gamma = (\gamma_1, \dots, \gamma_m) \in \Sigma^m$
JE $d(x, \gamma) = |\{i \in \{1, \dots, m\} : x_i \neq \gamma_i\}|$ = POČET POZIC, KDE SE X A \gamma LIŠÍ
- JE-LI X VSTUP A \gamma VÝSTUP KOMUNIKAČNÍHO KANÁLU, PAK $d(x, \gamma)$ JE POČET CHYB VLIKÝCH PŘI PŘENOSU X
- FUNKCE d JE METRIKA (LZE OVĚŘIT JAKO CVIČENÍ)
- A (Σ^m, d) JE TAK PŘÍKLADNĚ METRICKÉHO PROSTORU

- **(BLOKOVÝ) KÓD** JE PODMNOŽINA $C \subseteq \Sigma^m$ (C OBSAHUJE KÓOVNÍ SLONA SLONA, KTERÁ ODESÍLÁME)
- CO ZNAMENÁ, ŽE JSME POUČÍ KÓDY $C \subseteq \Sigma^m$ SCHVÍM UPRAVIT $\leq t$ CHYB?
- PRO KAŽDÉ $\gamma \in \Sigma^m$ EXISTUJE NEJVÍŠE JEHO $x \in C$ TAKOVÉ, ŽE $d(x, \gamma) \leq t$
- PAK MU PŘIJETÍ \gamma VÍDĚ, KTERÉ X BYLO ODESLÁNO
- ŽE MNOŽINA Σ^m VYBEREME NĚKTERÁ SLONA TAKOVÁ, ABYCHOM OUKAZALI $OPRAVIT \leq t$ CHYB

PARAMETRY KÓDU C:

- 1) DĚLKA m
 - 2) VELIKOST ABECEDY $q = |\Sigma|$
 - 3) DIMENZE $k = \log_q |C|$
 - 4) VZÁLEENOST $d = \min \{d(x, x') : x, x' \in C, x \neq x'\}$
- KÓD S PARAMETRY m, k, d, q ZNAČÍME $(m, k, d)_q$

- při použití kódu s parametry $(m, k, d)_q$ lze opravit $\leq \lfloor \frac{d-1}{2} \rfloor$ chyb (2)



- pro každé $x, x' \in C$ je $d(x, x') \geq d$ a tedy množina slov ve vztálosti $\leq \lfloor \frac{d-1}{2} \rfloor$ ob kódových slov jsou disjunktivní \Rightarrow lze opravit $\leq \lfloor \frac{d-1}{2} \rfloor$ chyb (na určitém straně více než d chyb už určitá kódy opravit nelze)

- nelze opravit více než $\lfloor \frac{m-1}{2} \rfloor$ chyb \rightarrow pro každý kód platí $d \leq m$

- příklady kódů:

1) **upřesňovací kód** - každý poslaný symbol m -krát zopakuje \rightarrow z abecedy velikosti q

\Rightarrow parametry $(m, 1, m)_q$

- opraví největší množství chyb, ale má malou velikost

2) **charakteristické vektory přínek konečné projektivní roviny:**

- konečná projektivní rovina (X, P) řádu m

- zvolíme kód $C = \{ \text{charakteristické vektory přínek} \} \subseteq \{0, 1\}^{m^2+m+1}$

\Rightarrow parametry $(m^2+m+1, \log_2 \underbrace{(m^2+m+1)}_{|P|}, \log_2 \underbrace{2}_{|Z|})_2$

Z přínek je vybráno v 1 souř. množství m^2+m přínek má na m přílech jedna příka zlevičky a druhá nulou, na valičím příkích to je obráceně

- pro $q=2$ existují ještě lepší kódy pro dané m a d

3) **Hadamardovy kódy:**

- sestaveny z řádků **Hadamardovy matice** $H \in \{-1, 1\}^{m \times m}$ splňující $H \cdot H^T = m \cdot I_m$, neboli každé dva řádky se liší v právě polovině symbolů

- zvolíme $C = \{ \text{řádky } H \} \cup \{ \text{řádky } -H \} \subseteq \{-1, 1\}^m$

\Rightarrow parametry $(m, 1 + \log_2(m), \frac{m}{2})_2$ (pokud pro dané m existuje Hadamardova matice $m \times m$)

- **Sylvesterova konstrukce** Hadamardovy matice:

$$H_1 = (1), H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, H_{2m} = \begin{pmatrix} H_m & H_m \\ H_m & -H_m \end{pmatrix} \text{ pro } m \geq 2$$

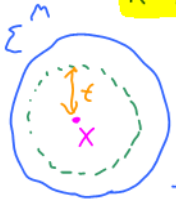
- **Dobsonova (Hadamardova podmínka)**

Hadamardovy matice existují pro každé m dělitelné 4

- ověřeno pro $m < 668$ nutná podmínka pro $m > 2$

- kódy $C, C' \subseteq \Sigma^m$ jsou **EKVIVALENTNÍ**, pokud existuje permutace $\pi \in S_m$
- tedy, že pro každé $x = (x_1, \dots, x_m) \in \Sigma^m$ platí $x \in C \iff \pi(x) = (x_{\pi(1)}, \dots, x_{\pi(m)}) \in C'$
- kódy se tím liší jen permutací pozic (stejná permutace u každého na všechny kódová slova)
- protože $d(x, y) = d(\pi(x), \pi(y))$, tak vidíme, že ekvivalentní kódy mají stejné parametry (existují ale neekvivalentní kódy se stejnými parametry)

- pro jaké volby parametrů m, k, d, q existují kódy?
 - **KOMBINATORICKÁ KULE** o středě x a poloměru t v Σ^m je



$$B(x, t) = \{y \in \Sigma^m : d(x, y) \leq t\}$$

- **putování n.z.1.:**

že-li C kód se vzdáleností $\geq t+1$, pak pro každé $x, y \in C$ platí $B(x, t) \cap B(y, t) = \emptyset$.

- **DK:**

- sporem $\exists z \in B(x, t) \cap B(y, t)$ a $d(x, y) \leq d(x, z) + d(z, y) \leq 2t \Rightarrow$ spor s $d(x, y) \geq 2t+1$ ☒

- velikost $B(x, t)$, neboli její **objem**, nezávisí na volbě x

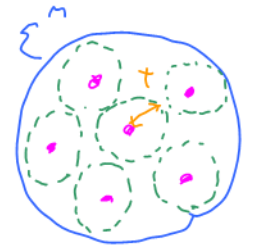
a je roven $V(t) = |B(x, t)| = \sum_{i=0}^t \binom{m}{i} (q-1)^i$

výběr odlišných symbolů na vybraných pozicích
 volba pozic, které přemění

- **VĚTA n.z. (HAMILTONSŮV OHLAD):**

pro každý kód C s parametry $(m, k, 2t+1)_q$ platí

$$|C| \leq \frac{q^m}{V(t)}$$



• = kódová slova

- **OK:**

- pakováním koulí
- velikost Σ^m je q^m a dostě $\Sigma^m \supseteq \bigcup_{x \in C} B(x, t)$
- protože vzdálenost je $\geq 2t+1$, tak podle **putování n.z.1.** jsou kombinatorické koule $B(x, t), B(x', t)$ s $x, x' \in C, x \neq x'$ disjunkční
- $\Rightarrow |C| \cdot |V(t)| \leq |\Sigma^m|$ a tedy $|C| \leq \frac{|\Sigma^m|}{|V(t)|} = \frac{q^m}{V(t)}$ ☒
- $\hookrightarrow B(x, t) \cap B(x', t) = \emptyset$ pro $x, x' \in C, x \neq x'$ a $\Sigma^m \supseteq \bigcup_{x \in C} B(x, t)$

- KÓDY S PARAMETRY $(m, k, 2t+1)_q$ SPLŇHJÍCÍ ROVNOST $|C| = \frac{q^m}{V(t)}$ SE (4)

MAŽYVATI PERFECTNÍ

- kombinatorické kódy pokrývají celé Σ^m , čili každé slovo z

Σ^m lze dekodovat

- PĚTI Tzv. **TRIVIÁLNÍ** PERFECTNÍ KÓDY PATŘÍ NAPŘÍKLAD OBKOVANÍ KÓD LICHÉ VELKÝ $q=2$,

- PŘÍKLAD NETRIVIÁLNÍHO PERFECTNÍHO KÓDU SI UKÁŽEME PŘÍŠTĚ

- EXISTUJE ANALYTICKÝ DŮLNÍ ODHAD K VĚTĚ 1

- **VĚTA 12.3 (SILBERTŮV-VARSHANŮV ODHAD):**

Pro každé $m, d, q \in \mathbb{N}$ existuje kód C s parametry $(m, k, d)_q$ takový, že

$$|C| \geq \frac{q^m}{V(d-1)}$$

$$k = m - \log_q(|C|)$$

- OBLICNÝ ODHAD, NĚMÍ PĚSNÝ VŮČI ODHADU Z VĚTY 12.2

DK:

- STAČÍ HLEDATĚ ODĚBÍRAT KÓDOVÁ SLOVA Z Σ^m SPULY SE SLOVY

že $V(d-1) \leq d-1$

- KÓDOVÁ SLOVA MOŽE ODĚBÍRAT PO $\geq \frac{q^m}{V(d-1)}$ KROKŮCH, PROTOŽE

$|\Sigma^m| = q^m$ A ODĚBÍRANÉ PRŮJITNÁ SLOVA NANEJDELIŽ TVŮŘÍ

ROZLIŠNÉ KOMBINATORICKÉ KÓDLE O PŮL PĚRHI $d-1$



LINEÁRNÍ KÓDY:

- EXISTUJÍ KÓDY, VE KTERÝCH UMÍME KÓDOVAT A DEKODOVAT EFEKTIVNĚ

- ČILI PRO VÝSIVNÍ SLOVO $y \in \Sigma^m$ LZE RYCHLE NAJÍT x , KTERÉ BYLO UDESLÁNO

- NĚMÍ POTŘEBA PROCHÁZĚT VŠECHNA x S $d(x, y) \leq d$

- PŘIPRAVÍME SI TEORII PRO POPIS TAKOVÝCH KÓDŮ

- POUŽÍME SPECIÁLNÍ ABSECVŮ S VLASTNOSTMI Z LINEÁRNÍ ALGEBRY

- **LINEÁRNÍ KÓD** JE PODPROSTOR VEKTOROVÉHO PROSTORU \mathbb{K}^m KŮE

\mathbb{K} JE KOMPEČNÉ TĚLESO (A ZÁRŮEŤ \mathbb{K} TVŮŘÍ ABSECVŮ Σ)

- S PARAMETRY m, k, d, q SE ZNAČÍ $[[m, k, d]]_q$

- \mathbb{F} LINEÁRNÍ ALGEBRA VÍNE, ŽE VEKTOROVÝ PROSTOR $C \subseteq K^m$ (5)
 SPLŇNĚ $|C| = |K|^{\dim(C)} = q^k \Rightarrow k$ JE CELOČÍSLNÉ

$|C| = |K| = q$

- PŘÍKLADY LINEÁRNÍCH KÓDŮ:

- 1) OPRAKOVACÍ KÓD JE LINEÁRNÍ NAD TĚLESEM \mathbb{Z}_q
 - KONTROLNÍ NA NÁSOBENÍ SKAINEPI SOUČET, OBSAHLÉ σ
- 2) CHARAKTERISTICKÉ VEKTORY KONEČNÝCH PROJEKTIVNÍCH ROVIN
 NEJLÉPŠÍ LINEÁRNÍ KÓD (NAD \mathbb{Z}_2)
- 3) HODNOCENÍ KÓDŮ NEJDEJÍ BYT LINEÁRNÍ, ALE TĚ ZÍSKANÉ
 SYLVESTRŮVŮ KONSTRUKCÍ LINEÁRNÍ JSOU (NAD TĚLESEM \mathbb{Z}_2)

- PRÁCE VE VEKTOROVÉM PROSTORU MÁN UPŮTÍ LÉPE POUŽÍVAT
 VZÁLEKOSTI - STAČÍ POUŽÍVAT VZÁLEKOSTI OD NULY

$\forall x, y, z \in K^m : d(x, y) = d(x+z, y+z) = d(x-\gamma, 0)$

x A y JSOU STEJNĚ
 NA PĚTAKÉ POUČÍ $\Leftrightarrow x+z$ A
 $y+z$ JSOU NA TĚTO POUČÍ STEJNĚ
 VOLBA $z = -y$

\Rightarrow MINIMÁLNÍ VZÁLEKOST 1 SE ROVNÁ $\min_{\substack{x, y \in C \\ x \neq y}} \{d(x, y)\} = \min_{\substack{x \in C \\ x \neq 0}} \{d(x, 0)\}$

\Rightarrow KE ZJIŠTĚNÍ A NEJÍ TŘEBA ŽKOUAT VŠECHNY BUDICE,
 STAČÍ POUŽÍVAT NEVULOVÉ SLOŽKY KÓDOVÝCH SLOV