

Teorie informace a kódování (KMI/TIK)

Lineární kódy



Lukáš Havrlant

Univerzita Palackého

4. prosince 2013

Grupa

- Grupa je algebraická struktura $\mathbf{G} = \langle G, + \rangle$, kde $+$ je binární operace na G splňující:
 - $\forall x, y, z \in G : x + (y + z) = (x + y) + z$ (asociativita)
 - Existuje prvek $0 \in G$ takový, že $\forall x \in G : x + 0 = 0 + x = x$ (neutrální prvek)
 - $\forall x \in G$ existuje $y \in G$ takový, že $x + y = y + x = 0$ (inverzní prvek)
- Pokud navíc $\forall x, y \in G : x + y = y + x$, pak mluvíme o komutativní grupě.
- Příklad: $\mathbb{Z}$ a $\mathbb{R}$ s klasickým sčítáním, $\mathbb{Z}_p = \{0, \dots, p-1\}$ s násobením modulo p .

Těleso

- Těleso je algebraická struktura $\mathbf{F} = \langle F, +, \cdot, 0, 1 \rangle$, kde $+$ a $\cdot$ jsou binární operace na F splňující:
 - $\langle F, +, 0 \rangle$ je komutativní grupa,
 - $\langle F \setminus \{0\}, \cdot, 1 \rangle$ je komutativní* grupa,
 - $\forall x, y, z \in G : x \cdot (y + z) = x \cdot y + x \cdot z$ (distributivita).
- Důsledky pro $x, y, z \in F$:
 - $x \cdot 1 = x$, $xy = xz$ implikuje $y = z$.
 - $x + y \in F$ a $xy \in F$. Pokud $x \neq 0, y \neq 0$, pak $xy \neq 0$.
 - Každý prvek x má opačný prvek $-x$ takový, že $x - x = 0$.
 - Každý prvek $x \neq 0$ má inverzní prvek x^{-1} takový, že $xx^{-1} = 1$.
- Příklady: $\mathbb{R}$ s klasickým sčítáním a násobením, $\mathbb{Z}_p$ modulo p , pokud je p prvočíslo.

Vektorový prostor

Definice: Nechť $\mathbf{F} = \langle F, +, \cdot, 0, 1 \rangle$ je těleso. Vektorový prostor na $\mathbf{F}$ je struktura $\mathbf{V}$ obsahující neprázdnou množinu vektorů V , binární operaci $+: V \times V \rightarrow V$ a binární operaci $\cdot: F \times V \rightarrow V$ takové, že $\forall a, b \in F, \mathbf{u}, \mathbf{v} \in V$:

- $\langle V, + \rangle$ je komutativní grupa,
- $(ab)\mathbf{v} = a(b\mathbf{v}),$
- $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v},$
- $1\mathbf{u} = \mathbf{u}.$

Příklad vektorového prostoru

- Nechť F je těleso. Pak množina $F^n = \{\langle a_1, \dots, a_n \rangle \mid a_i \in F\}$, kde sčítání $+$ vektorů a násobení $\cdot$ vektoru je definováno klasicky, tvoří vektorový prostor.
- $\mathbb{R}, \mathbb{Z}_p, \dots$
- Pro $p = 2$ dostáváme u $\mathbb{Z}_p$ vektorový prostor, který jsme použili u binárních lineárních kódů.

Vektorový podprostor

- Nechť V je vektorový prostor na tělese F . Pak $\emptyset \neq U \subseteq V$ s operacemi $+$ a $\cdot$ nazveme vektorový podprostor, pokud platí $\forall \mathbf{u}, \mathbf{v} \in U, a \in F$:
 - $\mathbf{u} + \mathbf{v} \in U$,
 - $a\mathbf{u} \in U$.
- Příklad: Pro těleso F , množina $\{\langle 0, a_2, \dots, a_n \rangle \mid a_i \in F\}$ je vektorový podprostor prostoru F^n .
- $\{\mathbf{0}\}$ je triviální vektorový podprostor.

Lineární kombinace

- Lineární kombinace vektorů $\mathbf{u}_1, \dots, \mathbf{u}_n \in V$ je vektor $a_1\mathbf{u}_1 + \dots + a_n\mathbf{u}_n$, kde $a_1, \dots, a_n \in F$.
- Pokud máme danou množinu vektorů $\mathbf{u}_1, \dots, \mathbf{u}_n \in V$, pak množina všech lineárních kombinací těchto vektorů tvoří vektorový podprostor prostoru V .
- Tento podprostor značíme $\text{obal}(\{\mathbf{u}_1, \dots, \mathbf{u}_n\})$.
- $\text{obal}(\{\mathbf{u}_1, \dots, \mathbf{u}_n\})$ je nejmenší podprostor obsahující vektory $\mathbf{u}_1, \dots, \mathbf{u}_n$.

Nezávislosti vektorů, báze, dimenze

- Množina vektorů $U \subseteq V$ se nazývá lineárně nezávislá, pokud žádný vektor $\mathbf{u} \in U$ není lineární kombinací $U \setminus \{\mathbf{u}\}$.
- Báze prostoru V je lineárně nezávislá množina $U \subseteq V$, pro kterou platí $\text{obal}(U) = V$.
- Pokud je U báze prostoru V , pak má prostor V dimenzi $|U|$.
- Pokud $U = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ je báze prostoru V , pak pro každé $\mathbf{u} \in V$ existují unikátní skaláry $a_1, \dots, a_n \in F$ tak, že $\mathbf{u} = a_1\mathbf{e}_1 + \dots + a_n\mathbf{e}_n$.
- Pokud $|F| = r$, pak každý k -rozměrný vektorový prostor na F má r^k prvků.

Lineární kódy

Definice: Nechť F je konečné těleso. Pak lineární (n, k) kód je k -dimenzionální vektorový (lineární) podprostor prostoru F^n .

- Lineární (n, k) kód má k informačních symbolů a $n - k$ kontrolních.
- Nechť C je lineární (n, k) kód. Pak má bázi $\mathbf{e}_1, \dots, \mathbf{e}_k$.
- Každé slovo $\mathbf{v} \in C$ lze vyjádřit jako lineární kombinace vektorů báze: $\mathbf{v} = \sum_{i=1}^k u_i \mathbf{e}_i$. Koeficienty $u_i \in F$ tvoří slovo $\mathbf{u}$ délky k .
- A naopak: každé slovo $\mathbf{u}$ délky k definuje kódové slovo $\mathbf{v}$:

$$\mathbf{v} = \sum_{i=1}^k u_i \mathbf{e}_i$$

Příklad

Báze kódu sudé parity délky 4:

$$\mathbf{e}_1 = 1100, \quad \mathbf{e}_2 = 1010, \quad \mathbf{e}_3 = 1001$$

Slovo $\mathbf{v} = 0011$ vyjádříme jako

$$\mathbf{v} = 0 \cdot 1100 + 1 \cdot 1010 + 1 \cdot 1001, \quad (\mathbf{u} = 011)$$

Slovo $\mathbf{v} = 1010$ jako

$$\mathbf{v} = 0 \cdot 1100 + 1 \cdot 1010 + 0 \cdot 1001, \quad (\mathbf{u} = 010)$$

Generující matice

Definice:

Pokud je C lineární kód s bází $\mathbf{e}_1, \dots, \mathbf{e}_k$, pak matice G typu $k \times n$ a tvaru

$$G = \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_k \end{pmatrix} = \begin{pmatrix} e_{11} & \dots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{k1} & \dots & e_{kn} \end{pmatrix}$$

se nazývá generující matice kódu C .

Příklad generující matice: kód sudé parity

Generující matice kódu sudé parity délky 4:

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \mathbf{e}_3 \end{pmatrix}$$

(Jak by vypadala matice pro kód liché parity?) Co musí platit:

- Každý řádek je kódové slovo.
- Řádky jsou nezávislé.
- Kód má délku 4, matice musí mít 4 sloupce.
- Kód má 1 kontrolní a 3 informační symboly, musí mít 3 řádky.
- Každé kódové slovo lze vyjádřit jako kombinace řádků matice.

Elementární úpravy generující matice

- Pokud je G generující matice kódu C , pak matice G' vzniklá z G pomocí elementárních řádkových maticových úprav je opět generující maticí kódu C .

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Další příklad

- Nechť $F = \mathbb{Z}_3$. Matice

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

je generující matice lineárního $(6, 3)$ kódu.

- Řádky jsou nezávislé, takže tvoří bázi 3-dimenzionálního podprostoru prostoru F^6 .

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

- Kód C obsahuje slova 112200, 220011, atd.

Kódování

- Nechť G je $k \times n$ generující matice obsahující vektory $\mathbf{e}_1, \dots, \mathbf{e}_k$.
- Každý vektor $\mathbf{u} = u_1 \dots u_k$ jednoznačně definuje vektor $\mathbf{v}$:
$$\mathbf{v} = \sum_{i=1}^k u_i \mathbf{e}_i$$
- Tedy $\mathbf{v} = \mathbf{u}G$
- Slovo $\mathbf{u}$ tak můžeme zakódovat pomocí předpisu:

$$e(\mathbf{u}) = \mathbf{u}G$$

Systematický kód

- Různé generující matice vedou k různým pravidlům kódování.
- Nejběžnější způsob je systematický kód: vybereme $u_1 \dots u_k$ symbolů a doplníme $u_{k+1} \dots u_n$.
- Generující matice má pak tvar $G = (E|B)$, kde E je jednotková $k \times k$ matice a B je $k \times n - k$ matice.

Definice: Lineární kód se nazývá systematický, pokud má generující matici tvaru $G = (E|B)$.

Příklad generující matice systematického kódu

Generující matice kódu sudé parity délky $n = 4$:

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

Generující matice Hammingova $(7, 4)$ kódu:

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

Příklad kódování

Zakódujeme slovo $\mathbf{u} = 100$ pomocí kódu sudé parity:

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

Výsledné kódové slovo je $\mathbf{v} = 1001$.

Případně můžeme slovo $\mathbf{v}$ spočítat pomocí koeficientů a vektorů báze:

$$\mathbf{v} = 1 \cdot (1001) + 0 \cdot (0101) + 0 \cdot (0011) = (1001)$$

Ekvivalentní kód

Definice: Kódy C_1 a C_2 se nazývají ekvivalentní, pokud existuje permutace π množiny $\{1, \dots, n\}$ taková, že pro všechna $u_1, \dots, u_n \in F$:

$$u_1, \dots, u_n \in C_1 \text{ právě když } u_{\pi(1)}, \dots, u_{\pi(n)} \in C_2$$

- Hammingův $(7, 4)$ kód je systematický, kód sudé parity délky 4 je systematický. Lineární $(6, 3)$ kód z předchozích slajdů není systematický, ale je ekvivalentní systematickému kódu.

Věta: Každý lineární kód je ekvivalentní systematickému kódu.

Kontrolní matice

Definice: Matice H , která má n sloupců a obsahuje prvky z tělesa F se nazývá kontrolní matice lineárního kódu C , jestliže pro všechna slova $\mathbf{u} \in F^n$ platí

$$\mathbf{u} \in C \text{ právě tehdy když } H\mathbf{u}^T = \mathbf{0}^T.$$

Vztah kontrolní a generující matice

Věta: Pro systematický kód C s generující maticí $G = (E_1|B)$ platí, že matice $H = (-B^T|E_2)$ je kontrolní matice kódu C , kde E_1 je jednotková matice typu $k \times k$ a E_2 je jednotková matice typu $n - k \times n - k$.

Důsledek: Každý lineární (n, k) kód má $n - k \times n$ kontrolní matici o hodnosti $n - k$.

Příklady kontrolní matice kódu sudé parity

Generující matice paritního kódu $n = 4, k = 3$:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = (E_1|B)$$

Takže kontrolní matice $H = (-B^T|E_2)$ by vypadala: $-B^T = (111)$, E_2 by byla typu 1×1 , tedy (1) :

$$H = (1 \quad 1 \quad 1 \quad 1)$$

Příklad kontrolní matice Hammingova kódu

Pro Hammingův (7, 4) kód máme generující matici:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (E_1|B)$$

Kontrolní matice:

$$H = (-B^T|E_2) = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Důkaz

Důkaz: Máme ověřit, že podprostor C generovaný generující maticí G je shodný s podprostorem C' všech řešení rovnice $H\mathbf{v}^T = \mathbf{0}$. Přitom platí:

$$HG^T = \left(-B^T | E_2\right) \cdot \begin{pmatrix} E_1 \\ B^T \end{pmatrix} = -B^T E_1 + E_2 B^T = -B^T + B^T = \mathbf{0}$$

Tedy pokud $G = (E_1 | B) = \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_k \end{pmatrix}$, pak $H\mathbf{e}_i^T = \mathbf{0}$ pro všechna i . Z

toho vyplývá, že všechna $\mathbf{e}_i$ jsou řešením rovnice $H\mathbf{v}^T = \mathbf{0}$ a že $\{\mathbf{e}_1, \dots, \mathbf{e}_k\} \subseteq C'$. Pokud $\{\mathbf{e}_1, \dots, \mathbf{e}_k\} \subseteq C'$, pak i $\text{obal}(\{\mathbf{e}_1, \dots, \mathbf{e}_k\}) \subseteq C'$, přičemž $\text{obal}(\{\mathbf{e}_1, \dots, \mathbf{e}_k\}) = C$. Prostor C je tak podprostorem prostoru C' .

Pokračování důkazu

$$G = (E_1|B), \quad H = (-B^T|E_2)$$

Nyní můžeme dokázat, že platí i $C \supseteq C'$, ale stačí nám dokázat, že prostory mají stejnou dimenzi, což bude jednodušší.

Matice G a tedy i matice B má k (lineárně nezávislých) řádků. Dimenze prostoru C je tak rovna k .

Jednotková matice E_2 je řádu $n - k$, takže matice H má hodnotu $h(H) = n - k$. Odtud plyne, že množina všech řešení rovnice $H\mathbf{v}^T = \mathbf{0}$ tvoří podprostor dimenze $n - h(H) = n - (n - k) = k$.

Dimenze prostorů C a C' jsou stejné, platí $C \subseteq C'$, takže $C = C'$. $\square$

Dekódování: Syndrom

- Opakování: pokud odešleme slovo $\mathbf{u}$ a přijmeme slovo $\mathbf{v}$, pak slovo $\mathbf{e} = \mathbf{v} - \mathbf{u}$ nazýváme chybové slovo.
- Pozor – už neplatí rovnost $\mathbf{v} - \mathbf{u} = \mathbf{v} + \mathbf{u}$.

Definice: Necht' H je $m \times n$ kontrolní matice kódu C . Syndrom slova $\mathbf{v}$ je slovo $\mathbf{s}$ definované jako

$$\mathbf{s}^T = H\mathbf{v}^T.$$

Vztah chybového slova a syndromu

Věta: Pokud vyšleme kódové slovo $\mathbf{u}$, přijmeme nekódové slovo $\mathbf{v}$, tak chybové slovo $\mathbf{e} = \mathbf{v} - \mathbf{u}$ a slovo $\mathbf{v}$ mají stejný syndrom. Tedy platí:

$$H\mathbf{e}^T = H\mathbf{v}^T$$

Důkaz: (využíváme faktu, že $H\mathbf{u}^T = \mathbf{0}^T$)

$$H\mathbf{e}^T = H(\mathbf{v} - \mathbf{u})^T = H\mathbf{v}^T - H\mathbf{u}^T = H\mathbf{v}^T - \mathbf{0}^T = H\mathbf{v}^T$$

Třída slova $\mathbf{e}$

- Nechť C je lineární (n, k) kód s kontrolní maticí H , která vznikla z generující matice G .
- Pro všechna slova $\mathbf{e} \in F^n$ definujeme množinu

$$\mathbf{e} + C = \{\mathbf{e} + \mathbf{u} \mid \mathbf{u} \in C\},$$

kterou nazveme třída slova $\mathbf{e}$.

- $\mathbf{e} + C$ je množina všech slov, která můžeme přijmout, pokud nastane chyba $\mathbf{e}$.

Vlastnosti třídy slov

- Pro libovolná $\mathbf{e}, \mathbf{e}' \in F^n$:
- Pokud $\mathbf{e} \in C$, pak $\mathbf{e} + C = C$.
- Buď $\mathbf{e} + C = \mathbf{e}' + C$, nebo $\mathbf{e} + C \cap \mathbf{e}' + C = \emptyset$.
- Počet slov v každé třídě je roven počtu kódových slov, tj.
 $|\mathbf{e} + C| = |C|$.
- Všechna slova z $\mathbf{e} + C$ mají stejný syndrom.

Příklad

Binární $(4, 3)$ kód sudé parity délky 3:

$$C = \{000, 101, 110, 011\}$$

Zvolme $\mathbf{e} = 110$:

$$\mathbf{e} + C = \{110, 011, 000, 101\}$$

Zvolme $\mathbf{e}' = 010$:

$$\mathbf{e}' + C = \{010, 111, 100, 001\}$$

Dekódování

- Reprezentant třídy $\mathbf{e} + C$ je slovo $\mathbf{r}$, které má minimální Hammingovu váhu ze všech slov z $\mathbf{e} + C$.
- Obecný princip dekodování pro jakýkoliv lineární kód:
- Přejmeme slovo $\mathbf{v}$. Spočítáme syndrom: $\mathbf{s}^T = H\mathbf{v}^T$.
- Z třídy slov $\mathbf{s} + C$ nalezneme reprezentanta $\mathbf{r}$. (Proč? Předpokládáme, že nastalo co nejméně chyb. Čím menší váhu slovo $\mathbf{r}$ bude mít, tím méně znaků změníme.)
- Dekódujeme na slovo $\mathbf{u} = \mathbf{v} - \mathbf{r}$.

Příklad

Kontrolní kód sudé parity délky 3 neopravuje žádnou chybu. Kontrolní matice:

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

Vyšleme slovo $\mathbf{u} = 110$, přijeme slovo $\mathbf{v} = 100$. Spočítáme syndrom:

$$\mathbf{s} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T = 1$$

Syndromu $\mathbf{s} = 1$ odpovídá třída $100 + C = \{010, 111, 100, 001\}$.

Vybereme reprezentanta $\rightarrow$ problém, tři slova mají váhu 1. Pokud vybereme $\mathbf{e} = 010$, opravíme správně:

$$\mathbf{u} = \mathbf{v} - \mathbf{e} = 100 - 010 = 110$$

Pokud vybereme $\mathbf{e} = 001$, opravíme špatně:

$$\mathbf{u} = \mathbf{v} - \mathbf{e} = 100 - 001 = 101$$

Poučení z příkladu

- Pokud má lineární kód opravovat chybu, musí ve třídě $\mathbf{e} + C$ existovat vždy jediný unikátní nejmenší reprezentant třídy.

Věta: Pokud má lineární kód C minimální vzdálenost $d(C)$, pak kód opravuje $t < d(C)/2$ chyb. Pokud došlo během přenosu k t chybám, kterým odpovídá chybové slovo $\mathbf{e}$, tak třída $\mathbf{e} + C$ obsahuje právě jedno slovo o váze $< d(C)/2$ a to slovo $\mathbf{e}$.

Důkaz

Dokážeme, že pokud lineární kód C opravuje t chyb, které reprezentuje chybové slovo $\mathbf{e}$ o váze t , tak třída $\mathbf{e} + C$ obsahuje právě jedno slovo o váze $< d(C)/2$ a to slovo $\mathbf{e}$.

Předpokládejme, že jsme poslali slovo $\mathbf{u}$, přijali slovo $\mathbf{v}$ a během přenosu nastalo t chyb, $\mathbf{e} = \mathbf{v} - \mathbf{u}$ a $|\mathbf{e}| = t$, kde $|\mathbf{e}|$ je váha slova $\mathbf{e}$.

Sporem předpokládejme, že třída $\mathbf{e} + C$ obsahuje různá slova $\mathbf{v}_1$ a $\mathbf{v}_2$ taková, že $|\mathbf{v}_1| < d(C)/2$ a $|\mathbf{v}_2| < d(C)/2$. Pak ale také $\delta(\mathbf{v}_1, \mathbf{v}_2) < d(C)$. Přitom ale $\mathbf{v}_1 = \mathbf{u}_1 + \mathbf{e}$ a $\mathbf{v}_2 = \mathbf{u}_2 + \mathbf{e}$ pro nějaká $\mathbf{u}_1, \mathbf{u}_2 \in C$. Po dosazení máme $\delta(\mathbf{u}_1 + \mathbf{e}, \mathbf{u}_2 + \mathbf{e}) < d(C)$ a tedy i $\delta(\mathbf{u}_1, \mathbf{u}_2) < d(C)$, což je spor s tím, že $\mathbf{u}_1, \mathbf{u}_2 \in C$. Třída $\mathbf{e} + C$ tak obsahuje jediné slovo o váze $< d(C)/2$. Přitom platí, že $\mathbf{0} \in C$, takže $\mathbf{e} + \mathbf{0} = \mathbf{e} \in \mathbf{e} + C$ a $|\mathbf{e}| = t < d(C)/2$. Tedy $\mathbf{e}$ je jediné slovo v třídě $\mathbf{e} + C$, které má váhu menší než $d(C)/2$. □

Příklad

Hammingův (7, 4) kód má kontrolní matici:

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

Slovo $\mathbf{e}_0 = 0000000$ má syndrom 000, slovo $\mathbf{e}_1 = 1000000$ má syndrom 001, slovo $\mathbf{e}_2 = 0100000$ má syndrom 010 atd. Dostáváme tak třídy $\mathbf{e}_0 + C, \mathbf{e}_1 + C, \mathbf{e}_2 + C, \dots$ a reprezentanty $\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2 \dots$

Pro $\mathbf{v} = 1010111$ máme $H\mathbf{v}^T = (110)^T$. Syndrom 110 má reprezentanta $\mathbf{e}_6 = 0000010$, takže dekódujeme

$$\mathbf{u} = \mathbf{v} - 0000010 = 1010101.$$