1) $\big((A\wedge B)'\wedge C'\big)\wedge\big(A'\vee(B\wedge C'\wedge D)\big) =$

$= (A'\vee B')\wedge C'\wedge\big(A'\vee(B\wedge C'\wedge D)\big)$

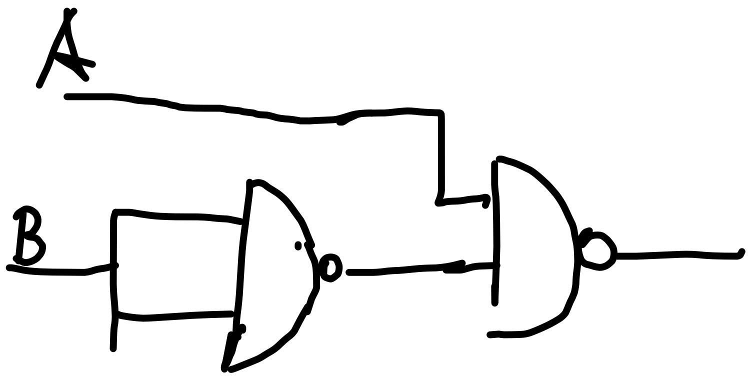
$= \big((A'\wedge C')\vee(B'\wedge C')\big)\wedge\big((A'\vee B)\wedge(A'\vee C')\wedge(A'\vee D)\big)$

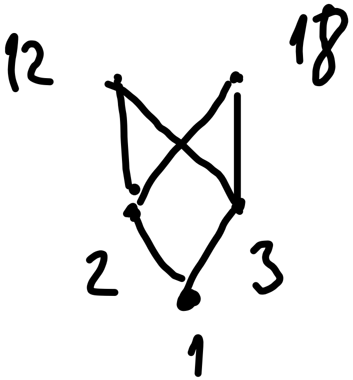
$= \underline{A'\wedge C'}$

$(\sim A'\wedge C'\wedge B\wedge D \vee (A'\wedge C'\wedge B'\wedge D)\vee(A'\wedge C'\wedge B\wedge D')$

$\vee\,(A'\wedge C'\wedge B'\wedge D'))$

$$(A \Rightarrow B) = A' \vee B = (A \wedge B')'$$





Lineární kódy

Typu (n, k) .... kódová slova mají délku n (bitovou)
kódujeme k-bitové zprávy (slova)

Kód generovaný polynomem $\left(x^3+x+1 =: p(x)\right)$

Zprávu interpretujeme jako polynom $\underbrace{1+x}_{z(x)}\ (+0\cdot x^2+0\cdot x^3)$

1100

$$b_1 \dots b_k \sim b_1 + b_2 x + b_3 x^2 + \dots + b_k x^{k-1}$$

Kódové slovo pak odpovídá polynomu

$z(x)\cdot x^3 + r(x)$, kde $r(x)$ je zbytek polynomu $z(x)\cdot x^3$ po dělení polynomem $p(x)$

Spočítáme zbytek polynomu $x^3(x+1)$ po dělení polynomem $p(x)=x^3+x+1$:

$$
\begin{array}{l}
x^4+x^3 : x^3+x+1 = x+1 \\
\underline{x^4+x^2+x} \\
\quad x^3+x^2+x \\
\quad \underline{x^3+x+1} \\
\qquad \underbrace{x^2+1}_{r(x)} =
\end{array}
$$

Kódový polynom je $x^4+x^3+x^2+1$, což odpovídá kódovému slovu $\underbrace{101}_{r(x)}\underbrace{1100}_{a(x)\cdot x^3}$

$11001 \sim 1+x+x^4$

Zjistíme zbytek $x^3(1+x+x^4)$ po dělení polynomem $1+x+x^3$:

$$
\begin{array}{l}
x^7 : x^3+x+1 = x^4+x^2+x+1 \\
\underline{x^7+x^5+x^4} \\
\quad x^5+x^4 \\
\quad \underline{x^5+x^3+x^2} \\
\qquad x^4+x^3+x^2 \\
\qquad \underline{x^4+x^2+x} \\
\qquad\quad x^3+x \\
\qquad\quad \underline{x^3+x+1} \\
\qquad\qquad 1
\end{array}
$$

zbytek $x^7+x^4+x^3$ je $1+x^2+1 = x^2$

$\Longrightarrow$ kódový polynom je 00111001

Lineární kód typu (n, k) je lin. zobrazení

$$(\mathbb{Z}_2)^k \longrightarrow (\mathbb{Z}_2)^n.$$

Kód ~ lineárním zobr. ~ matice

Stačí určit obrazy bázových vektorů

(1000), (0100), (0010), (0001)

tj. polynomů $1, x, x^2, x^3$, tedy zbytků polynomů

x^3, x^4, x^5, x^6 po dělení polynomem $\underbrace{x^3+x+1}_{p(x)}$:

$$x^3 \equiv x+1 \quad (p(x))$$

$$x^4 = x \cdot (x^3) \equiv x(x+1) = x^2+x \quad (p(x))$$

$$x^5 = x \cdot x^4 \equiv x^3 + x^2 \equiv x^2+x+1 \quad (p(x))$$

$$x^6 \equiv x(x^5) \equiv x(x^2+x+1) = x^3+x^2+x \equiv x^2+1 \quad (f(x))$$

Tedy matice daného lin. zobrazení je :

$$
G = \begin{array}{c} x^3 \quad x^4 \quad x^5 \quad x^6 \\ \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}
$$

$(1000) \longmapsto (1101000)$

?

1

2

$x^3 \quad \dots (x+1)$

$(0100) \longmapsto (0110100)$

$(0010) \longmapsto (1110010)$

$(0001) \longmapsto (1010001)$

Detekce chyb

Kontrolní matice H

$$G = \begin{pmatrix} P \\ \mathbb{E}_4 \end{pmatrix} \Rightarrow H = \begin{pmatrix} \mathbb{E}_3 & P \end{pmatrix}$$

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

$$H \cdot G = P + P = 0$$

$$H \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ je kódové slovo}$$

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

$$H \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \leftarrow \text{syndrom}$$

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

syndrom \ kód. slovo								
(000)	(000000)	(110100)	(011010)	(111001)	(101110)	(001101)	(100011)	(010111)
(001)	(001000)	(111100)	(010010)	(110001)	(100110)	(000101)	(101011)	(011111)
(010)	(010000)	(100100)	(001010)	(101001)	(111110)	(011101)	(110011)	(000111)
⋮								
(111)	(111000)	(001100)	(100010)	(000001)	(010110)	(110101)	(011011)	(101111)

Na každém řádku jsou červeně vyznačeni tzv. vedoucí representanti slov s daným syndromem, jsou to slova s nejmenším počtem jedniček z daného řádku a zároveň tedy udávají minimální vzdálenost slov na daném řádku od některého kódového slova.

Př. Syndrom daného slova (110101) je

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

Odečtením vedoucího representanta slov se syndromem (111) od přijatého slova dc dostaneme kódové slovo s minimální Hamingovou vzdáleností od přijatého slova, tj. kódové slovo, které bylo pravděpodobně odesláno, v našem případě tedy slovo $(110101 - \underbrace{000001}_{\text{vedoucí reprezentant}}) = 110100$,

tzn. pravděpodobně byla poslána zpráva 100.