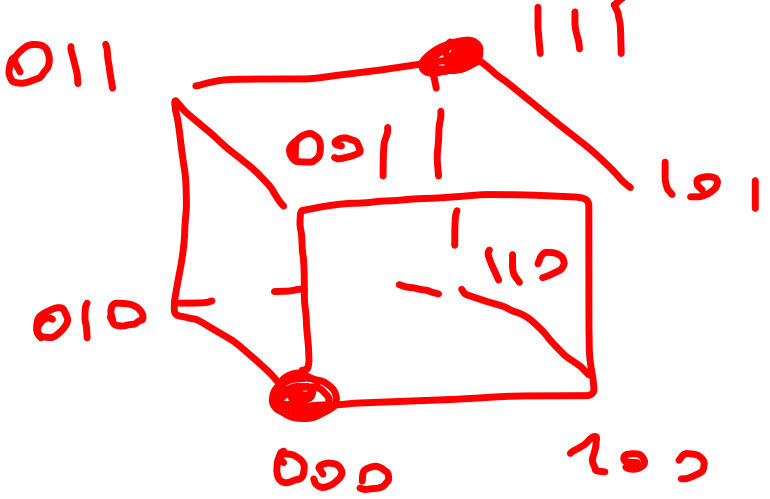
(3, 2) - kód (parity check)

$\mathbb{Z}_2[x]$



$p(x)$ [illegible] $\Rightarrow$ $(n, n-m)$-kód

$(b_0, \dots, b_{2-1}) + (c_0, \dots, c_{2-1}) = (b_0 + c_0, \dots)$

$q(x) \mid p(x)$?

pro $q(x) = (x-a)$ snadné:

def' $p(x) \Leftrightarrow p(a) = 0$

nad $\mathbb{Z}_2$ $x+1 = x-1 \Rightarrow$

$(x+1)$ dělí $v(x) \Leftrightarrow v(1) = 0$

$v(1)$ = počet jedniček mezi koeficienty

$p(x) = 1 + x + x^2 + \dots + x^\xi$ dělí řídí

"opakování ξx" $(\xi+1, 1)$-kód

$(3,1)$ kód opravuje

$\deg p(x) = 2$ $\quad v(x) = \begin{cases} 0 \\ p(x) \end{cases}$

$\deg v(x) = 2$

$\Rightarrow$

1) ireducibilní

$p(x)$ ... 2) "moc nedělí"

---

příklad: dělí $(1 + x^{2^{m-1}})$

nedělí $(1 + x^k)$ $k < 2^{m-1}$

$\deg p = m$

$p(x) \nmid e(x)$ má s max. 2 členy

$\Leftrightarrow$

1 člen: $e(x) = x^i$, $0 \le i \le n-1$

$\Rightarrow$ $p(x)$ je red. $\Rightarrow$ $p(0) = 1 \Rightarrow p(x) \nmid x^i$

2 členy: $e(x) = x^i + x^j$, $0 \le i < j < n$

$= x^i(1 + x^{j-i})$, $0 < j - i < n$

$p(x) \nmid x^i$ (je red)

$p(x) \nmid (1 + x^k)$ $\forall$ $k \le n-1$ (je primitivní)

$\Rightarrow$ $p(x)$ nedělí $e(x)$

Kódové slovo $v(x)$ je dělitelné

$p(x) = g(x)(1+x)$ tj. oběma

$\Rightarrow$ dělitelnost $g(x)$ rozpozná dvojité chyby (dělitelnost $(1+x)$ je test parity) $\Rightarrow$ rozpoznání všech lichých poč. chyb!

$x^3 + x + 1$

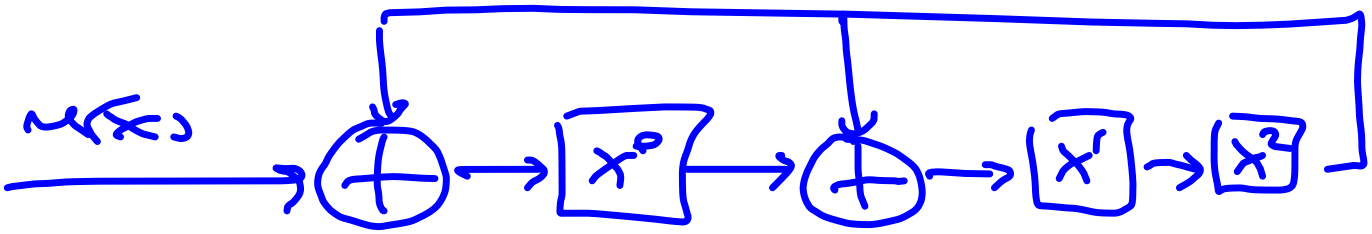
$(x^4 + x^3) : (x^3 + x + 1) = x + 1$

$x^4 + x^2 + x$

$x^3 + x^2 + x$

$x^3 + x + 1$

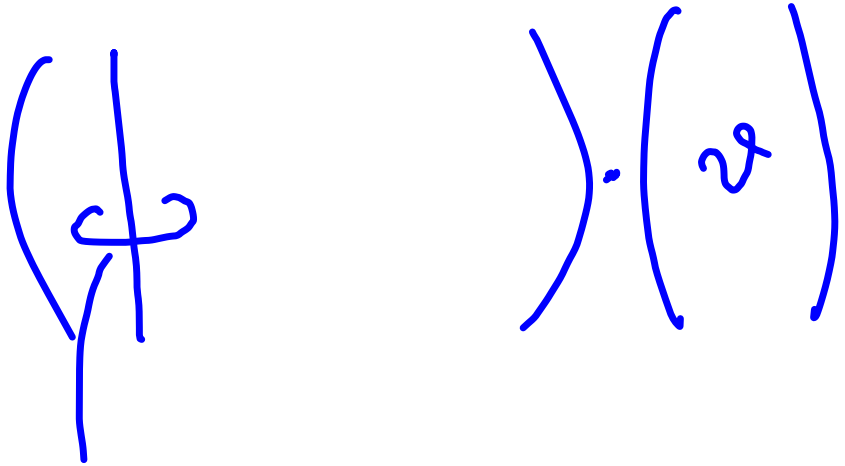
$x^2 + 1$



$(6,3)$ - kód

$u(x) = 0\ 0\ 0\ 1\ 1\ 0$

$(\mathbb{Z}_2)^2$ .. vektorový prostor



Smíšený součin

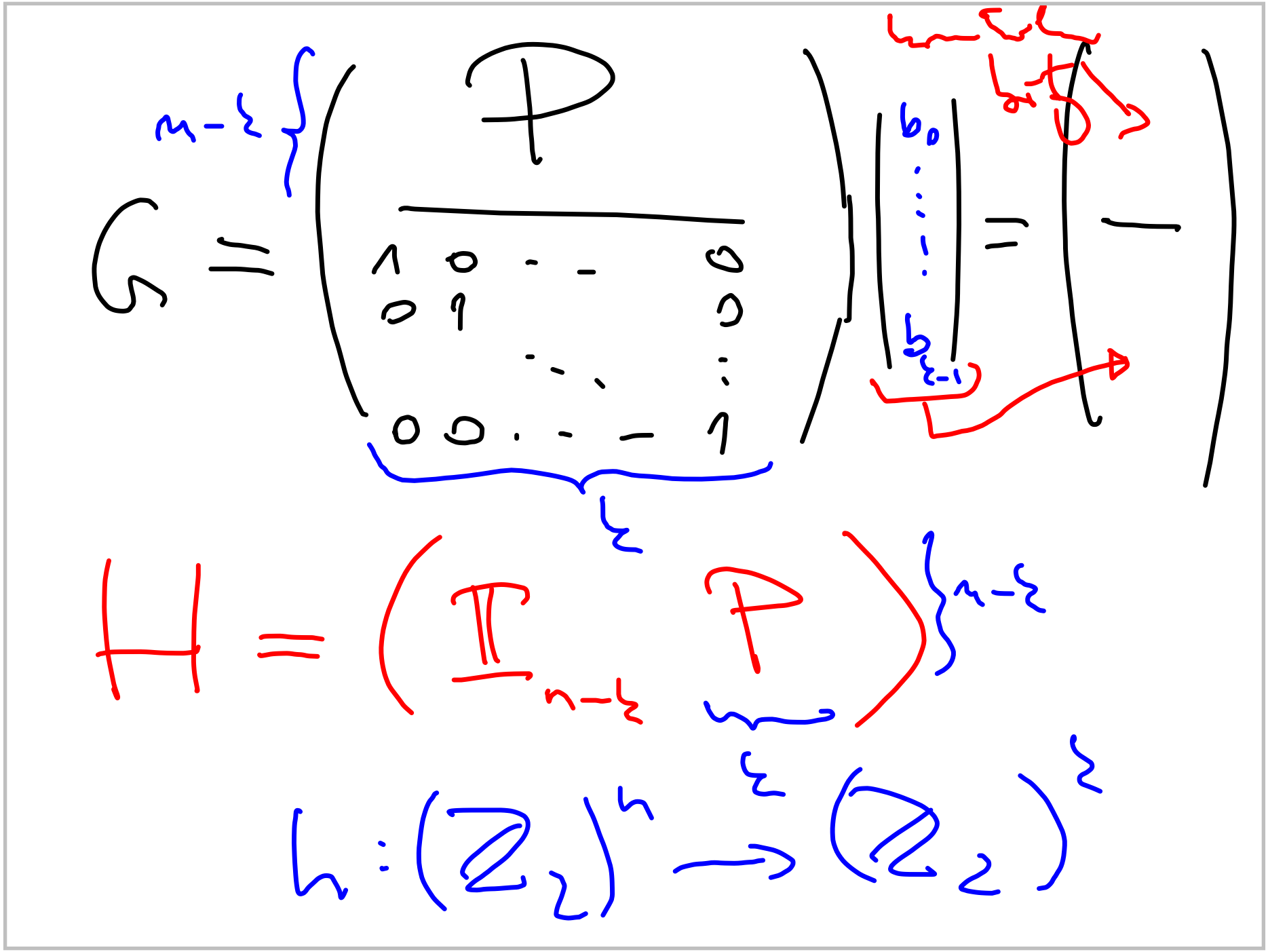
1. vektor báze

$v(x) \Rightarrow \underbrace{r(x) + x^{n-m} \cdot v(x)}_{v(x)}$

$v_1 + v_2$

$x^{n-m}(v_1(x) + v_2(x)) = q(x)\,p(x) + r(x)$

$= \boxed{q_1(x)\,p(x)} + r_1(x) + \boxed{q_2(x)\cdot p(x)} + r_2(x)$


n-k
P
1 0 . . 0
0 1 0
0 0 . . 1
k
b0
bk-1
=
1
H =
In-k
P
n-k
k
h : (Z2)^n → (Z2)^k

Důkaz: $h \circ g : (\mathbb{Z}_2)^k \to (\mathbb{Z}_2)^k$

$$H \cdot G = (\Pi_{n-k} P) \cdot \begin{pmatrix} P \\ \Pi_k \end{pmatrix}$$

$$= \Pi_{n-k} \cdot P + P \cdot \Pi_k = P + P = 0$$

$\dim \ker + \dim \operatorname{Im} = \dim V$

$\ker$ nad $\mathbb{Z}_2$

$\dim \operatorname{Im} g = k$

$\dim \operatorname{Im} h = n-k$

$$\left(\begin{array}{c|c} 1 \cdots 0 & \\ & P \\ 0 \cdots 1 & \end{array} \right) \left(\begin{array}{c} P \\ \hline \Pi_k \end{array} \right)$$

$u = v + e$

$v \in V$ ... prostý lineární kód

(vektorový prostor nad $(\mathbb{Z}_2)^n$)

dimenze V je k

$v \in u + V \in (\mathbb{Z}_2)^n / V$

$\Updownarrow$

hledání prostých kódů