Lineární kódy

Příklad 32

Uvažujme lineární prostor Z_2^5 (tj. množinu všech pětic z nul a jedniček). Rozhodněte, zda následující podmnožiny jsou lineárními kódy.

Kdy podmnožina tvoří lineární podprostor Z_2^5?

S každými dvěma značkami do ní patří i jejich součet.

S každou značkou tam patří i její libovolný skalární násobek, tedy nulová značka.

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Splňuje podmínku značka 00000 ?

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Splňuje podmínku značka 00000 ?

$x_2 = 0$, $x_3 = 0$

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Splňuje podmínku značka 00000 ?

$$x_2 = 0\ ,\ \ x_3 = 0\ ,\ \ x_5 = \ 0 + 0 = 0$$

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Splňuje podmínku obecná značka $z = x + y$?

$$x_2 + x_3 = x_5 \,, \quad y_2 + y_3 = y_5 \quad (x\,, y \;\in\; K_1)$$

$$z_2 = \; x_2 + y_2 \,, \quad z_3 = \; x_3 + y_3 \,, \; z_5 = \; x_5 + y_5$$

$$(z = x + y)$$

Pak $z_5 = \; x_5 + y_5 = x_2 + x_3 + y_2 + y_3 =$

$$= x_2 + (x_3 + y_2) + y_3 \; = x_2 + (y_2 + x_3) + y_3 =$$

$$= (x_2 + y_2) + (x_3 + y_3) \; = z_2 + z_3 \quad \text{OK}$$

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Dokázali jsme:

$$00000 \in K_1$$

$$\forall \; x, y \in K_1 : x + y \in K_1$$

Závěr:

K_1 je lineárním podprostorem $Z_2{}^{5}$,

K_1 je tedy lineární kód

Příklad 32

K_2 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = 1$$

Splňuje podmínku značka 00000 ?

$x_2 = 0$, $x_3 = 0$, $x_2 + x_3 = 0 + 0 = 0$ NE

Příklad 32

K_2 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = 1$$

Dokázali jsme:

$$00000 \notin K_1$$

Závěr:

K_2 není lineárním podprostorem $Z_2{}^5$,

K_2 tedy není lineární kód

Příklad 32

K_3 je tvořena všemi slovy s právě dvěma znaky 1

Splňuje podmínku značka 00000 ? NE

Dokázali jsme:

$$00000 \notin K_3$$

Závěr:

K_3 není lineárním podprostorem $Z_2^{\ 5}$,

K_3 tedy není lineární kód

Příklad 32

K_4 je tvořena všemi slovy s méně než třemi 1

Splňuje podmínku značka 00000 ? ANO

Příklad 32

K_4 je tvořena všemi slovy s méně než třemi 1

Splňuje podmínku obecná značka $x + y$?

Vezměme

$$x = 11000 \;,\; y = 00110 \qquad (x, y \in K_4)$$

Pak

$$z = x + y = 11000 + 00110 = 11110$$

$$(z \notin K_4) \qquad \text{NE}$$

Příklad 32

K_4 je tvořena všemi slovy s méně než třemi 1

Dokázali jsme:

$$\exists\, x\, \exists\, y : \; x + y \notin K_4$$

tedy neplatí $\forall\, x\, \forall\, y : \; x + y \in K_4$

Závěr:

K_4 není lineárním podprostorem $Z_2^{\;5}$,

K_4 tedy není lineární kód

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Určení dimenze:

- ve značce je pět prvků
- jeden z nich se počítá z těch ostatních

$$\Rightarrow$$

- čtyři prvky jsou libovolně (nezávisle) volitelné

$$\Rightarrow$$

- K_1 je lineární podprostor dimenze 4

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Určení báze:

$$\begin{array}{ccccc} x_1 & x_2 & x_3 & x_4 & x_5 \\ \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{K} \end{array}$$

Na místě informačních prvků prostřídáme právě jednu jedničku, kontrolní prvky (v našem případě jeden prvek) vždy dopočítáme z podmínky.

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Určení báze:

$$x_1 \; x_2 \; x_3 \; x_4 \; x_5$$

$$\mathrm{I} \quad \mathrm{I} \quad \mathrm{I} \quad \mathrm{I} \quad \mathrm{K}$$

$$b_1 = [10000]^T \qquad b_2 = [01001]^T$$

$$b_3 = [00101]^T \qquad b_4 = [00010]^T$$

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Určení generující matice:

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

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Určení kontrolní rovnice:

$$x_2 + x_3 = x_5 \qquad | + (-x_5)$$

$$x_2 + x_3 + (-x_5) = 0 \qquad -x_5 = x_5$$

$$x_2 + x_3 + x_5 = 0$$

Příklad 32

K_1 je tvořena všemi slovy, splňujícími podmínku

$$x_2 + x_3 = x_5$$

Určení kontrolní matice:

Kontrolní matice je matice soustavy homogenních kontrolních rovnic.

Řádky matice odpovídají levým stranám kontrolních rovnic v anulovaném tvaru (tj. s nulovou pravou stranou).

Příklad 32

Typy (rozměry) matic G a H:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad k/n$$

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \end{bmatrix} \quad (n\text{-}k)/n$$

n ... celkový počet prvků ve značce

k ... počet informačních prvků ve značce

Příklad 32

Vztah mezi maticemi G a H u systematických kódů ($n =$ délka značky, $k =$ počet inf. prvků):

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \qquad G = [I_k \mid \quad B]$$

$$H = [0 \quad 1 \quad 1 \quad 0 \quad 1] \qquad H = [-B^T \mid \quad I_{n-k}]$$

Příklad 33

Nad tělesem Z_5 uvažujme lineární kód generovaný maticí

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

Lze tento kód generovat maticí v systematickém tvaru?

= lze tuto maticí převést řádkovými úpravami na systematický tvar?

Příklad 33

Operace nad tělesem Z_5 :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Opačné prvky:

$-1 = 4$ $\quad$ $-3 = 2$

$-2 = 3$ $\quad$ $-4 = 1$

$-0 = 0$

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Inverzní prvky:

$1^{-1} = 1$ $\quad$ $3^{-1} = 2$

$2^{-1} = 3$ $\quad$ $4^{-1} = 4$

Příklad 33

Příklad výpočtu v Z_5 :

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$3 \cdot 4 + 2 \cdot 2 + 2 \cdot 3 \cdot 4 =$

$= 2 + 4 + 1 \cdot 4 = 2 + 4 + 4 =$

$= 1 + 4 = \mathbf{0}$

Alternativní způsob:

·	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$3 \cdot 4 + 2 \cdot 2 + 2 \cdot 3 \cdot 4 =$

$= 12 + 4 + 24 = 40$

$40 \bmod 5 = 0$

Příklad 33

Nad tělesem Z_5 uvažujme lineární kód generovaný maticí

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

Řádkovými úpravami převedeme matici na „stupňovitý tvar“ tak, aby hodnota všech „pivotových prvků“ byla 1.

Příklad 33

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

Příklad 33

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix} \qquad (2) = (2) - 2 \cdot (1)$$

Příklad 33

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix} \quad (2) = (2) - 2 \cdot (1) = (2) + 3 \cdot (1)$$

Příklad 33

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix} \quad (2) = (2) - 2 \cdot (1) = (2) + 3 \cdot (1)$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

Příklad 33

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

Příklad 33

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix} \quad (3) = (3) - 2 \cdot (2) = (3) + 3 \cdot (2)$$

Příklad 33

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix} \quad (3) = (3) - 2 \cdot (2) = (3) + 3 \cdot (2)$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

Příklad 33

$$A = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \quad (3) = (3) \cdot 2^{-1}$$

Příklad 33

$$A \sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \quad (3) = (3) \cdot 2^{-1} = (3) \cdot 3$$

Příklad 33

$$A \sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \quad (3) = (3) \cdot 2^{-1} = (3) \cdot 3$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Příklad 33

$$A \sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \quad (3) = (3) \cdot 2^{-1} = (3) \cdot 3$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Příklad 33

$$A \sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \quad (3) = (3) \cdot 2^{-1} = (3) \cdot 3$$

$$\sim \begin{bmatrix} \color{red}{1} & 4 & 1 & 1 & 1 \\ 0 & \color{red}{1} & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & \color{red}{1} \end{bmatrix}$$

Lineárně nezávislé jsou sloupce 1,2,5.

Příklad 33

$$A \sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \quad (3) = (3) \cdot 2^{-1} = (3) \cdot 3$$

$$\sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$ Lineárně nezávislé jsou sloupce 1,2,5.

Kód nelze generovat systematickou generující maticí

Příklad 33

$$A \sim \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \quad (3) = (3) \cdot 2^{-1} = (3) \cdot 3$$

$$\sim \begin{bmatrix} \color{red}{1} & 4 & 1 & 1 & 1 \\ 0 & \color{red}{1} & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & \color{red}{1} \end{bmatrix}$$ Lineárně nezávislé jsou sloupce 1,2,5.

Kód nelze generovat systematickou generující maticí $\Rightarrow$

Kód není systematický.

Příklad 33

$$G = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Příklad 33

$$G = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A i G generují stejný lineární prostor.

Příklad 33

$$G = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A i G generují stejný lineární prostor.

Permutací sloupců matice G lze vytvořit ekvivalentní kód, který bude systematický.

Příklad 33

$$G = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A i G generují stejný lineární prostor.

1 2 3 4 5

Permutací sloupců matice G lze vytvořit ekvivalentní kód, který bude systematický:

Příklad 33

$$G = \begin{array}{c} \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\ \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \end{array}$$

A i G generují stejný lineární prostor.

Permutací sloupců matice G lze vytvořit ekvivalentní kód, který bude systematický:

$$G' = \begin{array}{c} \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \\ \begin{array}{ccccc} 1 & 2 & 5 & 4 & 3 \end{array} \end{array}$$

Příklad 33

$$G = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A i G generují stejný lineární prostor.

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix}$$

Permutací sloupců matice G lze vytvořit ekvivalentní kód, který bude systematický:

$$G' = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

G‘ generuje jiný prostor než A a G.

$$\begin{matrix} 1 & 2 & 5 & 4 & 3 \end{matrix}$$

Příklad 33

Budeme pokračovat v hledání generující matice v systematickém tvaru řádkovými úpravami matice G′:

$$G' = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Příklad 33

Budeme pokračovat v hledání generující matice v systematickém tvaru řádkovými úpravami matice G′:

$$G' = \begin{bmatrix} 1 & {\color{red}4} & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Příklad 33

Budeme pokračovat v hledání generující matice v systematickém tvaru řádkovými úpravami matice G′:

$$G' = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (1) = (1) - 4\,(2)$$

Příklad 33

Budeme pokračovat v hledání generující matice v systematickém tvaru řádkovými úpravami matice G′:

$$G' = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (1) = (1) - 4\,(2) = (1) + (2)$$

Příklad 33

Budeme pokračovat v hledání generující matice v systematickém tvaru řádkovými úpravami matice G′:

$$G' = \begin{bmatrix} 1 & \color{red}{4} & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (1) = (1) - 4\,(2) = (1) + (2)$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 4 & 4 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Příklad 33

Budeme pokračovat v hledání generující matice v systematickém tvaru řádkovými úpravami matice G′:

$$G' = \begin{bmatrix} 1 & 0 & 0 & 4 & 4 \\ 0 & 1 & {\color{red}4} & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (2) = (2) - 4 \cdot (3) = (2) + (3)$$

Příklad 33

Budeme pokračovat v hledání generující matice v systematickém tvaru řádkovými úpravami matice G′:

$$G' = \begin{bmatrix} 1 & 0 & 0 & 4 & 4 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (2) = (2) - 4 \cdot (3) = (2) + (3)$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Příklad 33

Matice G“ je maticí systematického kódu v systematickém tvaru:

$$G'' = \begin{bmatrix} 1 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Příklad 33

Matice G“ je maticí systematického kódu v systematickém tvaru:

$$G'' = \begin{bmatrix} 1 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$G = [I_k \mid \quad B]$$

Příklad 33

Matice G“ je maticí systematického kódu v systematickém tvaru:

$$G'' = \begin{bmatrix} 1 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$G = [I_k \mid \quad B]$$

Kontrolní matice H“:

$$H = [-B^T \mid \quad I_{n-k}]$$

Příklad 33

Matice G“ je maticí systematického kódu v systematickém tvaru:

$$G'' = \begin{bmatrix} 1 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$G = [I_k \mid \quad B]$$

Kontrolní matice H“:

$$H'' = \begin{bmatrix} 1 & 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

$$H = [-B^T \mid \quad I_{n-k}]$$

Příklad 33

Jak najít kontrolní matici H ke kódu generovanému výchozí maticí A (respektive maticí G)?

Příklad 33

Jak najít kontrolní matici H ke kódu generovanému výchozí maticí A (respektive maticí G)?

Zpětnou permutací sloupců kontrolní matice H“

Příklad 33

Jak najít kontrolní matici H ke kódu generovanému výchozí maticí A (respektive maticí G)?

Zpětnou permutací sloupců kontrolní matice H“

$$G = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Příklad 33

Jak najít kontrolní matici H ke kódu generovanému výchozí maticí A (respektive maticí G)?

Zpětnou permutací sloupců kontrolní matice H“

$$G = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Kontrolní matice H“:

$$H'' = \begin{bmatrix} 1 & 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

Příklad 33

Jak najít kontrolní matici H ke kódu generovanému výchozí maticí A (respektive maticí G)?

Zpětnou permutací sloupců kontrolní matice H“

$$G = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Kontrolní matice H“: G a H'' „nepatří k sobě“ !!!

$$H'' = \begin{bmatrix} 1 & 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

Příklad 33

$$G = \begin{array}{c} \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\ \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \end{array}$$

Příklad 33

$$G = \begin{array}{c}\begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\ \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix}\end{array} \qquad G' = \begin{array}{c}\begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \\ \begin{matrix} 1 & 2 & 5 & 4 & 3 \end{matrix}\end{array}$$

Příklad 33

$$G = \begin{array}{c} \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\ \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \end{array}$$

$$G' = \begin{array}{c} \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \\ \begin{matrix} 1 & 2 & 5 & 4 & 3 \end{matrix} \end{array}$$

$$H'' = \begin{array}{c} \begin{bmatrix} 1 & 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 \end{bmatrix} \\ \begin{matrix} 1 & 2 & 5 & 4 & 3 \end{matrix} \end{array}$$

Příklad 33

$$G = \begin{array}{c} \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\ \begin{matrix} \color{red}{1} & \color{red}{2} & \color{red}{3} & \color{red}{4} & \color{red}{5} \end{matrix} \end{array} \qquad G' = \begin{array}{c} \begin{bmatrix} 1 & 4 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \\ \begin{matrix} \color{red}{1} & \color{red}{2} & \color{red}{5} & \color{red}{4} & \color{red}{3} \end{matrix} \end{array}$$

$$H = \begin{array}{c} \begin{bmatrix} 1 & 2 & 0 & 1 & 0 \\ 1 & 2 & 1 & 0 & 0 \end{bmatrix} \\ \begin{matrix} \color{red}{1} & \color{red}{2} & \color{red}{3} & \color{red}{4} & \color{red}{5} \end{matrix} \end{array} \qquad H'' = \begin{array}{c} \begin{bmatrix} 1 & 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 \end{bmatrix} \\ \begin{matrix} \color{red}{1} & \color{red}{2} & \color{red}{5} & \color{red}{4} & \color{red}{3} \end{matrix} \end{array}$$

Příklad 33

Závěr:

Příklad 33

Závěr:

Výchozí matice A a matice G generují stejný kód.

Příklad 33

Závěr:

Výchozí matice A a matice G generují stejný kód.

Matice G‘ a G‘‘ generují stejný kód.

Příklad 33

Závěr:

Výchozí matice A a matice G generují stejný kód.

Matice G‘ a G‘‘ generují stejný kód.

Matice H‘‘ má kontrolní vlastnost vůči kódu generovanému maticemi G‘ a G‘‘ .

Příklad 33

Závěr:

Výchozí matice A a matice G generují stejný kód.

Matice G‘ a G‘‘ generují stejný kód.

Matice H‘‘ má kontrolní vlastnost vůči kódu generovanému maticemi G‘ a G‘‘ .

Matice H má kontrolní vlastnost vůči kódu generovanému maticemi A a G .

Příklad 34

Nad tělesem Z_3 je dána generující matice

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

Určete kontrolní matici a kontrolní rovnice.

Příklad 34

Nad tělesem Z_3 je dána generující matice

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

Určete kontrolní matici a kontrolní rovnice.

Jedna možnost – postup viz příklad 33.

Příklad 34

Nad tělesem Z_3 je dána generující matice

$$\mathrm{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Určete kontrolní matici a kontrolní rovnice.

Jedna možnost – postup viz příklad 33.

Druhá možnost – využít vlastností kontrolní matice a vyřešit soustavu lineárních rovnic

Příklad 34

Nad tělesem Z_3 je dána generující matice

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

Každý řádek kontrolní rovnice musí být ortogo-nální na každý řádek generující matice.

Příklad 34

Nad tělesem Z_3 je dána generující matice

$$\mathrm{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Každý řádek kontrolní rovnice musí být ortogo-nální na každý řádek generující matice.

Předpokládejme obecný řádek matice H ve tvaru

$$\mathrm{h} = \begin{bmatrix} \mathrm{h}_1 & \mathrm{h}_2 & \mathrm{h}_3 & \mathrm{h}_4 & \mathrm{h}_5 \end{bmatrix}$$

Příklad 34

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

$$h = \begin{bmatrix} h_1 & h_2 & h_3 & h_4 & h_5 \end{bmatrix}$$

Příklad 34

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

$$h = [h_1 \quad h_2 \quad h_3 \quad h_4 \quad h_5]$$

Pak $h_1 + h_2 + h_3 + h_4 + h_5 = 0$

Příklad 34

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

$$h = [h_1 \quad h_2 \quad h_3 \quad h_4 \quad h_5]$$

Pak

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0$$

$$h_2 + h_3 + h_4 + h_5 = 0$$

Příklad 34

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

$$h = \begin{bmatrix} h_1 & h_2 & h_3 & h_4 & h_5 \end{bmatrix}$$

Pak

$$\begin{aligned} h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \\ h_2 + h_3 + h_4 + h_5 &= 0 \\ h_1 + h_2 \qquad\qquad\qquad &= 0 \end{aligned}$$

Příklad 34

Řešíme homogenní soustavu

$$
\begin{aligned}
h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \\
h_2 + h_3 + h_4 + h_5 &= 0 \\
h_1 + h_2 &= 0
\end{aligned}
$$

Příklad 34

Řešíme homogenní soustavu

$$
\begin{aligned}
h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \\
h_2 + h_3 + h_4 + h_5 &= 0 \\
h_1 + h_2 \phantom{{}+ h_3 + h_4 + h_5} &= 0
\end{aligned}
$$

3 rovnice pro 5 proměnných

Příklad 34

Řešíme homogenní soustavu

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0$$
$$h_2 + h_3 + h_4 + h_5 = 0$$
$$h_1 + h_2 + h_3 + h_4 + h_5 = 0$$

3 rovnice pro 5 proměnných $\Rightarrow$

řešením je lineární prostor dimenze 2

Příklad 34

Operace nad tělesem Z_3 :

+	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

·	**0**	**1**	**2**
0	0	0	0
1	0	1	2
2	0	2	1

Opačné prvky:

$-1 = 2$ $\quad$ $-0 = 0$

$-2 = 1$

Inverzní prvky:

$1^{-1} = 1$ $\quad$ $2^{-1} = 2$

Příklad 34

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0 \qquad (1)$$

$$h_2 + h_3 + h_4 + h_5 = 0 \qquad (2)$$

$$h_1 + h_2 = 0 \qquad (3)$$

Příklad 34

$$
\begin{aligned}
h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \qquad (1)\\
h_2 + h_3 + h_4 + h_5 &= 0 \qquad (2)\\
h_1 + h_2 &= 0 \qquad (3)
\end{aligned}
$$

Lze řešit intuitivně dosazováním:

Příklad 34

$$
\begin{aligned}
h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \qquad (1)\\
h_2 + h_3 + h_4 + h_5 &= 0 \qquad (2)\\
h_1 + h_2 &= 0 \qquad (3)
\end{aligned}
$$

Lze řešit intuitivně dosazováním:

(2) $\rightarrow$ (1)

Příklad 34

$$\mathrm{h}_1 + \mathrm{h}_2 + \mathrm{h}_3 + \mathrm{h}_4 + \mathrm{h}_5 = 0 \quad (1)$$

$$\mathrm{h}_2 + \mathrm{h}_3 + \mathrm{h}_4 + \mathrm{h}_5 = 0 \quad (2)$$

$$\mathrm{h}_1 + \mathrm{h}_2 = 0 \quad (3)$$

Lze řešit intuitivně dosazováním:

(2) $\rightarrow$ (1) $\quad \mathrm{h}_1 = 0 \quad$ (4)

Příklad 34

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0 \qquad (1)$$

$$h_2 + h_3 + h_4 + h_5 = 0 \qquad (2)$$

$$h_1 + h_2 = 0 \qquad (3)$$

Lze řešit intuitivně dosazováním:

(2) $\rightarrow$ (1) $\qquad h_1 = 0 \qquad$ (4)

(4) $\rightarrow$ (3)

Příklad 34

$$\begin{aligned}
h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \qquad (1)\\
h_2 + h_3 + h_4 + h_5 &= 0 \qquad (2)\\
h_1 + h_2 &= 0 \qquad (3)
\end{aligned}$$

Lze řešit intuitivně dosazováním:

(2) $\rightarrow$ (1) $\quad h_1 = 0 \qquad$ (4)

(4) $\rightarrow$ (3) $\quad h_2 = 0 \qquad$ (5)

Příklad 34

$$\begin{aligned} h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \quad (1) \\ h_2 + h_3 + h_4 + h_5 &= 0 \quad (2) \\ h_1 + h_2 \qquad\qquad\qquad &= 0 \quad (3) \end{aligned}$$

Lze řešit intuitivně dosazováním:

(2) $\rightarrow$ (1) $\quad h_1 = 0 \quad$ (4)

(4) $\rightarrow$ (3) $\quad h_2 = 0 \quad$ (5)

(5) $\rightarrow$ (2)

Příklad 34

$$\begin{aligned} h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \qquad (1) \\ h_2 + h_3 + h_4 + h_5 &= 0 \qquad (2) \\ h_1 + h_2 \phantom{{}+ h_3 + h_4 + h_5} &= 0 \qquad (3) \end{aligned}$$

Lze řešit intuitivně dosazováním:

$$\begin{aligned} (2) \rightarrow (1) \qquad h_1 &= 0 \qquad (4) \\ (4) \rightarrow (3) \qquad h_2 &= 0 \qquad (5) \\ (5) \rightarrow (2) \qquad h_3 + h_4 + h_5 &= 0 \qquad (6) \end{aligned}$$

Příklad 34

$$\begin{aligned} h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \qquad (1) \\ h_2 + h_3 + h_4 + h_5 &= 0 \qquad (2) \\ h_1 + h_2 &= 0 \qquad (3) \end{aligned}$$

Řešením bude libovolný vektor ve tvaru

Příklad 34

$$
\begin{aligned}
h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \qquad (1)\\
h_2 + h_3 + h_4 + h_5 &= 0 \qquad (2)\\
h_1 + h_2 &= 0 \qquad (3)
\end{aligned}
$$

Řešením bude libovolný vektor ve tvaru

$$h = [0 \quad 0 \quad h_3 \quad h_4 \quad h_5]$$

Příklad 34

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0 \qquad (1)$$

$$h_2 + h_3 + h_4 + h_5 = 0 \qquad (2)$$

$$h_1 + h_2 = 0 \qquad (3)$$

Řešením bude libovolný vektor ve tvaru

$$h = [0 \quad 0 \quad h_3 \quad h_4 \quad h_5]$$

kde $h_3 + h_4 + h_5 = 0$

Příklad 34

$$\begin{aligned} h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \quad (1) \\ h_2 + h_3 + h_4 + h_5 &= 0 \quad (2) \\ h_1 + h_2 \qquad\qquad\qquad &= 0 \quad (3) \end{aligned}$$

Řešením bude libovolný vektor ve tvaru

$$h = [0 \quad 0 \quad h_3 \quad h_4 \quad h_5]$$

kde $h_3 + h_4 + h_5 = 0$, čili $h_3 = - h_4 - h_5$

Příklad 34

$$
\begin{aligned}
h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \qquad (1)\\
h_2 + h_3 + h_4 + h_5 &= 0 \qquad (2)\\
h_1 + h_2 \qquad\qquad\qquad &= 0 \qquad (3)
\end{aligned}
$$

Za h_4 a h_5 budeme volit prvky kanonické báze:

Příklad 34

$$\begin{aligned} \mathrm{h}_1 + \mathrm{h}_2 + \mathrm{h}_3 + \mathrm{h}_4 + \mathrm{h}_5 &= 0 \qquad (1) \\ \mathrm{h}_2 + \mathrm{h}_3 + \mathrm{h}_4 + \mathrm{h}_5 &= 0 \qquad (2) \\ \mathrm{h}_1 + \mathrm{h}_2 &= 0 \qquad (3) \end{aligned}$$

Za h_4 a h_5 budeme volit prvky kanonické báze:

$\mathrm{h}_4 = 1, \;\; \mathrm{h}_5 = 0$

Příklad 34

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0 \qquad (1)$$

$$h_2 + h_3 + h_4 + h_5 = 0 \qquad (2)$$

$$h_1 + h_2 = 0 \qquad (3)$$

Za h_4 a h_5 budeme volit prvky kanonické báze:

$h_4 = 1, \ \ h_5 = 0 \qquad h = \begin{bmatrix} 0 & 0 & 2 & 1 & 0 \end{bmatrix}$

Příklad 34

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0 \qquad (1)$$

$$h_2 + h_3 + h_4 + h_5 = 0 \qquad (2)$$

$$h_1 + h_2 = 0 \qquad (3)$$

Za h_4 a h_5 budeme volit prvky kanonické báze:

$h_4 = 1,\ \ h_5 = 0 \qquad h = [0 \quad 0 \quad 2 \quad 1 \quad 0]$

$h_4 = 0,\ \ h_5 = 1$

Příklad 34

$$
\begin{aligned}
h_1 + h_2 + h_3 + h_4 + h_5 &= 0 \qquad (1)\\
h_2 + h_3 + h_4 + h_5 &= 0 \qquad (2)\\
h_1 + h_2 \qquad\qquad\qquad &= 0 \qquad (3)
\end{aligned}
$$

Za h_4 a h_5 budeme volit prvky kanonické báze:

$h_4 = 1,\ \ h_5 = 0 \qquad h = [0 \quad 0 \quad 2 \quad 1 \quad 0]$

$h_4 = 0,\ \ h_5 = 1 \qquad h = [0 \quad 0 \quad 2 \quad 0 \quad 1]$

Příklad 34

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0 \qquad (1)$$

$$h_2 + h_3 + h_4 + h_5 = 0 \qquad (2)$$

$$h_1 + h_2 = 0 \qquad (3)$$

$$h_3 = 1, \quad h_4 = 0 \qquad h = [0 \quad 0 \quad 2 \quad 1 \quad 0]$$

$$h_3 = 0, \quad h_4 = 1 \qquad h = [0 \quad 0 \quad 2 \quad 0 \quad 1]$$

Příklad 34

$$h_1 + h_2 + h_3 + h_4 + h_5 = 0 \qquad (1)$$

$$h_2 + h_3 + h_4 + h_5 = 0 \qquad (2)$$

$$h_1 + h_2 = 0 \qquad (3)$$

$$h_4 = 1, \;\; h_5 = 0 \qquad h = \begin{bmatrix} 0 & 0 & 2 & 1 & 0 \end{bmatrix}$$

$$h_4 = 0, \;\; h_5 = 1 \qquad h = \begin{bmatrix} 0 & 0 & 2 & 0 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 \end{bmatrix}$$

Příklad 34

Kontrolní matice:

$$\mathrm{H} = \begin{bmatrix} 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 \end{bmatrix}$$

Příklad 34

Kontrolní matice:

$$H = \begin{bmatrix} 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 \end{bmatrix}$$

Kontrolní rovnice: $2 \cdot v_3 + v_4 = 0$

$2 \cdot v_3 + v_5 = 0$

Příklad 34

Kontrolní matice:

$$H = \begin{bmatrix} 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 \end{bmatrix}$$

Kontrolní rovnice: $2 \cdot v_3 + v_4 = 0$

$2 \cdot v_3 + v_5 = 0$

Generující matice v systematickém tvaru:

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