SAMOOPRAVNÉ KÓDY:

- PŘENOS DAT x PŘES KOMUNIKAČNÍ KANÁL, PŘI PŘENOSU MŮŽE DOJÍT K CHYBÁM A NA VÝSTUPU MŮŽE BÝT PŘIJATO $y \neq x$
- CÍLE: 1) PŘENÉST CO NEJVÍC DAT
  2) OPRAVIT CO NEJVÍCE CHYB
- APLIKACE - KOMUNIKACE, UKLÁDÁNÍ DAT, ...

ZÁKLADNÍ TERMINOLOGIE:

- ABECEDA Σ = KONEČNÁ MNOŽINA SYMBOLŮ
- SLOVO DÉLKY n = USPOŘÁDANÁ n-TICE SYMBOLŮ
- Σ^n = MNOŽINA SLOV DÉLKY n NAD ABECEDOU Σ
- HAMMINGOVA VZDÁLENOST SLOV $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \Sigma^n$ JE $d(x,y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|$ = POČET POZIC, KDE SE x A y LIŠÍ
  - JE-LI x VSTUP A y VÝSTUP KOMUNIKAČNÍHO KANÁLU, PAK $d(x,y)$ JE POČET CHYB VZNIKLÝCH PŘI PŘENOSU x
  - FUNKCE d JE METRIKA (LZE OVĚŘIT JAKO CVIČENÍ)
  - A (Σ^n, d) JE PAK PŘÍKLADEM METRICKÉHO PROSTORU

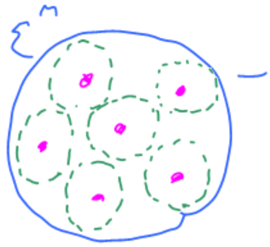
- (BLOKOVÝ) KÓD JE PODMNOŽINA $C \subseteq \Sigma^n$ (C OBSAHUJE KÓDOVÁ SLOVA)
  - (BLOKOVÝ): VŠECHNA SLOVA MAJÍ STEJNOU DÉLKU
  - KÓDOVÁ SLOVA: SLOVA, KTERÁ ODESÍLÁME
- CO ZNAMENÁ, ŽE JSME POMOCÍ KÓDU $C \subseteq \Sigma^n$ SCHOPNI OPRAVIT $\leq t$ CHYB?
  - PRO KAŽDÉ $y \in \Sigma^n$ EXISTUJE NEJVÝŠE JEDNO $x \in C$ TAKOVÉ, ŽE $d(x,y) \leq t$
    - PAK PO PŘIJETÍ y VÍME, KTERÉ x BYLO ODESLÁNO
- Z MNOŽINY Σ^n VYBEREME NĚKTERÁ SLOVA TAKOVÁ, ABYCHOM DOKÁZALI OPRAVIT $\leq t$ CHYB

PARAMETRY KÓDU C:

1) DÉLKA n
2) VELIKOST ABECEDY $q = |\Sigma|$
3) DIMENZE $k = \log_q |C|$
4) VZDÁLENOST $d = \min \{d(x,x') : x, x' \in C, x \neq x'\}$

- KÓD S PARAMETRY n, k, d, q ZNAČÍME $(n, k, d)_q$

– Při použití kódu s parametry $(n,k,d)_q$ lze opravit $\le \lfloor \frac{d-1}{2} \rfloor$ chyb



– Pro každé $x, x' \in C$ že $d(x,x') \ge d$ a tedy množiny slov ve vzdálenosti $\le \lfloor \frac{d-1}{2} \rfloor$ od kódových slov jsou disjunktní ⇒ lze opravit $\le \lfloor \frac{d-1}{2} \rfloor$ chyb (na druhou stranu více než d chyb už daným kódem opravit nelze)

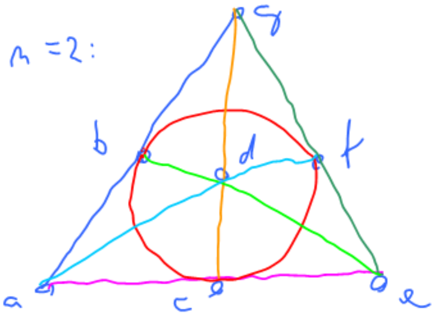
– Nelze opravit více než $\lfloor \frac{n-1}{2} \rfloor$ chyb → pro každý kód platí $d \le n$

– **Příklady kódů:**

1) **Opakovací kód** – každý poslaný symbol n-krát zopakujeme
↳ z abecedy velikosti q
⇒ parametry $(n,1,n)_q$
– opraví největší množství chyb, ale má malou velikost

2) **Charakteristické vektory přímek konečné projektivní roviny:**

$n=2$:



$C = \{1010100, 1100001, 0000111, 1001010, 0011001, 0101100, 0110010\}$

– konečná projektivní rovina (X, P) řádu n
– zvolme kód $C = \{$charakteristické vektory přímek z $P\} \subseteq \{0,1\}^{|X|}$

⇒ parametry $(n^2+n+1, \log_2(n^2+n+1), 2n)_2$

($n^2+n+1 = |X|$, $n^2+n+1 = |P|$, $\Sigma = \{0,1\}$)

2 přímky se shodují v 1 bodě, na zbylých n^2+n pozicích má na n pozicích jedna přímka jedničky a druhá nuly, na zbylých n pozicích to je obrácené

– pro $q=2$ existují ještě lepší kódy pro dané n a d

3) **Hadamardovy kódy:**
– sestrojeny z řádků **Hadamardových matic** $H \in \{-1,1\}^{n \times n}$ splňujících $H \cdot H^T = n \cdot I_n$, neboli každé dva řádky se liší v právě polovině symbolů
– zvolíme $C = \{$řádky $H\} \cup \{$řádky $-H\} \subseteq \{-1,1\}^n$
⇒ parametry $(n, 1+\log_2(n), \frac{n}{2})_2$ (pokud pro dané n existuje Hadamardova matice $n \times n$)
– **Sylvesterova konstrukce** Hadamardových matic:

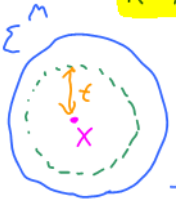
$$H_1 = (1), \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix} \text{ pro } n \ge 2$$

– **Domněnka** (**Hadamardova domněnka**): Hadamardovy matice existují pro každé n dělitelné 4 (nutná podmínka pro $n > 2$)
– ověřeno pro $n < 668$

- kódy $C, C' \subseteq \Sigma^n$ jsou **ekvivalentní**, pokud existuje permutace $\pi \in S_n$ taková, že pro každé $x = (x_1, \dots, x_n) \in \Sigma^n$ platí $x \in C \Leftrightarrow \pi(x) \in (x_{\pi(1)}, \dots, x_{\pi(n)}) \in C'$
  - kódy se tedy liší jen permutací pozic (stejná permutace je použita na všechna kódová slova)
  - protože $d(x,y) = d(\pi(x), \pi(y))$, pak vidíme, že ekvivalentní kódy mají stejné parametry (existují ale neekvivalentní kódy se stejnými parametry)

- pro jaké volby parametrů n, k, d, q existují kódy?
  - **kombinatorická koule** o středu x a poloměru t v Σ^n je

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

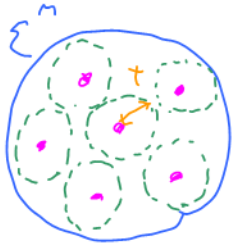


- **pozorování 1**:
  je-li C kód se vzdáleností $2t+1$, pak pro každé $x, y \in C$ platí $B(x,t) \cap B(y,t) = \emptyset$.
  (Δ-nerovnost, d je metrika)
  - **DK**:
    - sporem $\exists z \in B(x,t) \cap B(y,t)$ a $d(x,y) \le d(x,z) + d(z,y) \le 2t$
      $\Rightarrow$ spor s $d(x,y) \ge 2t+1$ ☒

- velikost $B(x,t)$, nebuli jejich **objem**, nezávisí na volbě x a je rovен $V(t) = |B(x,t)| = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$
  - $\binom{n}{i}$: volba pozic, které měníme
  - $(q-1)^i$: výběr odlišných symbolů na vybraných pozicích

- **Věta 1** (**Hammingův odhad**):
  pro každý kód C s parametry $(n, k, 2t+1)_q$ platí

$$|C| \le \frac{q^n}{V(t)}$$



- kódová slova

- **DK**:
  - pokrývání koulí
  - velikost Σ^n je q^n a platí $\Sigma^n \supseteq \bigcup_{x \in C} B(x,t)$
  - protože vzdálenost je $2t+1$, pak podle **pozorování 1** jsou kombinatorické koule $B(x,t), B(x',t)$ s $x, x' \in C, x \ne x'$ disjunktní
  - $\Rightarrow |C| \cdot |V(t)| \le |\Sigma^n|$ a tedy $|C| \le \frac{|\Sigma^n|}{|V(t)|} = \frac{q^n}{V(t)}$ ☒

(↳ $B(x,t) \cap B(x',t) = \emptyset$ pro $x, x' \in C$, $x \ne x'$ a $\Sigma^n \supseteq \bigcup_{x \in C} B(x,t)$)

- KÓD S PARAMETRY $(n,k,2t+1)_q$ SPLŇUJÍCÍ ROVNOST $|C| = \frac{q^n}{V(t)}$ SE NAZÝVAJÍ **PERFEKTNÍ**
  - KOMBINATORICKÉ KOULE POKRÝVAJÍ CELÉ Σ^n, TJ. KAŽDÉ SLOVO Z Σ^n LZE DEKÓDOVAT
  - MEZI TZV. **TRIVIÁLNÍ** PERFEKTNÍ KÓDY PATŘÍ NAPŘÍKLAD OPAKOVACÍ KÓD LICHÉ DÉLKY S $q=2$,
  - PŘÍKLAD NETRIVIÁLNÍHO PERFEKTNÍHO KÓDU SI UKÁŽEME PŘÍŠTĚ
- EXISTUJE ANALOGICKÝ DOLNÍ ODHAD K VĚTĚ 1
- **VĚTA 2** (**GILBERTŮV-VARSHAMOVŮV ODHAD**):
  Pro každé $n, d, q \in \mathbb{N}$ existuje kód C s parametry $(n, k, d)_q$ takový, že $k = \log_q(|C|)$
  $$|C| \geq \frac{q^n}{V(d-1)}$$
  - obecný odhad, není těsný vůči odhadu z věty 1

DK:
- stačí hladově odebírat kódová slova z Σ^n spolu se slovy ve vzdálenosti $\leq d-1$
- kódová slova jde odebírat po $\geq \frac{q^n}{V(d-1)}$ krocích, protože $|\Sigma^n| = q^n$ a odebírané množiny slov nanejvýš tvoří disjunktní kombinatorické koule o poloměru $d-1$ ☒

- **LINEÁRNÍ KÓDY**:
  - EXISTUJÍ KÓDY, VE KTERÝCH UMÍME KÓDOVAT A DEKÓDOVAT EFEKTIVNĚ
  - čili pro výstupní slovo $y \in \Sigma^n$ lze rychle najít x, které bylo odesláno
    - není potřeba procházet všechna x s $d(x,y) \leq d$
  - PŘIPRAVÍME SI TEORII PRO POPIS TAKOVÝCH KÓDŮ
  - POUŽIJEME SPECIÁLNÍ ABECEDU S VLASTNOSTMI Z LINEÁRNÍ ALGEBRY
  - **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 $[n, k, d]_q$

- Z LINEÁRNÍ ALGEBRY VÍME, ŽE VEKTOROVÝ PODPROSTOR $C \subseteq \mathbb{K}^n$ (5)
SPLŇUJE $|C| = |\mathbb{K}|^{\dim(C)} = q^k \Rightarrow k$ JE CELOČÍSELNÉ
($|\mathbb{K}| = |\Sigma| = q$)

- PŘÍKLADY LINEÁRNÍCH KÓDŮ:

1) OPAKOVACÍ KÓD JE LINEÁRNÍ NAD TĚLESEM $\mathbb{Z}_{q-1}$
- NAVÍC JE NA SKALÁRNÍ SOUČIN I SOUČET

2) CHARAKTERISTICKÉ VEKTORY KONEČNÝCH PROJEKTIVNÍCH ROVIN NETVOŘÍ LINEÁRNÍ KÓD (NAD $\mathbb{Z}_2$)

3) HADAMARDOVY KÓDY NEMUSÍ BÝT LINEÁRNÍ, ALE JE ZÍSKÁME SYLVESTROVOU KONSTRUKCÍ LINEÁRNÍCH

- PRÁCE VE VEKTOROVÉM PROSTORU NÁM USNADNÍ LÉPE POČÍTAT VZDÁLENOSTI - STAČÍ POČÍTAT VZDÁLENOSTI OD NULY

- $\forall x, y, z \in \mathbb{K}^n : d(x,y) = d(x+z, y+z) = d(x-y, 0)$

x A y JSOU STEJNÉ NA NĚJAKÉ POZICI $\Leftrightarrow x+z$ A $y+z$ JSOU NA TÉTO POZICI STEJNÉ

VOLÍM $z = -y$

$\Rightarrow$ MINIMÁLNÍ VZDÁLENOST d SE ROVNÁ $\min\{d(x-y,0) : x,y \in C, x \neq y\} = \min\{d(x,0) : x \in C, x \neq 0\}$

$\Rightarrow$ KE ZJIŠTĚNÍ d NENÍ TŘEBA ZKOUMAT VŠECHNY DVOJICE, STAČÍ POČÍTAT NENULOVÉ SLOŽKY KÓDOVÝCH SLOV