# Cvičení 7 (Kapitola 7.)
## Duální kód, Syndromové dekódování

### Duální kód

Def: skalární součin $\vec{u}, \vec{v} \in V(n,q)$ $\quad \underbrace{\vec{u}\cdot\vec{v}} = u_1v_1 + \dots + u_nv_n$, kde $\in GF(q)$

Věta: $\forall \vec{u}, \vec{v}$ a $\vec{w} \in V(n,q)$ a $\alpha, \beta \in GF(q)$ platí:
(i) $\vec{u}\cdot\vec{v} = \vec{v}\cdot\vec{u}$
(ii) $(\alpha\vec{u} + \beta\vec{v})\cdot\vec{w} = \alpha(\vec{u}\cdot\vec{w}) + \beta(\vec{v}\cdot\vec{w})$

Důkaz: sami jako cvič.

Def: Duální kód. Mějme $[n,k]$-kód $C$, duální kód $C^\perp$ je množina vektorů ve $V(n,q)$, které jsou ortogonální ke každému kódovému slovu $C$.

$$C^\perp = \{\vec{v} \in V(n,q) \mid \vec{v}\cdot\vec{u} = 0, \forall \vec{u} \in C\}$$

Věta: $\vec{v} \in C^\perp \Leftrightarrow \vec{v}\cdot G^T = \vec{0}$ Důkaz: viz přednáška

Věta: Je-li $C$ $[n,k]$-kód nad $GF(q)$, pak $C^\perp$ je lineární $[n, n-k]$-kód.

Důkaz: předn.

Příklady duálních kódů.

Věta: Pro každý $[n,k]$-kód $C$ platí: $(C^\perp)^\perp = C$.

### Kontrolní matice

Def: Kontrolní matice $H$ lineárního $[n,k]$-kódu $C$ je generující matice $C^\perp$.

Platí: $H$ je $(n-k)\times n$ matice taková, že $GH^T = O$ (nulová matice)

a $C = \{\vec{x} \in V(n,q) \mid \vec{x}\cdot H^T = \vec{0}\}$.

Tj. lineární $[n,k]$-kód je plně zadaný svou kontrolní maticí.
Řádky kontrolní matice udávají kontrolní součty, které musí splňovat každé slovo kódu $C$.

Věta: Je-li $G = [I_k | A]$ standardní tvar generující matice $[n,k]$-kódu $C$, pak kontrolní matice kódu $C$ je $H = [-A^T | I_{n-k}]$.
Tento tvar $H$ se nazývá „standardní tvar kontrolní matice".

Důkaz - předn.

**Def:** Mějme $H$ - kontrolní matici $[n, k]$-kódu $C$.
Pak pro kterýkoli vektor $\vec{y} \in V(n, q)$ nazýváme $1 \times (n-k)$ řádkový vektor $S(\vec{y}) = \vec{y} \cdot H^T$ SYNDROMEM vektoru $\vec{y}$.

**Vlastnosti:**
- Jsou-li $\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_{n-k}$ řádky $H$.
  $S(\vec{y}) = (\vec{y} \cdot \vec{h}_1, \vec{y} \cdot \vec{h}_2, \ldots, \vec{y} \cdot \vec{h}_{n-k})$
- $S(\vec{y}) = \vec{0} \iff \vec{y} \in C$

**Lemma:** $\vec{u}, \vec{v} \in$ stejnému kosetu kódu $C \iff S(\vec{u}) = S(\vec{v})$ !
(mají stejný syndrom)

**Důsl:** Existuje bijekce mezi kosety a syndromy.

Syndromová vyhledávací tabulka:

| syndromy $\vec{s}$ | reprezentanti $f(\vec{s})$ |
|---|---|
| vektory $1 \times n-k$ | vektory $1 \times n$ |

Dekódování pomocí syndromů:
Odeslané slovo $\vec{x}$, přijaté slovo $\vec{y}$

1.) Pro přijaté slovo vypočteme syndrom $S(\vec{y}) = \vec{y} \cdot H^T$
2.) Je-li $\vec{s} = S(\vec{y})$, najdeme $\vec{s}$ v prvním sloupci tabulky.
3.) Dekódujeme $\vec{y}$ jako $\vec{x} = \vec{y} - f(\vec{s})$ ← Příklady v přednášce a dále ve cvičení.

(Lybí „incomplete decoding" = neúplné dekódování
(viz další předn. asi?)

Př. 1. Je-li $E_n$ binární kód obsahující všechny vektory (slova) sudé váhy z $V(n,2)$ dokažte, že $E_n^\perp$ je binární opakovací kód délky $n$.

Víme, že $E_n$ je binární $(n, 2^{n-1}, 2)$-kód.

$E_n$ je také bin. lin. $[n, n-1, 2]$-kód.

Generující matice pro $E_n$ je např.

$$G = \left[\begin{array}{c|c} I_{n-1} & \begin{matrix}1\\1\\\vdots\\1\end{matrix} \end{array}\right]$$

Co víme o $C^\perp$
- obsahuje vektory v $V(n,q)$ ortogonální k $C$ (Def)
- vektory z $C^\perp$ jsou ortog. k řádkům $G_C$ (lemma)
- Je-li $C$ $[n,k]$-kód, je $C^\perp$ $[n, n-k]$-kód (věta)
- Platí: $(C^\perp)^\perp = C$.
- kontrolní matice $H$ kódu $C$ je generující matice duálního kódu $C^\perp$. (Def)

$E_n^\perp$ je $[n, 1]$-kód (věta o dimenzi duál. kódu)

Gener. matice je kontrolní matice pro $E_n$, která má st. tvar $H = [11\ldots1 \,|\, I_1] = [11\ldots1]$

rozměr $1 \times n$

↑ Gener. matice opak. kódu délky $n$.

kontr. součet pro vektory z $E_n$ je

$\forall \vec{x} \in E_n$ platí $x_1 + x_2 \ldots + x_n = 0$

$\vec{x} \cdot H^T = \vec{0}$ ← vektor o rozměru $n-k$

Př. (2.) Popište jednoduchou strategii (postup) detekování chyb lineárním kódem užitím syndromů.

Mějme $C$ $q$-ární lin. $[n, k]$-kód, s gener. maticí $G$ o rozměrech $k \times n$ a kontrolní maticí $H$ o rozm. $n-k \times n$.

Slepisnovo rozm. je tabulka o rozm. $q^{n-k} \times q^k$, kde první sloupec obsahuje $q^{n-k} - 1$ nenulových kosetů reprezentantů.

## Detekce chyb pomocí SR.

Odesláno slovo $\vec{x}$, přijato slovo $\vec{y}$. Pokud $\vec{y}$ není v prvním řádku SR, pak došlo k alespoň 1 chybě.
Tj. je třeba srovnat $\vec{y}$ se všemi $q^k$ vektory kódu $C$.

Co víme o syndromech:

- $S(\vec{y}) = \vec{y} \cdot H^T$ ← řádkový vektor rozměru $n-k$
- vektory ze stejného kosetu $[n,k]$-kódu mají stejný syndrom (bijekce mezi syndromy a reprezentanty kosetů)
- Místo SR lze sestavit menší Syndromovou vyhledávací tabulku a použít syndromové dekódování.

## Detekce chyb pomocí syndromů.

Odesláno slovo $\vec{x}$, přijato $\vec{y}$.
Vypočteme syndrom $S(\vec{y}) = \vec{y} \cdot H^T$.
Je-li $S(\vec{y}) = \vec{0}$, pak $\vec{y} \in C$ (nedošlo k chybě).
Je-li $S(\vec{y}) \neq \vec{0}$, pak $\vec{y} \notin C$ (je detekována chyba).
Stačí tedy spočítat $n-k$ skal. součinů $\vec{y} \cdot \vec{h}_1, \vec{y} \vec{h}_2, \dots, \vec{y} \vec{h}_{n-k}$ místo porovnávání $\vec{y}$ s $q^k$ vektory kódu $C$.

Př. (3.) Mějme binární lineární $[n,k]$-kód s kontrolní maticí $H$. Ukažte, že transponovaný syndrom přijatého slova je roven součtu sloupců $H$, které odpovídají pozicím s chybami.

$$S(\vec{y}) = \vec{y} \cdot H^T \iff S(\vec{y})^T = H \cdot \vec{y}^T$$

$\vec{x} = x_1, x_2, \dots, x_n$, $\vec{y} = x_1, \dots, x_i + 1, \dots, x_j + 1, \dots, x_n$

$\vec{y} = \vec{x} + \vec{e}$ ← sloupcové vektory

$$S(\vec{y})^T = H(\vec{x}^T + \vec{e}^T) = H \cdot \vec{x}^T + H\vec{e}^T = e_1 \cdot \vec{s}_1 + e_2 \cdot \vec{s}_2 + \dots + e_n \vec{s}_n$$

$\vec{x}^T$: $n-k \times n$, $n \times 1$, $n-k \times 1$

$S(\vec{y})^T = (\vec{y} \cdot H^T)^T = H \cdot \vec{y}^T$

$$= \sum_{i=1}^{n} e_i \cdot \vec{s}_i, \text{ kde } \vec{s}_i \text{ jsou sloupce } H.$$

(Lze využít při sestavování syndr. tabulky)

Př. (4.) Sestavte syndromovou vyhledávací tabulku pro perfektní binární lineární $[7,4,3]$-kód s generující maticí.

$$\left[\begin{array}{cccc|ccc} 1&0&0&0&1&1&1 \\ 0&1&0&0&1&1&0 \\ 0&0&1&0&1&0&1 \\ 0&0&0&1&0&1&1 \end{array}\right]$$

$I_4$ $A$

Použijte syn. tab. k dekódování vektorů

$0000011 = \vec{y}_1$
$1111111 = \vec{y}_2$
$1100110 = \vec{y}_3$
$1010101 = \vec{y}_4$

1. K sestavení syn. tab. potřebujeme znát reprezentanty kosetů a spočítat jejich syndromy.

- Protože $[7,4,3]$-kód je perfektní, jsou reprezentanty kosetů právě všechna slova váhy 1 z $V(7,2)$

Tabulka má rozměr $q^{n-k} \times 2 = 2^3 \times 2 = 8 \times 2$

- Pro výpočet syndromů potřebujeme kontrolní matici. Určíme její standardní tvar z matice generující

$$H = \left[\begin{array}{cccc|ccc} 1&1&1&0&1&0&0\\ 1&1&0&1&0&1&0\\ 1&0&1&1&0&0&1 \end{array}\right]$$

$-A^T$ $\quad$ $I_3$

sloupce $H$

| syndrom $\vec{s}$ $S(\vec{z})$ | rep. kosety $f(\vec{s})$ $\vec{z}$ | |
|---|---|---|
| 000 | 00....0 | |
| 111 | 1000000 | $\vec{e}_1$ |
| 110 | 0100000 | $\vec{e}_2$ |
| 101 | 0010000 | $\vec{e}_3$ |
| 011 | 0001000 | $\vec{e}_4$ |
| 100 | 0000100 | $\vec{e}_5$ |
| 010 | 0000010 | $\vec{e}_6$ |
| 001 | 0000001 | $\vec{e}_7$ |

$$S(\vec{z}) = \vec{z}\cdot H^T = (\vec{z}\vec{h}_1, \vec{z}\vec{h}_2, \vec{z}\vec{h}_3)$$

Dekód. vektorů

$$\begin{array}{l} \vec{y}_1\\ \vec{y}_2\\ \vec{y}_3\\ \vec{y}_4 \end{array}\left[\begin{array}{ccccccc} 0&0&0&0&0&1&1\\ 1&1&1&1&1&1&1\\ 1&1&0&0&1&1&0\\ 1&0&1&0&1&0&1 \end{array}\right] \cdot \underbrace{\left[\begin{array}{ccc} 1&1&1\\ 1&1&0\\ 1&0&1\\ 0&1&1\\ 1&0&0\\ 0&1&0\\ 0&0&1 \end{array}\right]}_{H^T} = \left[\begin{array}{ccc} 0&1&1\\ 0&0&0\\ 1&1&1\\ 1&1&1 \end{array}\right] \begin{array}{l} \leftarrow S(y_1)\\ \leftarrow S(y_2)\\ \leftarrow S(y_3)\\ \leftarrow S(y_4) \end{array}$$

$\Rightarrow$ dekód

$\vec{y}_1 \rightarrow \vec{x}_1 = \vec{y}_1 + \vec{e}_4 = 0001011$

$\vec{y}_2 \rightarrow \vec{x}_2 = \vec{y}_2$ je kód. slovo

$\vec{y}_3 \rightarrow \vec{x}_3 = \vec{y}_3 + \vec{e}_1 = 0100110$

$\vec{y}_4 \rightarrow \vec{x}_4 = \vec{y}_4 + \vec{e}_1 = 0010101$

Př. (5.) Mějme $C$ ternární lineární kód s gener. maticí

$$\left[\begin{array}{cccc} 1&1&1&0\\ 2&0&1&1 \end{array}\right]$$

a) Najděte standardní tvar gener. matice.

b) Najděte kontrolní matici kódu $C$ ve standardním tvaru.

c) Použijte syndromové dekódování k dekódování přijatých slov (vektorů) $\vec{y}_1 = 2121$, $\vec{y}_2 = 1201$, $y_3 = 2222$

Vyřešte sami.

Př. (6) Mějme lineární $[10,8]$-kód nad $GF(11)$ zadaný kontrolní maticí

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}.$$

1.) Najděte gener. matici ve st. tvaru

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix} + r_2 \sim \begin{bmatrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix} \begin{matrix} (-1) \\ (-1) \end{matrix} \sim$$

$$\begin{bmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix} -2r_1 \sim \begin{bmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 \end{bmatrix}$$

$$G = \left[\begin{array}{c:c} I_8 & \begin{matrix} 2 & 8 \\ 3 & 7 \\ 4 & 6 \\ 5 & 5 \\ 6 & 4 \\ 7 & 3 \\ 8 & 2 \\ 9 & 1 \end{matrix} \end{array}\right]$$

Dále uvažujme kód $C$, který vznikne z $[10,8]$-kódu odstraněním všech slov, která obsahují č. 10. Pak $C$ je 10-tkový kód, který není lineární. Sestává ze slov, která vyhovují kontrolním součtům $\sum_{i=1}^{10} x_i \equiv 0 \pmod{11}$ a $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$.

Dá se ukázat (P. Inkl. Exkl.), že $|C| = 82\,644\,629$

2.) Jak vypadají slova kódu?

$$C = \{(x_1, x_2, \ldots, x_8, 2x_1 + 3x_2 + \cdots + 9x_8, 8x_1 + 7x_2 + \cdots + 1x_8)\}$$

kde $x_1, \ldots, x_8$ jsou jakékoli hodnoty $0, 1, \ldots, 9, 10$

3.) Ukažte, že tento kód $C$ opraví kteroukoli 1 chybu a současně detekuje chybu vzniklou transpozicí dvou symbolů.

Popíšeme neúplné dekódování pomocí syndromů.

$\bar{x}$ ← odeslané slovo  $\bar{y}$ ← přijaté slovo

Syndrom $\bar{y} \cdot H^T = \left( \sum_{i=1}^{10} y_i , \sum_{i=1}^{10} i y_i \right) = (A, B)$

- Předpl., že došlo k 1 chybě, pak

$\bar{y} = y_1, y_2, \dots, y_{10} = x_1, \dots, x_j + k, \dots, x_{10}$

$A = \sum_{i=1}^{10} y_i = \sum_{i=1}^{10} x_i + k \equiv k \pmod{11}$ ($=A$) ← velikost chyby

$B = \sum_{i=1}^{10} i y_i = \sum_{i=1}^{10} i x_i + jk \equiv jk \pmod{11}$ ← $j = B \cdot A^{-1} \bmod 11$

($=B$) ← pozice chyby

$B \equiv j \cdot A \pmod{11}$

$\Rightarrow j = B \cdot A^{-1}$

- Dekódovací schema

(i) pro $S(\bar{y}) = (A, B) = (0, 0) \Rightarrow \bar{y} \in C$ předpokl., že k chybám nedošlo

(ii) pro $S(\bar{y}) = (A, B)$, $A \neq 0 \wedge B \neq 0 \Rightarrow$ Předpokl. že nastala jedna chyba a dekodujeme na $\bar{x}$, kdy od $\bar{y}$ odečteme $A$ na $B \cdot A^{-1}$ - pozici.

(iii) Je-li $A = 0$ nebo $B = 0$, ale ne obojí $\Rightarrow$ Nastalo více než 1 chyba $A = 0 \wedge B \neq 0$ odpovídá transpozici symbolů.

4.) Pomocí výše popsaného kódu a syndr. dekódování dekódujte slova $\bar{y}_1 = 0610271355$ a $y_2 = 0617960587$

$\bar{x}_2 = 0612960587$

Pro $\bar{y}_1$: $S(\bar{y}_1) = (A, B) = (8, 6)$

$A = 0+6+1+0+2+7+1+3+5+5 \equiv 8 \pmod{11}$

$B = 10 + 2 \cdot 6 + 3 \cdot 1 + 4 \cdot 0 + 5 \cdot 2 + 6 \cdot 7 + 7 \cdot 1 + 8 \cdot 3 + 9 \cdot 5 + 10 \cdot 5 \equiv 6 \pmod{11}$

$B \cdot A^{-1} = 6 \cdot 8^{-1} = 6 \cdot 7 \equiv 9 \pmod{11}$

$\bar{y}_1 = 0610271355$

$\bar{x} = 0610271385$

$5 - 8 \equiv 8 \pmod{11}$

Pro $\vec{y}_2$ : $S_{y_2} = (A, B) =$

$A = 0+6+1+7+9+6+0+5+8+7 \equiv 5 \pmod{11}$

$B = 0+2\cdot 6+3\cdot 1+4\cdot 7+5\cdot 9+6\cdot 6+7\cdot 0+8\cdot 5+9\cdot 8+10\cdot 7 \equiv 9 \pmod{11}$

$j = B\cdot A^{-1} = 9\cdot 5^{-1} \equiv 9\cdot 9 = 81 \equiv 4 \pmod{11}$

$X_2 = 0617960587 + (000-5000000) = 0612960587$