

**Násobení matic v aritmetice modulo 2**

**A ⊗ B = C** Každý výsledek elementární operace (násobení nebo sčítání) se podělí dvěma a vezme se zbytek.

$$\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \end{bmatrix} \otimes \begin{bmatrix} b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} \\ b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} \\ b_{3,1} & b_{3,2} & b_{3,3} & b_{3,4} \end{bmatrix} = \begin{bmatrix} c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} \\ c_{2,1} & c_{2,2} & c_{2,3} & c_{2,4} \end{bmatrix}$$

$$c_{1,1} = a_{1,1} \otimes b_{1,1} \oplus a_{1,2} \otimes b_{2,1} \oplus a_{1,3} \otimes b_{3,1} \quad c_{1,2} = a_{1,1} \otimes b_{1,2} \oplus a_{1,2} \otimes b_{2,2} \oplus a_{1,3} \otimes b_{3,2} \quad c_{1,3} = a_{1,1} \otimes b_{1,3} \oplus a_{1,2} \otimes b_{2,3} \oplus a_{1,3} \otimes b_{3,3} \quad c_{1,4} = \dots$$

$$c_{2,1} = a_{2,1} \otimes b_{1,1} \oplus a_{2,2} \otimes b_{2,1} \oplus a_{2,3} \otimes b_{3,1} \quad c_{2,2} = a_{2,1} \otimes b_{1,2} \oplus a_{2,2} \otimes b_{2,2} \oplus a_{2,3} \otimes b_{3,2} \quad c_{2,3} = a_{2,1} \otimes b_{1,3} \oplus a_{2,2} \otimes b_{2,3} \oplus a_{2,3} \otimes b_{3,3} \quad c_{2,4} = \dots$$

V binární aritmetice modulo 2:

$a$	$b$	$a \otimes b$
0	0	0
0	1	0
1	0	0
1	1	1

⇒ jedná se o obyčejnou konjunkci (AND)

$a$	$b$	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

⇒ jedná se o exkluzivní disjunkci (XOR)

Př.:

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

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \quad (\text{Příklad zabezpečení sudou paritou}).$$

**Zadání a řešení vzorových příkladů na LB kódy**

1) Zabezpečte 3bitovou posloupnost  $\mathbf{p} = [1 \ 1 \ 0]$  lineárním blokovým kódem (7,3) definovaným generující maticí  $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$ .

$$\mathbf{f} = \mathbf{p} \otimes \mathbf{G} = [1 \ 1 \ 0] \otimes \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} = \underline{\underline{[1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1]}}$$

2) Zabezpečte posloupnost bitů 0 1 1 1 1 0 0 1 0 0 1 1 lineárním blokovým kódem definovaným generující maticí  $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$ .

Z rozměrů matice G vyplývá, že se jedná o LB kód (7,4), tudíž vstupní posloupnost musím rozdělit po 4 bitech: 0 1 1 1 | 1 0 0 1 | 0 0 1 1 .

$$\mathbf{F} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Zabezpečená posloupnost je 0 1 1 1 1 0 0 1 0 0 1 1 0 0 0 0 1 1 0 0 1.

- 3) Dekódujte přijatou posloupnost bitů 1 0 0 1 0 0 0 0 1 1 1 0 1 1 0 1 0 0 1 1, která byla na vysílací straně zakódována lineárním blokovým kódem definovaným generující maticí  $\mathbf{G}$ .

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

Z rozměrů matice  $\mathbf{G}$  vyplývá, že se jedná o LB kód (7,4), tudíž přijatou posloupnost musím rozdělit po 7 bitech: 1 0 0 1 0 0 0 | 0 0 1 1 1 0 1 | 1 0 1 0 0 1 1 .

$$\mathbf{s} = \mathbf{f}_p \otimes \mathbf{H}^T = [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0] \otimes \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 1] \Rightarrow \text{chyba ve 2. bitu}$$

← odpovídá 2. řádku matice  $\mathbf{H}^T$


$$\mathbf{f} = [1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0] \Rightarrow \mathbf{p} = [1 \ 1 \ 0 \ 1]$$

$$\mathbf{s} = \mathbf{f}_p \otimes \mathbf{H}^T = [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1] \otimes \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [1 \ 1 \ 1] \Rightarrow \text{chyba ve 3. bitu}$$

← odpovídá 3. řádku matice  $\mathbf{H}^T$

$$\mathbf{f} = [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1] \Rightarrow \mathbf{p} = [0 \ 0 \ 0 \ 1]$$

$$\mathbf{s} = \mathbf{f}_p \otimes \mathbf{H}^T = [1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1] \otimes \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 0] \Rightarrow \text{chyba v 6. bitu}$$


 odpovídá 6. řádku matice  $\mathbf{H}^T$

$$\mathbf{f} = [1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1] \Rightarrow \mathbf{p} = [1 \ 0 \ 1 \ 0]$$

Dekódovaná posloupnost je 1 1 0 1 0 0 0 1 1 0 1 0.