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

Kdy je tento výraz pravdivý?

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

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

pravdivý pouze pokud $\Rightarrow A' = 1$

$C' = 1$

"0"

0

$$= A' \wedge C' = (A' \wedge C' \wedge B \wedge D) \vee (A' \wedge C' \wedge B' \wedge 0)$$

Zpráva má 7 bitů, odpovídá polynomu

$$a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

$a_i = 0, 1 \quad (\in \mathbb{Z}_2)$

$a_3 a_4 a_5 a_6$ – zpráva

a_0, a_1, a_2 – kontrolní bity

Konvence: zprávu zapisujeme od a_0.
(čtení zleva)

$1 \; x^1 \; x^2 \; x^3$

Kód zprávy 1010 bude kódový slovo

$\underbrace{(1+x^2)x^3}_{p(x)} + r(p(x))$

Pokračujeme zjištěním $r(P(x))$, tj. zbytek polynomu $(1+x^2)x^3 = x^3+x^5$ po dělení generujícím polynomem x^3+1

$$x^5+x^3 : x^3+1 = \underline{\underline{x^2+1}} \leftarrow \text{celý podíl}$$

$$\begin{array}{r} x^5+x^2 \\ \hline x^3+x^2 \\ x^3+1 \\ \hline \underline{\underline{x^2+1}} \end{array} \leftarrow \text{zbytek po dělení}$$

$$x^5+x^3 = (x^3+1)(x^2+1) + x^2+1 = x^5+x^2+x^3+1+x^2+1 = x^5+x^3$$

Kódové slovo odpovídá polynomu $x^5+x^3+x^2+1$

Tedy je tvaru $1011\underbrace{010}$

10111 kódujeme (7,5) kódem generovaným polynomem x^2+x+1:

$$\underbrace{10111}_{r(x)} \sim \underbrace{1+x^2+x^3+x^4}_{r(x)}$$

$$P(x) = r(x)\cdot x^2 = x^6+x^5+x^4+x^2$$

Získáme zbytek $P(x)$ po dělení polynomem $1+x+x^2$

$$x^6+x^5+x^4+x^2 : x^2+x+1 = x^4+1$$

$$\begin{array}{r} x^6+x^5+x^4 \\ \hline x^2 \\ x^2+x+1 \\ \hline x+1 \end{array}$$

Kódový polynom je $1+x+x^2+x^4+x^5+x^6$, kódové slovo je tedy

$$1\,1\,1\,0\,1\,1\,1$$

Lineární kód představuje lin. zobrazení f

(n, k)

$$f : (\mathbb{Z}_2)^k \to (\mathbb{Z}_2)^n.$$

Generující matice kódu je matice kohokoli lineárního zobrazení ve standardní bázi.

Potřebujeme zjistit na co jaká slova se mám zakódovat vektory ze st. báze $\mathbb{Z}_2^4$

tj. vektory (zprávy) 1000, 0100, 0010, 0001

$1000 \sim x^5$
$0100 \sim x^6$
$0010 \sim x^7$
$0001 \sim x^8$

$x^5 : x^5 + x^4 + x^2 + 1 = 1$

$x^4 + x^2 + 1$

$x^6 \equiv x\,(x^4 + x^2 + 1) = x^5 + x^3 + x : x^4 + x^3 + x^2 + x + 1$

$x^7 \equiv x\,(x^6) \overset{x^5}{=} x^5 + x^4 + x^3 + x^2 + x \equiv x^3 + x + 1$

$x^8 \equiv x^4 + x^2 + x$

$x^5 \rightsquigarrow 1 + x^2 + x^3 + x^5$

$x^6 \rightsquigarrow 1 + x + x^2 + x^3 + x^4 + x^6$

$x^7 \rightsquigarrow 1 + x + x^3 + x^7$

$x^8 \rightsquigarrow x + x^2 + x^4 + x^8$

$1000 \rightsquigarrow 101011000$

$0100 \rightsquigarrow 111110100$

$0010 \rightsquigarrow 110100010$

$0001 \rightsquigarrow 011010001$

$G = \begin{pmatrix} P \\ Id \end{pmatrix} \Rightarrow \mathcal{G} =$

$\begin{pmatrix} 1&1&1&0 \\ 0&1&1&1 \\ 1&1&0&1 \\ 0&1&1&0 \\ 1&1&0&1 \\ \hline 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = (100001110)$

$8 \times 8 \sim Id_8$

Matice kontroly parity, reprezentují ~~tzv~~ lin. zobrazení z prostoru $\mathbb{Z}_2^q$ všech možných (i nesprávných) kódů do prostoru "chyb". V našem případě $H \sim g : (\mathbb{Z}_2)^9 \to (\mathbb{Z}_2)^5$

$$H = (Id_5 | P) = \left(\begin{array}{ccccc|c} 1&0&0&0&0&1&1&1&0 \\ 0&1&0&0&0&0&1&1&1 \\ 0&0&1&0&0&1&1&0&1 \\ 0&0&0&1&0&0&1&1&0 \\ 0&0&0&0&1&1&1&0&1 \end{array}\right) \left|\begin{array}{c} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{array}\right. = (10110)$$

$$H \cdot G = (Id_5 | P) \cdot \begin{pmatrix} P \\ Id_4 \end{pmatrix} = P + P = 0 \qquad \neq (00000)$$

$\Rightarrow$ aplikací H na kódové slovo musíme dostat nulový vektor.
Dané slovo není kódové.

Zkoumejme na jakých slovech se shodují všechny možné správy:

$$\begin{pmatrix} 001 \\ 010 \\ 101 \\ 010 \\ 100 \\ 100 \\ 010 \\ 001 \end{pmatrix}$$

$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = (10100001)$ $\Big)5$ $\quad 100000000$

$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = (01010010)$

$\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = (11110011)$

$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = (00101100)$

$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = (10001101)$

$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = (11011111)$ $\Big)3$

$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = (01111110)$

Min Ham. vzdálenost (počet bitů, ve kterých se dané slova liší) je 3.

$H(s) = n$

$H(s+l) = n$

Možné syndromy:	Slova (110110) (011011)
(000)	(000000) (001001) (010010) (100100) (101101) (111111)
(001)	(001000) (000001) (011010) (101100) (100101) (110111) ...
(010)	
(011)	
(100)	
(101)	
(110)	
(111)	(111000) (110001) (100010) (010100) (010101) (000111) ...

1. řádek - slova se syndromem (000), tedy kódová slova. Uvažme (6,3) kód generovaný polynomem $1 + x + x^3$

Generující matice:

$x^3 \equiv 1$
$x^1 \equiv x$
$x^5 \equiv x^2$

$x^3 \rightsquigarrow 1+x^3$
$x^3 \rightarrow x+x^3$
$x^5 \rightarrow x^2+x^5$

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

$\begin{pmatrix}0\\0\\0\end{pmatrix} = 0000000$
$\begin{pmatrix}0\\0\\1\end{pmatrix} = 001001$
$\begin{pmatrix}0\\1\\0\end{pmatrix} = 010010$
$\begin{pmatrix}0\\1\\1\end{pmatrix} = 011011$
$\begin{pmatrix}1\\0\\0\end{pmatrix} = 100100$
$\begin{pmatrix}1\\0\\1\end{pmatrix} = 101101$
$\begin{pmatrix}1\\1\\0\end{pmatrix} = 110110$
$\begin{pmatrix}1\\1\\1\end{pmatrix} = 111111$

$(100) \rightarrow (100100)$
$(010) \rightarrow (010010)$
$(001) \rightarrow (001001)$

Pošud bychom přijali slovo (011010),
zjistili bychom, že má syndrom (001) a
dle heuristiky odečtáme slovo z příslušné
brudy se sbejným syndromem (2. z zdola) s nejmenším
počtem jedniček ((001000)), dostáváme
pravděpodobně ~~to~~ odeslané kódové slovo
(010010)