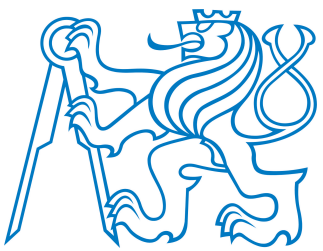
Hammingův kód

Vladislav Kosejk

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská
Detašované pracoviště Děčín



Obsah prezentace

- Richard Wesley Hamming
- Hammingův kód
  1. Algoritmus Hammingova kódu
  2. Generující matice
  3. Kontrolní matice
- Hamingův rozšířený kód
  1. Algoritmus Hammingova rozšířeneho kódu
  2. Generující matice
  3. Kontrolní matice

Životopis

- Narozen v Chicagu, 11. února 1915
- Americký matematik, jehož práce značně ovlivnila informatiku a telekomunikace. Jeho příspěvky zahrnují Hammingův kód, Hammingova okna (digitální filtry schopné odstarnit šum z řeči), Hammingovu síť
- Obdržel bakalářský titul z Univerzity v Chicagu v roce 1937 a magisterský titul na univerzitě v Nebrasce v roce 1939 a nakonec Ph.D. na univerzitě v Illinois v roce 1942. Byl profesorem na univerzitě v Louisville v průběhu druhé světové války, pracoval na projektu Manhattan v roce 1945, programoval jeden z prvních digitálních počítačů, které byly potřeba pro řešení fyzikálních rovnic.
- Získal mnoho vyznamenání, Turingovo ocenění od Asociace pro výpočetní stroje v 1968.

Hammingův kód

- Binární kód se nazývá Hammingův, jestliže má kontrolní matici, jejíž sloupce jsou všechna nenulová slova dané délky $n - k = r$ a žádné z nich se neopakuje. Jedná se o speciální případ lineárních binárních (n, k) kódů. Tyto kódy opravují jednu chybu a objevují dvojnásobné chyby při minimální vzdálenosti kódu $\mu(K) = 3$

Algoritmus Hammingova kódu

- Všechny bitové pozice, jejichž hodnota je rovná mocnině 2, jsou použity pro paritní bit (1, 2, 4, 8, 16, 32, . . .).
- Ostatní bitové pozice náleží kódovanému informačnímu slovu (3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, . . .).
- Každý paritní bit je vypočítán z některých bitů informačního slova. Pozice paritního bitu udává sekvenci bitů, které jsou v kódovém slově zkontrolovány a které přeskočeny.
  1. Pro paritní bit p_1 (pozice 1) se ve zbylém kódovém slově 1 bit přeskočí, 1 zkontroluje, 1 bit přeskočí, 1 zkontroluje, atd.
  2. Pro paritní bit p_2 (pozice 2) se přeskočí první bit, 2 zkontrolují, 2 přeskočí, 2 zkontrolují, atd.
  3. Pro p_3 (pozice 4) se přeskočí první 3 bity, 4 zkontrolují, 4 přeskočí, 4 zkontrolují, atd.

Hammingův kód (7,4)

- Generující matice $\mathbb{G}_H$ Hammingova kódu (7,4)

$$\mathbb{G}_H = \begin{pmatrix} p_{11} & p_{21} & 1 & p_{31} & 0 & 0 & 0 \\ p_{12} & p_{22} & 0 & p_{32} & 1 & 0 & 0 \\ p_{13} & p_{23} & 0 & p_{33} & 0 & 1 & 0 \\ p_{14} & p_{24} & 0 & p_{34} & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Hammingův kód (7,4)

- Generující matice $\mathbb{G}_H$ Hammingova kódu (7,4)

$$\mathbb{G}_H = \begin{pmatrix} p_{11} & p_{21} & 1 & p_{31} & 0 & 0 & 0 \\ p_{12} & p_{22} & 0 & p_{32} & 1 & 0 & 0 \\ p_{13} & p_{23} & 0 & p_{33} & 0 & 1 & 0 \\ p_{14} & p_{24} & 0 & p_{34} & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

- Kontrolní matice Hammingova kódu (7,4) se určí tak, aby platila soustava rovnic, která byla použita při sestavování generující matice.

$$\begin{aligned} s_1 &= b_4 \oplus b_5 \oplus b_6 \oplus b_7 \\ s_2 &= b_2 \oplus b_3 \oplus b_6 \oplus b_7 \\ s_3 &= b_1 \oplus b_3 \oplus b_5 \oplus b_7 \end{aligned} \Rightarrow \mathbb{H}_H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Dekódování a kontrola

- Nejprve se po přijetí kódového slova $\overline{b}$ určí syndrom $\overline{s} = \mathbb{H}_H \cdot \overline{b}^T$
- Například pro přijaté slovo $\overline{b} = (1010111)$ je syndrom

$$\mathbb{H}_H \cdot \overline{b}^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Dekódování a kontrola

- Nejprve se po přijetí kódového slova $\overline{b}$ určí syndrom $\overline{s} = \mathbb{H}_H \cdot \overline{b}^T$
- Například pro přijaté slovo $\overline{b} = (1010111)$ je syndrom

$$\mathbb{H}_H \cdot \overline{b}^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

- Vidíme, že syndrom $\overline{s}$ je nenulový, tj. při přenosu došlo k chybě. Syndrom, který vyšel $\overline{s} = (1, 1, 0)$ odpovídá sloupci 6 kontrolní matice $\mathbb{H}_H$ a z toho vyplývá, že je třeba opravit šestý bit přijatého slova na kódové slovo $\overline{b}' = (1010101)$.

Algoritmus rozšířeného Hammingova kódu (8,4)

- Rozšíření Hammingova binárního kódu vychází z toho, že přidáme na začátek každého kódového slova nový symbol určený pro kontrolu parity celého kódového slova. Bit p_0 je zvolen tak, aby $p_0 \oplus b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_5 \oplus b_6 \oplus b_7$ vycházelo nula. Rozšířený kód dovoluje, tak jako předchozí, opravit jednu chybu a navíc je schopen detekovat tři chyby, protože minimální vzdálenost kódu je $\mu(K) = 4$

Algoritmus rozšířeného Hammingova kódu (8,4)

- Rozšíření Hammingova binárního kódu vychází z toho, že přidáme na začátek každého kódového slova nový symbol určený pro kontrolu parity celého kódového slova. Bit p_0 je zvolen tak, aby $p_0 \oplus b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_5 \oplus b_6 \oplus b_7$ vycházelo nula. Rozšířený kód dovoluje, tak jako předchozí, opravit jednu chybu a navíc je schopen detekovat tři chyby, protože minimální vzdálenost kódu je $\mu(K) = 4$
- Generující matice Hammingova kódu (8,4)

$$\mathbb{G}_H = \begin{pmatrix} p_{01} & p_{11} & p_{21} & 1 & p_{31} & 0 & 0 & 0 \\ p_{01} & p_{12} & p_{22} & 0 & p_{32} & 1 & 0 & 0 \\ p_{01} & p_{13} & p_{23} & 0 & p_{33} & 0 & 1 & 0 \\ p_{01} & p_{14} & p_{24} & 0 & p_{34} & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Literatura


Ing.Radomil Matoušek,Ph.D.
Metody kódování
VUT Brno, 2006.


Sharon Heumann.
http://www.mdstud.chalmers.se/ md7sharo/coding/main/node32.html