Bezpečnostní kódy

Lineární kódy

1. Budeme pracovat nad tělesem $\mathbb{Z}_2$. Nad ním vytvoříme lineární prostor $\mathbb{Z}_2^5$, tedy množinu všech pětic. Zjistěte, zda následující podmnožiny jsou lineární kódy.
a) $\boldsymbol{K}_1$: všechna slova splňující $x_2 + x_3 = x_5$
b) $\boldsymbol{K}_2$: všechna slova splňující $x_2 + x_3 = 1$
c) $\boldsymbol{K}_3$: všechna slova obsahující méně než tři jedničky
U podmnožin, které jsou lineárními kódy, určete jejich dimenzi, navrhněte bázi, generující matici a kontrolní matici.

Abychom zjistili, zda je podmnožina lineárním kódem, ověříme, zda má vlastnosti lineárního prostoru (podprostoru $\mathbb{Z}_2^5$). Vlastnosti lineárního prostoru jsou:

- Operace sčítání je uzavřená. $\forall\ u, v \in \boldsymbol{K}$: $u + v \in \boldsymbol{K}$
- Operace násobení skalárem je uzavřená. $\forall\ c \in \mathbb{Z}_2$, $\forall\ u \in \boldsymbol{K}$: $c \cdot u \in \boldsymbol{K}$
- Existuje nulový prvek. $\exists\ o \in \boldsymbol{K}$: $\forall\ u \in \boldsymbol{K}$: $u + o = u$
- Pro každý prvek existuje opačný prvek. $\forall\ u \in \boldsymbol{K}\ \exists\ -u \in \boldsymbol{K}$: $u + (-u) = o$

Ověřme teď vlastnosti u zadaných podmnožin.

a) $\boldsymbol{K}_1$: všechna slova splňující $x_2 + x_3 = x_5$

- Uzavřenost operace sčítání

Podívejme se obecně na součet dvou prvků $u, v \in \boldsymbol{K}_1$

u_1	u_2	u_3	u_4	u_5
v_1	v_2	v_3	v_4	v_5
u_1+v_1	u_2+v_2	u_3+v_3	u_4+v_4	u_5+v_5

Potřebujeme ověřit, zda součet je prvkem $\boldsymbol{K}_1$, tedy zda platí

$$u_2+v_2 + u_3+v_3 = u_5+v_5$$

Malou změnou uspořádání dostaneme

$$u_2+u_3 + v_2+v_3 = u_5+v_5$$

Víme, že platí

$$u_2 + u_3 = u_5$$
$$v_2 + v_3 = v_5$$

Dosazením do ověřované rovnice získáme

$$u_5 + v_5 = u_5 + v_5$$

Rovnost vždy platí.

- Uzavřenost operace násobení skalárem

Násobit můžeme jen čísly 0 nebo 1. Při násobení libovolného prvku nulou získáme [00000] $\in \boldsymbol{K}_1$. Když libovolné $u \in \boldsymbol{K}_1$ vynásobíme jedničkou, dostaneme opět u. Operace násobení skalárem je uzavřená.

- Existence nulového prvku

Nulový prvek je [00000].

- Existence opačného prvku

Nad tělesem $\mathbb{Z}_2$ počítáme modulo 2. Každý prvek je tak sám k sobě opačný.

Množina $\boldsymbol{K}_1$ má všechny vlastnosti lineárního prostoru, takže to je lineární kód.

b) $\boldsymbol{K}_2$: všechna slova splňující $x_2 + x_3 = 1$

Než začneme ověřovat všechny vlastnosti lineárního prostoru, zkusme najít příklad, kterým vyvrátíme, že je podmnožina lineárním prostorem. V podmnožině $\boldsymbol{K}_2$ neexistuje nulový prvek, protože [00000] nesplňuje podmínku $x_2 + x_3 = 1$. Množina $\boldsymbol{K}_2$ nemá vlastnosti lineárního prostoru, takže to není lineární kód.

c) $\boldsymbol{K}_3$: všechna slova obsahující méně než tři jedničky

Zkusme znovu najít příklad, kterým vyvrátíme, že je podmnožina lineárním prostorem. Vezměme prvky [11000] a [00110]. Jejich součet [11110] obsahuje čtyři jedničky a tedy není prvkem $\boldsymbol{K}_3$. Operace sčítání není uzavřená. Množina $\boldsymbol{K}_3$ nemá vlastnosti lineárního prostoru, takže to není lineární kód.

Dále se budeme zabývat lineárním kódem $\boldsymbol{K}_1$. Uvažme obecné slovo $[u_1\ u_2\ u_3\ u_4\ u_5] \in \boldsymbol{K}_1$. První čtyři prvky můžeme zvolit, pátý dopočítáme podle zadané podmínky $u_2 + u_3 = u_5$. Dimenze tohoto lineárního prostoru je tedy $\dim(\boldsymbol{K}_1) = 4$. První čtyři prvky u_1, u_2, u_3, u_4 nazveme *informační* (můžeme do nich uložit libovolnou informaci), pátý prvek u_5 je *zabezpečovací* (slouží pro kontrolu správnosti kódového slova). Zabezpečení je zde velmi slabé. Kontroluje se vlastně jen druhý a třetí prvek. Ale to nám pro tuto chvíli nevadí.

Bázi prostoru $\boldsymbol{K}_1$ můžeme zvolit mnoha způsoby. Zpravidla se volí kanonická (ortonormální) báze, kde každý z prvků má vždy na jedné informační pozici jedničku. Báze tedy bude vypadat takto

$$[1\ 0\ 0\ 0\ 0]^{\mathrm{T}}$$
$$[0\ 1\ 0\ 0\ 1]^{\mathrm{T}}$$
$$[0\ 0\ 1\ 0\ 1]^{\mathrm{T}}$$
$$[0\ 0\ 0\ 1\ 0]^{\mathrm{T}}$$

Budeme pracovat se sloupcovými vektory, proto jsou prvky báze zapsané s transpozicí.

Generující matici lineárního kódu vytvoříme tak, že do jejích řádků naskládáme bázové prvky.

$$G = \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}}_{n} \Bigg\} k$$

Počet řádků k je roven počtu informačních prvků kódu (tj. dimenzi lineárního prostoru). Počet sloupců n je roven počtu všech prvků kódu.

Označme u informační část (sloupec k prvků) a v kódovou značku (sloupec n prvků). Zakódování provedeme tak, že transponovanou generující matici vynásobíme informační částí

$$v = \mathbf{G}^{\mathrm{T}} \cdot u$$

Kontrolní rovnice je dána definicí lineárního prostoru $\boldsymbol{K}_1$

$$v_2 + v_3 = v_5$$

Upravíme rovnici tak, aby byla na pravé straně nula

$$v_2 + v_3 - v_5 = 0$$

Nad tělesem $\mathbb{Z}_2$ počítáme modulo 2, přičemž platí

$$-1 \bmod 2 = 1$$

Kontrolní rovnici tedy můžeme zapsat jako

$$v_2 + v_3 + v_5 = 0$$

Kontrolních rovnic je obecně $n - k$, tedy tolik, kolik je zabezpečovacích prvků. Zapíšeme-li soustavu kontrolních rovnic jako

$$\mathbf{H} \cdot v = \mathbf{0},$$

pak matici **H** nazveme kontrolní maticí lineárního kódu. V našem případě je

$$H = \underbrace{(0 \quad 1 \quad 1 \quad 0 \quad 1)}_{n} \Big\} n - k$$

Počet řádků $n - k$ je roven počtu zabezpečovacích prvků. Počet sloupců n je roven počtu všech prvků kódu.

Generující matici **G** můžeme rozdělit na bloky $\mathbf{G} = (\mathbf{I}_k \mid \mathbf{B})$, kde $\mathbf{I}_k$ je jednotková matice řádu k a **B** je blok za jednotkovou maticí. O takovém kódu říkáme, že je v *systematickém tvaru*. Kontrolní matice je pak tvořena bloky $\mathbf{H} = (-\mathbf{B}^{\mathrm{T}} \mid \mathbf{I}_{n-k})$, kde $-\mathbf{B}^{\mathrm{T}}$ je záporný transponovaný blok **B** z matice **G** a $\mathbf{I}_{n-k}$ je jednotková matice řádu $n - k$.