Domácí úkol č.2 - Lineární kódy

1. Ověřte, zda je binární kód lineární. Pokud ano, najděte pro něj generující a kontrolní matici.

   a) $K = \{(1\,1\,1\,1), (1\,0\,1\,0), (0\,1\,0\,1), (0\,0\,0\,0)\}$

   b) $K = \{\bar{v}$ délky 5, která mají právě 2 jedničky$\}$

2. Binární kód postupné kontroly parity délky 7 obsahuje všechna slova tvaru $\bar{v} = (a_1\,a_2\,b_1\,a_3\,a_4\,b_2\,b_3)$, kde a_i jsou informační znaky a b_i kontrolní znaky přidané tak, aby byla sudá parita v podslovech $(a_1\,a_2\,b_1)$ a $(a_3\,a_4\,b_2)$ a sudá parita v celém slově $\bar{v}$.

   a) Najděte generující a kontrolní matici tohoto kódu.

   b) Kolik chyb tento kód objevuje a kolik chyb opravuje? Která chybová slova kód objeví?

3. Kód ISBN (International Standard Book Number) je kód délky 10 nad $\mathbb{Z}_{11} = \{0, 1, \ldots, 9, X\}$ splňující rovnici:

$$\bar{v} \in K \quad \text{iff} \quad \sum_{i=1}^{10} i \cdot v_i = 0 \;\text{ v }\; \mathbb{Z}_{11}$$

   a) Doplňte kontrolní znak tak, aby vzniklo kódové slovo:

$$80 - 7113 - 175 - b_1$$

   b) Najděte kontrolní matici ISBN kódu.

   c) Najděte systematickou generující matici ISBN kódu.

4. Lineární $(6,2)$-kód K nad $\mathbb{Z}_5$ má generující matici $\mathbb{G} = \begin{pmatrix} 3 & 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$.

   a) Zakódujte informaci $\bar{a} = (1\,2)$.

   b) Najděte kontrolní matici $\mathbb{H}$.

   c) Zkontrolujte přijaté slovo $\bar{w} = (3\,3\,4\,2\,2\,2)$, popřípadě opravte chybu (předpokládáme, že nastala nejvýše jedna chyba).

   d) Kolik chyb objevuje a kolik chyb opravuje kód K?

5. Binární kód (dvourozměrné) křížové kontroly parity vznikne takto: s informačních slov délky d se napíše do sloupců matice typu $d \times s$. Přidají se znaky kontroly parity do každého řádku a do každého sloupce a ještě znak celkové kontroly parity. Vznikne tak matice typu $(d+1) \times (s+1)$.

   Maticový zápis můžeme převést na kódové slovo tak, že sloupce matice napíšeme do řádků za sebe, $\bar{v} = (S_1^T S_2^T \ldots S_{s+1}^T)$. Délka kódového slova je $n = (d+1)(s+1)$, počet informačních znaků $k = ds$.

   (Tím jsme popsali nejen kód, ale i kódování.)

   a) Kolik chyb tento kód objevuje a kolik opravuje?

   b) Jaká chybová slova mají jednoznačnou opravu? Navrhněte rozumné částečné dekódování.

   c) Napište kontrolní matici kódu křížové parity délky $n = 32$.

   Toto kódování se používá pro ukládání znaků v ASCII kódu. Původní ASCII kód má $2^7 = 128$ znaků, kterým odpovídají binární slova délky $d = 7$. Tři znaky ASCII kódu (tedy tři slova délky $d = 7$) se ukládají najednou jako slovo délky $n = 4 \cdot 8 = 32$ s použitím kódu křížové kontroly parity.

6. Napište kontrolní matici $\mathbb{H}$ pro ternální Hammingův kód (tj. nad $\mathbb{Z}_3$) se dvěma, resp. se třemi kontrolními znaky. Jak dlouhá budou kódová slova ternálního Hammingova kódu s m kontrolními znaky? Zobecněte postup pro Hammingovy kódy nad $\mathbb{Z}_p$.

Výsledky

1. a) ano (kód je uzavřen na součty i číselné násobky), $\mathbb{G} = \mathbb{H} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$,

   b) ne (kód neobsahuje nulové slovo)

2. $\mathbb{G} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$, $\mathbb{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$, kód odhaluje 1 chybu.

3. $v_{10} = X$, $\mathbb{H} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \end{pmatrix}$, $\mathbb{G} = \left(\begin{array}{c|c} & 1 \\ & 2 \\ \mathbb{E}_9 & \vdots \\ & 9 \end{array}\right)$.

4. $\bar{v} = (0\,4\,3\,2\,2\,2)$, $\mathbb{H} = \begin{pmatrix} 1 & 3 & 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 \\ 2 & 2 & 0 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix}$, $\bar{s} = \begin{pmatrix} 1 \\ 4 \\ 4 \\ 4 \end{pmatrix} = 2S_2$, tedy $\bar{v} = (3\,1\,4\,2\,2\,2)$.

   Kód objevuje 2 chyby a opravuje 1 chybu, protože každé dva sloupce v $\mathbb{H}$ jsou lineárně nezávislé.

5. a) Kód objevuje 3 chyby a opravuje 1 chybu, protože nenulové kódové slovo nejmenší váhy má Hammingovu váhu $||\bar{u}||_H = 4$.

   b) Chybová slova mající lichý počet 1 a všechny v jednom řádku (anebo naopak v jednom sloupci) umíme opravit, neboť známe pozice chyb. Částečné dekódování: Pokud je chybná parita pouze v jednom řádku (resp. sloupci), tak v něm oprav znaky na těch pozicích, kde je chybná sloupcová parita (resp. řádková parita). Poznámka: Toto dekódování opraví správně jednu chybu, více chyb už správně opravit nemusí.

   c) První tři řádky v H jsou z rovnic pro sudou parity ve třech sloupcích, dalších sedm řádků jsou z rovnic pro sudou parity v řádcích a poslední řádek je rovnice pro sudou parity v celém kódovém slově.

6. Pro $m = 2$ je $\mathbb{H} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$.

   Obecně pro m kontrolních znaků budou sloupce v $\mathbb{H}$ všechny nenulové m-tice nad $\mathbb{Z}_3$ s prvním nenulovým znakem rovným 1. Délka slov bude $n = \frac{3^m-1}{2}$. Analogicky vypadá $\mathbb{H}$ pro Hammingovy kódy nad $\mathbb{Z}_p$ s m kontrolními znaky, délka slov bude $n = \frac{p^m-1}{p-1}$.