Diskrétní matematika – cvičení 7. týden

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

jaro 2020

Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

Řešení

$$\begin{tikzcd}
01 \arrow[r, dash] \arrow[d, dash] & 11 \arrow[d, dash] \\
00 \arrow[r, dash] & 10
\end{tikzcd}$$

Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

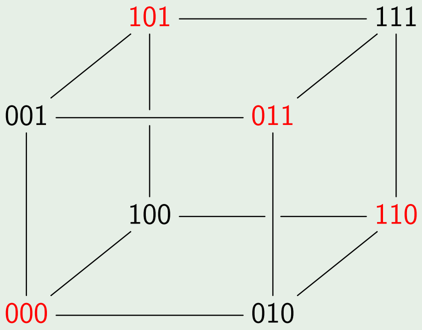
Řešení

$$
\begin{tikzcd}
01 \arrow[r, dash] \arrow[d, dash] & 11 \arrow[d, dash] \\
00 \arrow[r, dash] & 10
\end{tikzcd}
$$

Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

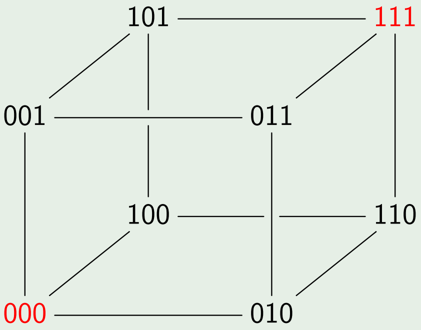
Řešení



Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

Řešení



Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

Řešení

Jestliže má kód opravovat jednoduché chyby, musí být okolí kódových slov poloměru 1 disjunktní (tj. slova musí mít vzdálensot alespoň 3). Jestliže jsou kódová slova délky ℓ, pak takové okolí obsahuje právě $\ell + 1$ slov. Musí proto být

$$4(\ell + 1) \leq 2^\ell$$

(2^ℓ je počet všech slov délky ℓ), což přímým ověřením neplatí pro $\ell = 1, 2, 3, 4$. Jako nejmenší ℓ tedy v úvahu připadá $\ell = 5$. Ukážeme nyní, jak kódová slova délky 5 lze volit.

Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

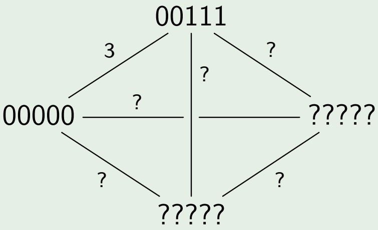
Řešení

První můžeme (bez újmy na obecnosti) volit jako 00000. Protože zjevně každá dvě slova ve vzdálenosti 4 (tj. mající 4 jedničky a 1 nulu) jsou od sebe vzdálena 2 (z oněch 4 jedniček budou vždy přesně 3 společné), musí mít zbylá slova od našeho prvního vzdálenosti 3, 3, 4 (snadno si lze rozmyslet, že v případě 3, 3, 3 by pak tato slova musela být vzájemně vzdálena o 4 a to podle předchozího nelze).

Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

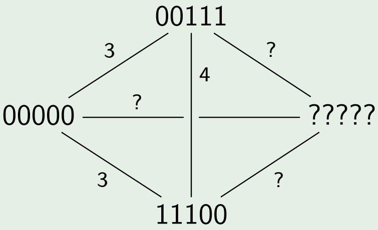
Řešení



Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

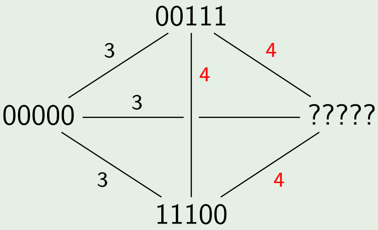
Řešení



Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

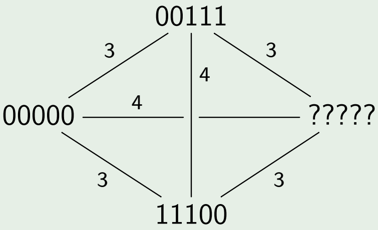
Řešení



Příklad

Množinu čtyř slov chceme přenášet binárním kódem opravujícím jednoduché chyby. Jakou nejménší délku slov (chceme pro všechna slova stejnou) můžeme mít? Udejte příklad takových čtyřech slov.

Řešení



Příklad

Vysvětlete $(5,3)$-kód nad $\mathbb{Z}/2$ generovaný polynomem $x^2 + x + 1$. Vypište všechna kódová slova, najděte generující matici a matici kontroly parity.

Příklad

Vysvětlete $(5,3)$-kód nad $\mathbb{Z}/2$ generovaný polynomem $x^2 + x + 1$. Vypište všechna kódová slova, najděte generující matici a matici kontroly parity.

Řešení

Zprávu i kódová slova (pro $(5,3)$-kód mají zprávy délku 3 a kódová slova délku 5) zapisujeme jako vektory skládající se z 0 a 1 a budeme s nimi tedy počítat modulo 2 (např. $101 + 110 = 011$, tj. XOR). Standardně kódové slovo vznikne ze zprávy tím, že k ní přidáme (zleva) tzv. kontrolní bity: například kontrola parity

$$11001 \mapsto 1|11001, \qquad 10111 \mapsto 0|10111;$$

tedy kódová slova jsou právě vektory obsahující sudý počet jedniček.

Řešení

V případě kódu generovaného polynomem $p = 1 + x + x^2$: slova ztotožňujeme s polynomy, konkrétně polynom chápeme jako vektor jeho koeficientů a stále je bereme modulo 2, např. $1 + x^2 + x^3$ odpovídá $10|110$ (koeficienty postupně od x^0 do x^4, aby jich bylo 5). Kódovými slovy jsou právě polynomy dělitelné polynomem p, tj. právě násobky polynomu p (počítáme modulo 2):

$$
\begin{aligned}
0 \cdot (1 + x + x^2) &= 0 & 00|000 \\
1 \cdot (1 + x + x^2) &= 1 + x + x^2 & 11|100 \\
x \cdot (1 + x + x^2) &= x + x^2 + x^3 & 01|110 \\
(1 + x) \cdot (1 + x + x^2) &= 1 + x^3 & 10|010 \\
x^2 \cdot (1 + x + x^2) &= x^2 + x^3 + x^4 & 00|111 \\
(1 + x^2) \cdot (1 + x + x^2) &= 1 + x + x^3 + x^4 & 11|011 \\
(x + x^2) \cdot (1 + x + x^2) &= x + x^4 & 01|001 \\
(1 + x + x^2) \cdot (1 + x + x^2) &= 1 + x^2 + x^4 & 10|101
\end{aligned}
$$

Řešení

Lineární kód (např. kontrola parity nebo kód generovaný polynomem) je dán násobením maticí G, která je pro $(5,3)$-kód rozměrů 5×3 a standardně je v následujícím tvaru s tzv. maticí kontroly H (jejíž význam si vysvětlíme později):

$$G = \begin{pmatrix} P \\ \hline E \end{pmatrix} = \left(\begin{array}{cccc} ? & \cdots & \cdots & ? \\ \vdots & \ddots & \ddots & \vdots \\ ? & \cdots & \cdots & ? \\ \hline 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{array}\right), \qquad H = \left(E \mid P\right)$$

Řešení

$$
\begin{aligned}
1 \cdot (1 + x + x^2) &= 1 + x + x^2 & \qquad 11|100 \\
(1 + x) \cdot (1 + x + x^2) &= 1 + x^3 & \qquad 10|010 \\
(x + x^2) \cdot (1 + x + x^2) &= x + x^4 & \qquad 01|001
\end{aligned}
$$

Kód generovaný polynomem je lineární. V našem případě tedy:

$$
G \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \left(\begin{array}{c} 1 \\ 1 \\ \hline 1 \\ 0 \\ 0 \end{array}\right), \qquad
G \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \left(\begin{array}{c} 1 \\ 0 \\ \hline 0 \\ 1 \\ 0 \end{array}\right), \qquad
G \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \left(\begin{array}{c} 0 \\ 1 \\ \hline 0 \\ 0 \\ 1 \end{array}\right)
$$

Řešení

$$G \cdot \begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\1\\\hline 1\\0\\0\end{pmatrix}, \qquad G \cdot \begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\\hline 0\\1\\0\end{pmatrix}, \qquad G \cdot \begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\\hline 0\\0\\1\end{pmatrix}$$

Protože to jsou postupně sloupce matice G, máme tak:

$$G = \begin{pmatrix}1 & 1 & 0\\1 & 0 & 1\\\hline 1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}, \qquad H = \left(\begin{array}{cc|ccc}1 & 0 & 1 & 1 & 0\\0 & 1 & 1 & 0 & 1\end{array}\right)$$

Řešení

Prvně vysvětlíme algoritmický postup pro $p = 1 + x^2$:

$$G = \begin{pmatrix} 1 & ? & ? & \\ 0 & ? & ? & \\ 1 & ? & ? & \\ 0 & ? & ? & \\ 0 & ? & ? & \end{pmatrix}$$

Řešení

Prvně vysvětlíme algoritmický postup pro $p = 1 + x^2$:

$$G = \begin{pmatrix} 1 & 0 & ? & \\ 0 & 1 & ? & \\ 1 & 0 & ? & \\ 0 & 1 & ? & \\ 0 & 0 & ? & \end{pmatrix}$$

Řešení

Prvně vysvětlíme algoritmický postup pro $p = 1 + x^2$:

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

Řešení

Prvně vysvětlíme algoritmický postup pro $p = 1 + x^2$:

$$G = \begin{pmatrix} 1 & 0 & 0 + {\color{red}1} = 1 \\ 0 & 1 & 0 + {\color{red}0} = 0 \\ 1 & 0 & 1 + {\color{red}1} = 0 \\ 0 & 1 & 0 + {\color{red}0} = 0 \\ 0 & 0 & 1 + {\color{red}0} = 1 \end{pmatrix}$$

Řešení

Prvně vysvětlíme algoritmický postup pro $p = 1 + x^2$:

$$G = \begin{pmatrix} \boxed{1} & \boxed{0} & 0+1=\boxed{1} \\ \boxed{0} & \boxed{1} & 0+0=\boxed{0} \\ \boxed{1} & \boxed{0} & 1+1=\boxed{0} \\ \boxed{0} & \boxed{1} & 0+0=\boxed{0} \\ \boxed{0} & \boxed{0} & 1+0=\boxed{1} \end{pmatrix}$$

Řešení

Nyní ukážeme algoritmický postup pro $p = 1 + x + x^2$:

$$G = \begin{pmatrix} 1 & ? & ? \\ 1 & ? & ? \\ 1 & ? & ? \\ 0 & ? & ? \\ 0 & ? & ? \end{pmatrix}$$

Řešení

Nyní ukážeme algoritmický postup pro $p = 1 + x + x^2$:

$$G = \begin{pmatrix} 1 & 0 & ? \\ 1 & 1 & ? \\ 1 & 1 & ? \\ 0 & 1 & ? \\ 0 & 0 & ? \end{pmatrix}$$

Řešení

Nyní ukážeme algoritmický postup pro $p = 1 + x + x^2$:

$$G = \begin{pmatrix} 1 & 0 + 1 = 1 & ? \\ 1 & 1 + 1 = 0 & ? \\ 1 & 1 + 1 = 0 & ? \\ 0 & 1 + 0 = 1 & ? \\ 0 & 0 + 0 = 0 & ? \end{pmatrix}$$

Řešení

Nyní ukážeme algoritmický postup pro $p = 1 + x + x^2$:

$$G = \begin{pmatrix} 1 & 0+1=1 & 0 \\ 1 & 1+1=0 & 1 \\ 1 & 1+1=0 & 0 \\ 0 & 1+0=1 & 0 \\ 0 & 0+0=0 & 1 \end{pmatrix}$$

Řešení

Nyní ukážeme algoritmický postup pro $p = 1 + x + x^2$:

$$G = \begin{pmatrix} \boxed{1} & 0+1=\boxed{1} & \boxed{0} \\ \boxed{1} & 1+1=\boxed{0} & \boxed{1} \\ \boxed{1} & 1+1=\boxed{0} & \boxed{0} \\ \boxed{0} & 1+0=\boxed{1} & \boxed{0} \\ \boxed{0} & 0+0=\boxed{0} & \boxed{1} \end{pmatrix}$$

Příklad

V předchozím kódu zakódujte zprávu 101.

Příklad

V předchozím kódu zakódujte zprávu 101.

Řešení

Připomeňme, že kódování se realizuje násobením maticí kódu, tj. v našem případě:

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \left(\begin{array}{c} 1 \\ 0 \\ \hline 1 \\ 0 \\ 1 \end{array}\right)$$

Příklad

V předchozím kódu zakódujte zprávu 101.

Řešení

Připomeňme, že kódování se realizuje násobením maticí kódu, tj. v našem případě:

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \left(\begin{array}{c} 1 \\ 0 \\ \hline 1 \\ 0 \\ 1 \end{array}\right)$$

Příklad

V předchozím kódu zakódujte zprávu 101.

Řešení

Připomeňme, že kódování se realizuje násobením maticí kódu, tj. v našem případě:

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \hline 1 \\ 0 \\ 1 \end{pmatrix}$$

Příklad

V předchozím kódu zakódujte zprávu 101.

Řešení

Připomeňme, že kódování se realizuje násobením maticí kódu, tj. v našem případě:

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline \color{red}{1} & \color{red}{0} & \color{red}{0} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \cdot \begin{pmatrix} \color{red}{1} \\ \color{red}{0} \\ \color{red}{1} \end{pmatrix} = \left(\begin{array}{c} 1 \\ 0 \\ \hline \color{red}{1} \\ 0 \\ 1 \end{array}\right)$$

Příklad

V předchozím kódu zakódujte zprávu 101.

Řešení

Připomeňme, že kódování se realizuje násobením maticí kódu, tj. v našem případě:

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ \color{red}{0} & \color{red}{1} & \color{red}{0} \\ 0 & 0 & 1 \end{array}\right) \cdot \begin{pmatrix} \color{red}{1} \\ \color{red}{0} \\ \color{red}{1} \end{pmatrix} = \left(\begin{array}{c} 1 \\ 0 \\ \hline 1 \\ \color{red}{0} \\ 1 \end{array}\right)$$

Příklad

V předchozím kódu zakódujte zprávu 101.

Řešení

Připomeňme, že kódování se realizuje násobením maticí kódu, tj. v našem případě:

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ \color{red}{0} & \color{red}{0} & \color{red}{1} \end{pmatrix} \cdot \begin{pmatrix} \color{red}{1} \\ \color{red}{0} \\ \color{red}{1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \hline 1 \\ 0 \\ \color{red}{1} \end{pmatrix}$$

Příklad

V předchozím kódu zakódujte zprávu 101.

Řešení

Připomeňme, že kódování se realizuje násobením maticí kódu, tj. v našem případě:

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \hline 1 \\ 0 \\ 1 \end{pmatrix}$$

V každém případě si povšimněme, že všechna kódová slova vzniknou tak, že sečteme některé sloupce matice G.

Příklad

Vysvětlete, jak polynom $x + 1$ generuje pro všechna $n \geq 1$ známý $(n+1, n)$-kód kontroly parity.

Příklad

Vysvětlete, jak polynom $x+1$ generuje pro všechna $n \geq 1$ známý $(n+1, n)$-kód kontroly parity.

Řešení

Podle předchozího postupu lze snadno sestavit matici kódu:

$$G = \left(\begin{array}{ccccc}
\boxed{1} & 0+1=\boxed{1} & 0+1=\boxed{1} & \cdots & 0+1=\boxed{1} \\
\hline
\boxed{1} & 1+1=\boxed{0} & 1+1=\boxed{0} & \cdots & 1+1=\boxed{0} \\
\boxed{0} & 1+0=\boxed{1} & 0+0=\boxed{0} & \cdots & 0+0=\boxed{0} \\
\boxed{0} & 0+0=\boxed{0} & 1+0=\boxed{1} & \cdots & 0+0=\boxed{0} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\boxed{0} & 0+0=\boxed{0} & 0+0=\boxed{0} & \cdots & 1+0=\boxed{1}
\end{array}\right)$$

Řešení

O něco přehledněji:

$$G = \left(\begin{array}{ccc} 1 & \cdots & 1 \\ \hline 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{array}\right)$$

a tím pádem:

$$G \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \left(\begin{array}{ccc} 1 & \cdots & 1 \\ \hline 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{array}\right) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \left(\begin{array}{c} a_1 + \cdots + a_n \\ \hline a_1 \\ \vdots \\ a_n \end{array}\right)$$

přičemž evidentně $(a_1 + \cdots a_n) + a_1 + \cdots + a_n \equiv 0 \pmod 2$ a tedy počet jedniček v kódovém slově je vždy sudý.

Příklad

Uvažujme $(7, 3)$-kód generovaný polynomem $x^4 + x^3 + x + 1$. Napište jeho generující a kontrolní matice. Metodou vedoucích reprezentantů dékodujte přijatou zprávu 0110010, za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Příklad

Uvažujme $(7,3)$-kód generovaný polynomem $x^4 + x^3 + x + 1$. Napište jeho generující a kontrolní matice. Metodou vedoucích reprezentantů dékodujte přijatou zprávu 0110010, za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Řešení

Podle předchozího postupu lze snadno sestavit matici kódu:

$$G = \left(\begin{array}{ccc} \boxed{1} & 0+1=\boxed{1} & 0+1=\boxed{1} \\ \boxed{1} & 1+1=\boxed{0} & 1+1=\boxed{0} \\ \boxed{0} & 1+0=\boxed{1} & 0+0=\boxed{0} \\ \boxed{1} & 0+1=\boxed{1} & 1+1=\boxed{0} \\ \hline \boxed{1} & 1+1=\boxed{0} & 1+1=\boxed{0} \\ \boxed{0} & 1+0=\boxed{1} & 0+0=\boxed{0} \\ \boxed{0} & 0+0=\boxed{0} & 1+0=\boxed{1} \end{array}\right)$$

Řešení

O něco přehledněji:

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Budeme-li chvíli předpokládat, že přijaté slovo 0110|010 je kódové, musí se nutně jednat o kódové slovo odpovídající zprávě 010 (ta je obsažena v informačních bitech). Tomu však ve skutečnosti odpovídá jiné kódové slovo:

Řešení

$$G \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \left(\begin{array}{c} 1 \\ 0 \\ 1 \\ 1 \\ \hline 0 \\ 1 \\ 0 \end{array}\right) \neq \left(\begin{array}{c} 0 \\ 1 \\ 1 \\ 0 \\ \hline 0 \\ 1 \\ 0 \end{array}\right).$$

Řešení

$$G \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ \hline 0 \\ 1 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ \hline 0 \\ 1 \\ 0 \end{pmatrix}.$$

Mohlo se samozřejmě stát, že vskutku bylo posláno toto kódové slovo a při přenosu došlo k chybě na bitech 1, 2 a 4:

Řešení

$$
G \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \left(\begin{array}{c} 1 \\ 0 \\ 1 \\ 1 \\ \hline 0 \\ 1 \\ 0 \end{array}\right) \neq \left(\begin{array}{c} 0 \\ 1 \\ 1 \\ 0 \\ \hline 0 \\ 1 \\ 0 \end{array}\right).
$$

Mohlo se samozřejmě stát, že vskutku bylo posláno toto kódové slovo a při přenosu došlo k chybě na bitech 1, 2 a 4:

$$
\left(\begin{array}{c} 0 \\ 1 \\ 1 \\ 0 \\ \hline 0 \\ 1 \\ 0 \end{array}\right) = \left(\begin{array}{c} 1 \\ 0 \\ 1 \\ 1 \\ \hline 0 \\ 1 \\ 0 \end{array}\right) + \left(\begin{array}{c} 1 \\ 1 \\ 0 \\ 1 \\ \hline 0 \\ 0 \\ 0 \end{array}\right).
$$

Jiné možnosti dostaneme pozměněním kódového slova přičtením nějakých sloupců matice G. Za každý sloupec přibude chyba v informačním bitu $\Rightarrow$ prvně jednotlivé sloupce.

Řešení

První sloupec:

$$
\begin{pmatrix} 0\\1\\1\\0\\ \hline 0\\1\\0 \end{pmatrix}
=
\left(
\begin{pmatrix} 1\\0\\1\\1\\ \hline 0\\1\\0 \end{pmatrix}
+
{\color{red}\begin{pmatrix} 1\\1\\0\\1\\ \hline 1\\0\\0 \end{pmatrix}}
\right)
+
\left(
\begin{pmatrix} 1\\1\\0\\1\\ \hline 0\\0\\0 \end{pmatrix}
+
{\color{red}\begin{pmatrix} 1\\1\\0\\1\\ \hline 1\\0\\0 \end{pmatrix}}
\right)
=
\begin{pmatrix} 0\\1\\1\\0\\ \hline 1\\1\\0 \end{pmatrix}
+
\begin{pmatrix} 0\\0\\0\\0\\ \hline 1\\0\\0 \end{pmatrix}
$$

Řešení

Druhý sloupec:

$$\begin{pmatrix}0\\1\\1\\0\\\hline 0\\1\\0\end{pmatrix} = \left(\begin{pmatrix}1\\0\\1\\1\\\hline 0\\1\\0\end{pmatrix} + \color{red}{\begin{pmatrix}1\\0\\1\\1\\\hline 0\\1\\0\end{pmatrix}}\right) + \left(\begin{pmatrix}1\\1\\0\\1\\\hline 0\\0\\0\end{pmatrix} + \color{red}{\begin{pmatrix}1\\0\\1\\1\\\hline 0\\1\\0\end{pmatrix}}\right) = \begin{pmatrix}0\\0\\0\\0\\\hline 0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\1\\1\\0\\\hline 0\\1\\0\end{pmatrix}$$

Řešení

Třetí sloupec:

$$\left(\begin{array}{c}0\\1\\1\\0\\\hline 0\\1\\0\end{array}\right) = \left(\left(\begin{array}{c}1\\0\\1\\1\\\hline 0\\1\\0\end{array}\right) + {\color{red}\left(\begin{array}{c}1\\0\\0\\0\\\hline 0\\0\\1\end{array}\right)}\right) + \left(\left(\begin{array}{c}1\\1\\0\\1\\\hline 0\\0\\0\end{array}\right) + {\color{red}\left(\begin{array}{c}1\\0\\0\\0\\\hline 0\\0\\1\end{array}\right)}\right) = \left(\begin{array}{c}0\\0\\1\\1\\\hline 0\\1\\1\end{array}\right) + \left(\begin{array}{c}0\\1\\0\\1\\\hline 0\\0\\1\end{array}\right)$$

Řešení

Našli jsme čtyři možnosti, zbylé vzniknou přičítáním alespoň dvojice sloupců a odpovídají tedy alespoň dvojnásobným chybám. Mezi čtyřmi možnostmi se vyskytuje jednoduchá chyba, je tedy řešením úlohy:

$$\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ \hline 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ \hline 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \hline 1 \\ 0 \\ 0 \end{pmatrix}$$

kde levá strana je přijaté slovo, první vektor napravo je odeslané slovo $0110|110$ a druhý vektor napravo je chyba, ke které došlo při přenosu.

Poznámka

K čemu je kontrolní matice H? Předchozí způsob lze také zapisovat takto: K danému obdrženému slovu spočítáme tzv. syndrom

$$H \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ \hline 0 \\ 1 \\ 0 \end{pmatrix} = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right) \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ \hline 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

který je roven kontrolním bitům iniciální chyby (ta s informačními bity nulovými).

Příklad

V lineárním $(7,4)$-kódu zadaném maticí

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

byly přijaty zprávy $101|0001$ a $100|1110$. Dekódujte je (tj. nalezněte odesílané zprávy) za předpokladu, že při přenosu každého slova došlo k nejmenšímu možnému počtu chyb.

Řešení

Pro první potenciální zprávu 0001 ze zadání (informační bity přijatého slova) dostáváme kódové slovo

$$\left(\begin{array}{cccc} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \left(\begin{array}{c} 0 \\ 1 \\ 1 \\ \hline 0 \\ 0 \\ 0 \\ 1 \end{array}\right); \qquad \left(\begin{array}{c} 1 \\ 0 \\ 1 \\ \hline 0 \\ 0 \\ 0 \\ 1 \end{array}\right) = \left(\begin{array}{c} 0 \\ 1 \\ 1 \\ \hline 0 \\ 0 \\ 0 \\ 1 \end{array}\right) + \left(\begin{array}{c} 1 \\ 1 \\ 0 \\ \hline 0 \\ 0 \\ 0 \\ 0 \end{array}\right)$$

a liší se od přijatého slova. Zjevně se vyplatí přičíst druhý sloupec:

Řešení

$$\begin{pmatrix}1\\0\\1\\\hline 0\\0\\0\\1\end{pmatrix} = \left(\begin{pmatrix}0\\1\\1\\\hline 0\\0\\0\\1\end{pmatrix} + \color{red}{\begin{pmatrix}1\\1\\0\\\hline 0\\1\\0\\0\end{pmatrix}}\right) + \left(\begin{pmatrix}1\\1\\0\\\hline 0\\0\\0\\0\end{pmatrix} + \color{red}{\begin{pmatrix}1\\1\\0\\\hline 0\\1\\0\\0\end{pmatrix}}\right) = \begin{pmatrix}1\\0\\1\\\hline 0\\1\\0\\1\end{pmatrix} + \begin{pmatrix}0\\0\\0\\\hline 0\\1\\0\\0\end{pmatrix}$$

Přičtením jiných sloupců jedné chyby nedocílíme, přičtením dvou a více vznikne alespoň dovjnásobná chyba. Jedná se tedy o optimální "rozklad" na odeslané slovo a chybu.

Řešení

Pro druhou potenciální zprávu 1110 ze zadání (informační bity přijatého slova) dostáváme kódové slovo

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \hline 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}; \qquad \begin{pmatrix} 1 \\ 0 \\ 0 \\ \hline 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \hline 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ \hline 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

a liší se od přijatého slova. Přičteném žádného sloupce se nepodaří počet chyb snížit oproti výše uvedené možnosti jednoduché chyby. Poslaná slova tedy jsou: $101|0101$ a $000|1110$ a původní zprávy pak 0101 a 1110.