20SK – Signály a kódy

Přednáška 11 – Hammingovy a binární cyklické kódy (10.12.2018)

Probíraná témata:

- Perfektní kódy
- Hammingovy kódy jako perfektní kódy pro opravu jednoduché chyby: Definice, vlastnosti kontrolní a generující matice.
- Syndrom. Oprava chyby u Hammingova kódu.
- Příklady, konstrukce kódu z kontrolní matice, přímá konstrukce generující matice.

Relevantní literatura je [1, kapitoly 2 a 3], [2, kapitoly 5 a 10], [3, kapitoly 3 a 4] a [4, kapitoly III a V].

Seznam literatury

[1] Morelos-Zaragoza, R. H.: *The Art of Error-Correcting Coding*. 2nd edition, John Wiley & Sons, 2006, 263pp.

[2] Adámek, J: *Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory*. Wiley Interscience, 1991, 352 pp.

[3] Moon, T. K.: *Error Correction Coding – Mathematical Methods and Algorithms.* Wiley Interscience, 2005, 756 pp.

[4] Adámek, J: Kódování. Matematika pro vysoké školy technické, sešit XXXI. SNTL, 1989, 192 pp.

PERFEKTNÍ KÓDY

→ nejkratší možný kód pro danou konfiguraci
→ kódová slova jsou od sebe vždy stejně & minimálně možné vzdálená

Příklad: pro opravu jednoduché chyby $d(\vec{v}_i, \vec{v}_j) = 3$ vždy

Hammingova hranice pro (n,k) kód:

$$n \leq 2^{n-k} - 1$$

→ pokud splněno, opravuje jednoduché chyby

Př.: (7,4) kód (P)

$7 \leq 2^3 - 1 = 7$

→ nelze pro všechna k splnit rovnost

Př.: pro $k=2$

$n \leq 2^{n-2} - 1$

$3 \leq 2 - 1$ ✗

$4 \leq 4 - 1$ ✗

$5 \leq 8 - 1 = 7$ ✓

není 'perfektní'!
musíš přidat další 2 bity informace

Př.: (3,1) kód (P) perfektní

$n = 3$
$n - k = 2$

$3 \leq 2^2 - 1 = 3$ ✓

→ platí, opravuje jednoduché chyby

(4,3)-kód

$4 \leq 2 - 1$

→ neplatí, neopravuje!

Př: (7,4) kód

$7 \le 2^3 - 1 = 7$ (P)

→ nelze pro všechna k splnit rovnost

Př. pro $k=2$

$n \le 2^{n-2} - 1$

$3 \le 2-1$ ×

$4 \le 4-1$ ×

$5 \le 8-1 = 7$ ✓

není perfektní!
můžu přidat další 2 bity! informace

PERFEKTNÍ KÓDY

↳ platí $n = 2^{n-k} - 1$

(3,1), (5,2), (6,3), (7,4), ... → perfektní

Hammingův kód

$n = 2^m - 1$ $m = 2, 3, \dots$

$k = 2^m - m - 1$ → (3,1), (7,4), (15,11), ...

$d_{min} = 3$

Př: 7,4

H je 3×7:

$$\begin{bmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{bmatrix} = H$$

↓ ↓ ↓ ↓
1 2 6 7

Př:

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$ opak. kód délky 3 (3,1)

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$ $m = n-k$

n

(7,4)

(nesystematický)

$$H_{sys} = \left(\begin{array}{ccc:ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

HAMMINGOVY KÓDY

- perfektní kód pro opravu jedné chyby
- pro m zabezpečovacích bitů

$$n = 2^m - 1$$

$$k = 2^m - m - 1$$

$$d = 3$$

Definice: Binární kód $\mathbb{K}$ opravuje jednoduché chyby tehdy a jen tehdy, pokud jeho kontrolní matice H má nenulové a vzájemně odlišné sloupce

Návrh: H konstruujeme výčtem binárních reprezentací čísel $1 \dots n$ ve sloupcích

$$\vec{v} = \vec{u} \cdot G_{sys}$$

$$\rightarrow \left[\begin{array}{c:c} \mathbb{I}_{kxk} & \mathbb{P}_{kx(n-k)} \end{array}\right]$$

Př:

$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ opak. kód délky 3 (3,1)

$H = \begin{pmatrix} 0001111 \\ 0110011 \\ 1010101 \end{pmatrix}$ $\left.\vphantom{\begin{pmatrix} 0001111 \\ 0110011 \\ 1010101 \end{pmatrix}}\right\}$ $m = n-k$

n (7,4)

(nesystematický)

$H_{sys} = \left(\begin{array}{ccc:ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$

$\vec{v} \cdot H^T = \vec{0}$

↳ z H_{sys} vyjde:

$v_1 \oplus v_2 \oplus v_3 \oplus v_4 = 0$
$v_0 \oplus v_2 \oplus v_3 \oplus v_5 = 0$
$v_0 \oplus v_1 \oplus v_3 \oplus v_6 = 0$

$\Rightarrow$

$v_1 \oplus v_2 \oplus v_3 = v_4$ (4 inf. znaky)
$v_0 \oplus v_2 \oplus v_3 = v_5$
$v_0 \oplus v_1 \oplus v_3 = v_6$ (3 kontrolní)

Kódování: $u_0 \to v_0$; $u_1 \to v_1$; $u_2 \to v_2$; $u_3 \to v_3$

v_4, v_5, v_6 ... dopočítám

→ z toho sestavím generující matici G

$\vec{v} = \vec{u} \cdot G$

Dekódování:

Přijmu $\vec{w}$ a spočtu

$\vec{w} \cdot H^T$ — $\vec{0}$ ... kód. slovo
$\neq \vec{0}$ ... chyba

$\vec{w} = \vec{v} + \vec{e}$ → obsahuje pouze 1 bit hodnoty 1

$\vec{w} \cdot H^T = (\vec{v} + \vec{e}) H^T =$

$= \underbrace{\vec{v} \cdot H^T}_{0} + \underbrace{\vec{e} \cdot H^T}_{\text{syndrom}} =$

(kopie sloupce v H, kde nastala chyba)

Př. (7,4) Hamming

G_{sys} z rovnic:

zde rovnice →

$$G_{sys} = \left(\begin{array}{cccc|ccc} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{array}\right)$$

$v_4 = v_1 \oplus v_2 \oplus v_3 = u_1 \oplus u_2 \oplus u_3$

$v_5 = u_0 \oplus u_2 \oplus u_3$

$v_6 = u_0 \oplus u_1 \oplus u_3$

$$H_{sys} = \begin{pmatrix} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{pmatrix}$$

$\vec{u} = (0101)$

$(0101)\begin{pmatrix}0\\1\\1\\1\end{pmatrix}$ $(0101)\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$

$\vec{v} = \vec{u} \cdot G_{sys} = (0101) \cdot (\dots) = (0101010)$

$$H \cdot \vec{v} = \vec{v} \cdot H^T = (e_0, e_1, e_2)$$

$$\begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \\ 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix} = H^T$$

$$G_{sys} = \left(\begin{array}{c|ccc} & 0&1&1 \\ I_{4\times4} & 1&0&1 \\ & 1&1&0 \\ & 1&1&1 \end{array}\right) \Rightarrow$$

$$P = \begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix} \Rightarrow P^T = \begin{pmatrix} 0&1&1&1 \\ 1&0&1&1 \\ 1&1&0&1 \end{pmatrix}$$

$$H_{sys} = \left(\begin{array}{cccc|ccc} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{array}\right)$$

$$e_0 = \underbrace{(0101010)}_{\vec{v}} \cdot \begin{pmatrix}0\\1\\1\\1\\1\\0\\0\end{pmatrix} = 0$$

$$e_1 = (0101010) \cdot \begin{pmatrix}1\\0\\1\\1\\0\\1\\0\end{pmatrix} = 0$$

$$e_2 = (0101010) \cdot \begin{pmatrix}1\\1\\0\\1\\0\\0\\1\end{pmatrix} = 0$$

Př. (7,4) Hamming

G_{SRS} z rovnic:

zde rovnice →

$$G_{SRS} = \left(\begin{array}{cccc:ccc} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{array}\right)$$

$v_4 = v_1 \oplus v_2 \oplus v_3 = u_1 \oplus u_2 \oplus u_3$

$v_5 = u_0 \oplus u_2 \oplus u_3$

$v_6 = u_0 \oplus u_1 \oplus u_3$

Př.: chyba při přenosu:

$\vec{v} = (0101010) \rightarrow \vec{w} = (0100010)$

$\vec{w} \cdot H^T = (0100010) \cdot H^T = (1\ 1\ 1)$

→ musím opravit pozici, na níž je v H_{SRS} sloupec $\begin{pmatrix}1\\1\\1\end{pmatrix}$

→ 4. sloupec

$\rightarrow \vec{v} \Rightarrow (0101010)$

$$\begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \\ \hline 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix} = H$$

možno

$$H = \begin{pmatrix} 0&0 & & 1 \\ 0&1 & \cdots & 1 \\ 1&0 & & 1 \end{pmatrix}$$

Poznámka: H_{SRS} je pro opravy méně vhodná, než H

u H označuje syndrom součet → index chybového bitu