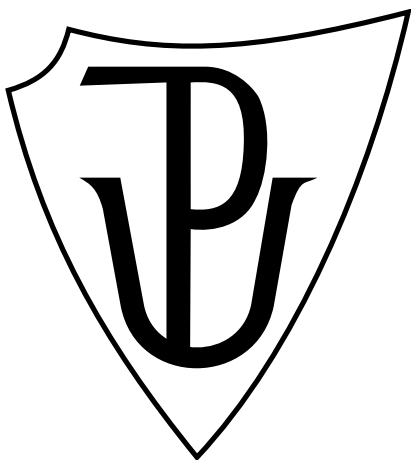
Teorie informace a kódování (KMI/TIK)

Binární lineární kódy



Lukáš Havrlant

Univerzita Palackého

20. listopadu 2012

Lineární kódy

- Základní myšlenka: ke kódové abecedě B přidáme algebraické operace $+$ a $\cdot$ tak, abychom z B dostali těleso a z B^n vektorový prostor.

- Kódy potom můžeme popsat rovnicemi.

Binární lineární kódy na $Z_2 = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

a

$\cdot$	0	1
0	0	0
1	0	1

- 0 je neutrální vzhledem k $+$, máme tak inverzní prvky vzhledem k $+$: $0 + 0 = 0$, takže $0 = -0$ a $1 + 1 = 0$, takže $1 = -1$.
- Slova můžeme vidět jako vektory: $1101 = \langle 1, 1, 0, 1 \rangle$
- Skalární násobení: $a \cdot \langle u_1, \ldots, u_n \rangle = \langle a \cdot u_1, \ldots, a \cdot u_n \rangle, a \in Z_2$.
- Sčítání: $\langle u_1, \ldots, u_n \rangle + \langle v_1, \ldots, v_n \rangle = \langle u_1 + v_1, \ldots, u_n + v_n \rangle$.

Kódy jako rovnice

- Důležité kódy jsme schopni popsat rovnicemi:
- Pro slovo x délky n u kódu kontroly sudé parity

$$x_1 + x_2 + \cdots + x_n = 0$$

- Řešením této rovnice jsou všechna kódová slova.
- Opakovací kód $C_n = \{a^n \mid a \in Z_2\}$, např. $C_3 = \{000, 111\}$.

$$\begin{aligned} x_1 + x_n &= 0 \\ &\cdots \\ x_{n-1} + x_n &= 0 \end{aligned}$$

Vektorový podprostor

- Opakování: nechť V je vektorový prostor na množině K. Pak $C \subset V$ je vektorový podprostor, pokud:
  - $\forall u, v \in C : \quad u + v \in C$
  - $\forall a \in K, u \in C : \quad a \cdot u \in C$
- Množina všech řešení systému homogenních rovnic tvoří vektorový podprostor.
- Tj. Z_2^n tvoří vektorový prostor, množina řešení C tvoří vektorový podprostor.

Binární lineární blokové kódy

Definice: Binární blokový kód C se nazývá lineární, pokud $\forall u, v \in C$ platí $u + v \in C$.

- V našem případě: $V = \{0,1\}^n, K = \{0,1\}$
- Proč tam nemusí být podmínka $\forall a \in K, u \in C : \quad a \cdot u \in C$?
- Protože $1 \cdot u = u$ a $0 \cdot u = \mathbf{0} \longrightarrow$ potřebujeme, aby C obsahovalo nulový vektor. Ten obsahuje, protože $u + u = \mathbf{0}$.

Lemma: Pro $n \in \mathbb{N}$, množina C všech řešení homogenního systému rovnic na množině Z_2 je vektorový podprostor Z_2^n. Tedy C je lineární blokový kód.

- Důsledek: pokud popíšeme blokový kód homogenním systémem rovnic, je tento kód lineární.

- Je kód dva-z-pěti lineární? (Pro připomenutí: délka 5, obsahuje vždy dvě 1: 00011, 01010, atd.)

Chybové slovo, Hammingova váha

Definice: Pokud pošleme slovo u a přijmeme slovo v, pak slovo e, které má 1 na pozicích, na kterých se u od v liší, se nazývá *chybové slovo*.

Přitom platí: $v = u + e$ a také $e = v - u\,(= v + u)$.

Definice: *Hammingova váha* slova u je rovna počtu symbolů v u, které se liší od 0.

Definice: *Minimální váha* netriviálního kódu C je nejmenší Hammingova váha slova z C kromě nulového slova.

Vztah minimální váhy a minimální vzdálenosti kódu

Věta: Minimální váha netriviálního kódu C je rovna $d(C)$.

Důkaz: Směr min_weight(C) $\geq d(C)$: Nechť c je minimální váha C. Nechť u je slovo s váhou c. Zřejmě $c = \delta(u, 0 \ldots 0) \geq d(C)$.

Směr min_weight(C) $\leq d(C)$: Nechť $d(C) = \delta(u, v)$ pro nějaká $u, v \in C$. Pak jistě také $u + v \in C$. Přitom Hammingova váha $u + v$ je rovna $\delta(u, v)$, protože $u + v$ má 1 na těch pozicích, na kterých se slova u, v liší. Tedy min_weight(C) $\leq d(C)$.

Celkově tak máme $d(C) =$ min_weight(C).

Kontrolní matice kódu

Definice: Kontrolní matice binárního blokového kódu C o délce n je binární matice H taková, že pro všechny $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ máme

$$H \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

právě tehdy, když $x \in C$.

Matice H je kontrolní maticí kódu C, pokud platí:

$$C = \{x \in \{0,1\}^n \mid Hx^T = \mathbf{0}^T\}$$

Příklady kontrolních matic

- Pokud jsou řádky kontrolní matice nezávislé, H je $n-k \times n$ matice. Kód pak má $n-k$ kontrolních symbolů a n celkových.
- Kontrolní matice kódu kontroly sudé parity o délce n je matice $1 \times n$:

$$H = (1 \ldots 1)$$

- Kontrolní matice pro opakovací kód délky 5 je matice 4×5:

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

Věta o kontrolní matici I

Věta: Pokud binární kód C opravuje jednoduché chyby, pak kontrolní matice kódu C má nenulové a navzájem různé sloupce.

Důkaz: Pokud C opravuje jednoduché chyby, pak $d(C) > 2$ a minimální váha je také > 2. Nechť H je kontrolní matice pro C. Nechť vektor $b^i \in \{0,1\}^n$ má 1 právě na pozici i. Nechť vektor $b^{i,j} \in \{0,1\}^n$ má 1 právě na pozicích i a j. Pokud by matice H měla i-tý sloupec nulový, pak $Hb^{i^T} = \mathbf{0}^T$. Ale b^i je přitom slovo s Hammingovou váhou 1, což je spor s tím, že minimální váha kódu C je > 2.

Pokud by H měla stejné sloupce i a j, pak $Hb^{i,j^T} = \mathbf{0}^T$. ($Hb^{i,j^T}$ je součet sloupců i a j). Nicméně $b^{i,j}$ je slovo s váhou 2, což je opět spor s tím, že minimální vzdálenost kódu C je > 2. □

Věta o kontrolní matici II

Věta: Každá binární matice s nenulovými a navzájem různými sloupci je kontrolní matice binárního lineárního kódu, který opravuje jednoduché chyby.

Důkaz: Nechť H je matice, která má nenulové a navzájem různé sloupce. Z předchozího slajdu je zřejmé, že žádné slovo b^i a $b^{i,j}$ není kódovým slovem, tedy minimální váha a tím i minimální vzdálenost kódu je > 2. $\square$

Příklad

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

. . . je kontrolní matice binárního lineárního kódu. Přepíšeme do rovnic:

$$\begin{aligned} (0x_1 + 0x_2 &= 0) \\ x_2 &= 0 \\ x_1 + x_2 &= 0 \end{aligned}$$

Systém má jediné, nulové řešení. Systém tak generuje kód $C = \{00\}$.

Přidáme sloupec. . .

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

Systém má opět jediné, nulové řešení, takže $C = \{000\}$.

Přidáme ještě jeden sloupec...

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

- Kódová slova mají délku 4. Jak vypadá C?
- Jak by vypadalo C, kdybychom prohodili poslední dva sloupce?
- Přidáním dalších sloupců zvyšujeme počet informačních symbolů.
- Kolik sloupců může matice nejvýše mít?
- Takový kód opravuje právě jednu chybu. Proč ne dvě?

Kód opravuje jednu chybu

Aby opravoval dvě chyby, musel by mít kód C minimální váhu > 4. Tedy matice musí mít > 4 sloupce. Ovšem pokud má 3 řádky, pak jistě existují tři nebo čtyři sloupce, jejichž součet je nulový sloupec.

Vezmeme libovolné čtyři sloupce i, j, k, l. Protože matice má 3 řádky, hodnost je maximálně 3, tak určitě alespoň jeden ze sloupců je lineárně závislý. Nechť i-tý sloupec je lineárně závislý, tj. $H_i = a_j \cdot H_j + a_k \cdot H_k + a_l \cdot H_l$. Dva nebo tři koeficienty musí být rovné 1 – řekněme, že buď a_j, a_k, nebo a_j, a_k, a_l. Pak součet sloupců i, j, k nebo sloupců i, j, k, l je roven nulovému sloupci.

Což znamená, že pro vektor u s 1 na pozicích i, j, k nebo i, j, k, l platí $Hu^T = \mathbf{0}^T$, tedy u je kódové slovo. Ale váha u je tři, nebo čtyři, stejně tak minimální váha (a tím pádem i vzdálenost) kódu.

Hammingovy kódy

- Perfektní kódy pro opravu jednoduchých chyb.
- Kódová slova mají délku $n = 2^m - 1$, m symbolů je kontrolních. Minimální vzdálenost je 3.
- Nazývají se $(2^m - 1, 2^m - m - 1)$ kódy, např. $(7, 4)$.
- Sloupce kontrolní matice jsou všechny nenulové vektory seřazené lexikograficky (= podle hodnot, pokud bychom je převedli na číslo v desítkové soustavě). Pro $m = 2$:

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

Definice Hammingova kódu

Definice: Hammingův kód je binární lineární kód, který má, pro nějaké m, $m \times 2^m - 1$ kontrolní matici, jejíž sloupce obsahují všechny nenulové binární vektory.

Příklad kontrolní matice (jedné z mnoha) pro $m = 3$. Dostáváme matici 3×7:

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

Zakódování

Předchozí matici můžeme přepsat na tento systém rovnic:

$$\begin{aligned} x_4 + x_5 + x_6 + x_7 &= 0 \\ x_2 + x_3 + x_6 + x_7 &= 0 \\ x_1 + x_3 + x_5 + x_7 &= 0 \end{aligned}$$

A to můžeme přepsat na:

$$\begin{aligned} x_5 &= x_2 + x_3 + x_4 \\ x_6 &= x_1 + x_3 + x_4 \\ x_7 &= x_1 + x_2 + x_4 \end{aligned}$$

Vidíme, že x_1, x_2, x_3, x_4 můžeme brát jako informační symboly a x_5, x_6, x_7 jako kontrolní, které dopočítáme.

Dekódování

- Pokud je u kódové slovo, pak $Hu^T = \mathbf{0}^T$.
- Pokud nastane chyba na pozici i, přijmeme slovo $v = u + e^i$.

$$Hv^T = H(u + e^i)^T = Hu^T + He^{iT} = \mathbf{0}^T + He^{iT} = He^{iT} = H_i$$

- Součin Hv^T je tak rovný i-tému sloupci matice H.
- V i-tém sloupci je uloženo číslo i v binární podobě.
- $\longrightarrow$ opravíme i-tý znak ve slově v.

Informační poměr

- Informační poměr Hammingova kódu je $R(C) = \frac{2^m - m - 1}{2^m - 1} = 1 - \frac{m}{2^m - 1} \longrightarrow$ malá redundance pro velká m.
- Vždy jsme ale schopni opravit jen jednu chybu.
- Hammingovy kódy jsou perfektní, protože mají nejmenší možnou redundanci na množině kódů opravující jednoduché chyby.
- Každé slovo délky $n = 2^m - 1$ je buď kódové, nebo je od kódového slova vzdáleno o jedna.
- (Během dekódování buď získáme kódové slovo, nebo nám stačí změnit jeden bit.)