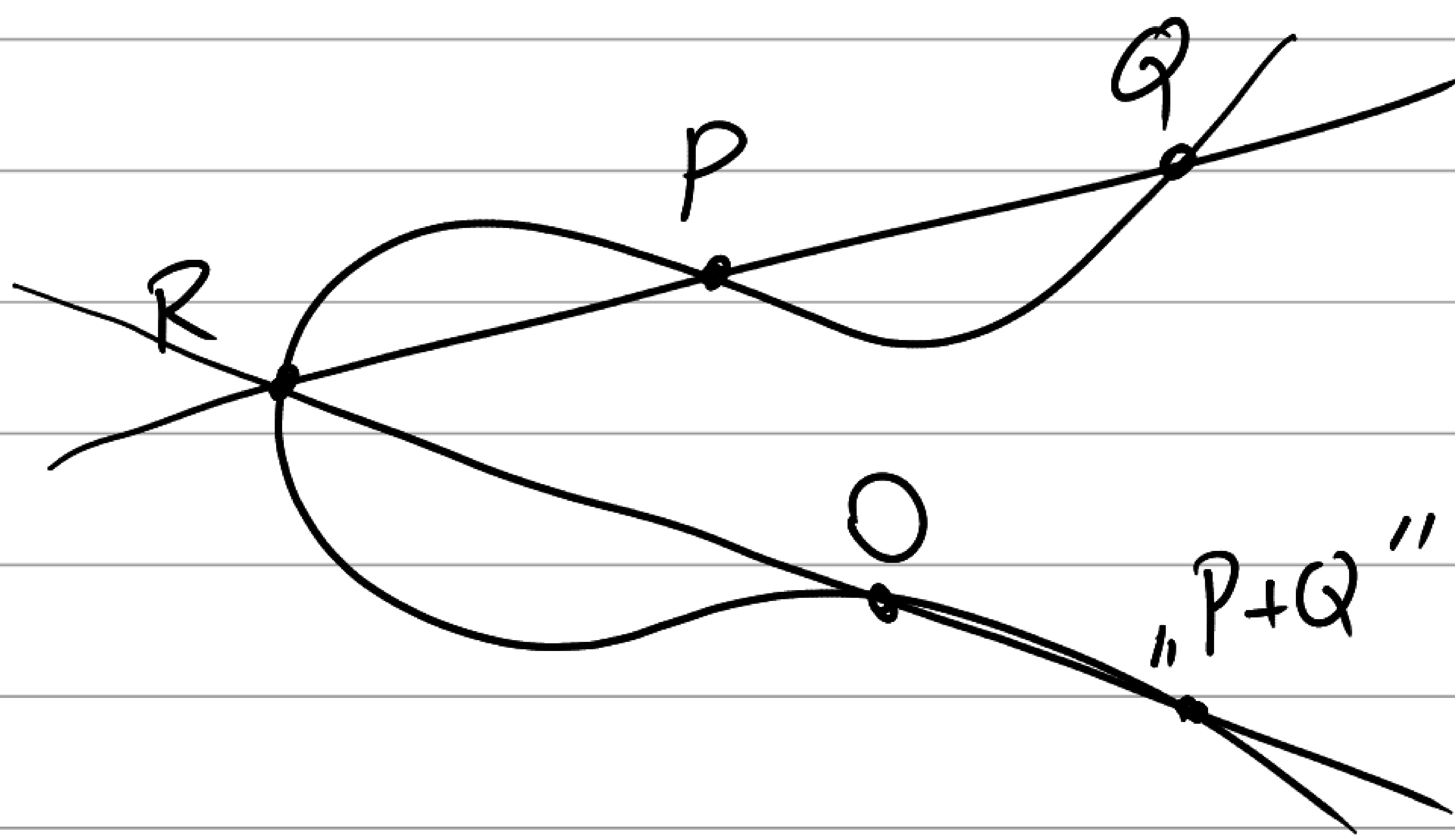
$$\begin{array}{ccccc} \text{Alice} & & \text{Cecil} & & \text{Bob} \\ a & \underset{g^c}{\overset{g^a}{\rightleftarrows}} & c & \underset{g^b}{\overset{g^c}{\rightleftarrows}} & b \end{array}$$

$$g^{ac} \qquad\qquad g^{bc}$$



$$R+P+Q = R+O+\text{„}P+Q\text{"}$$

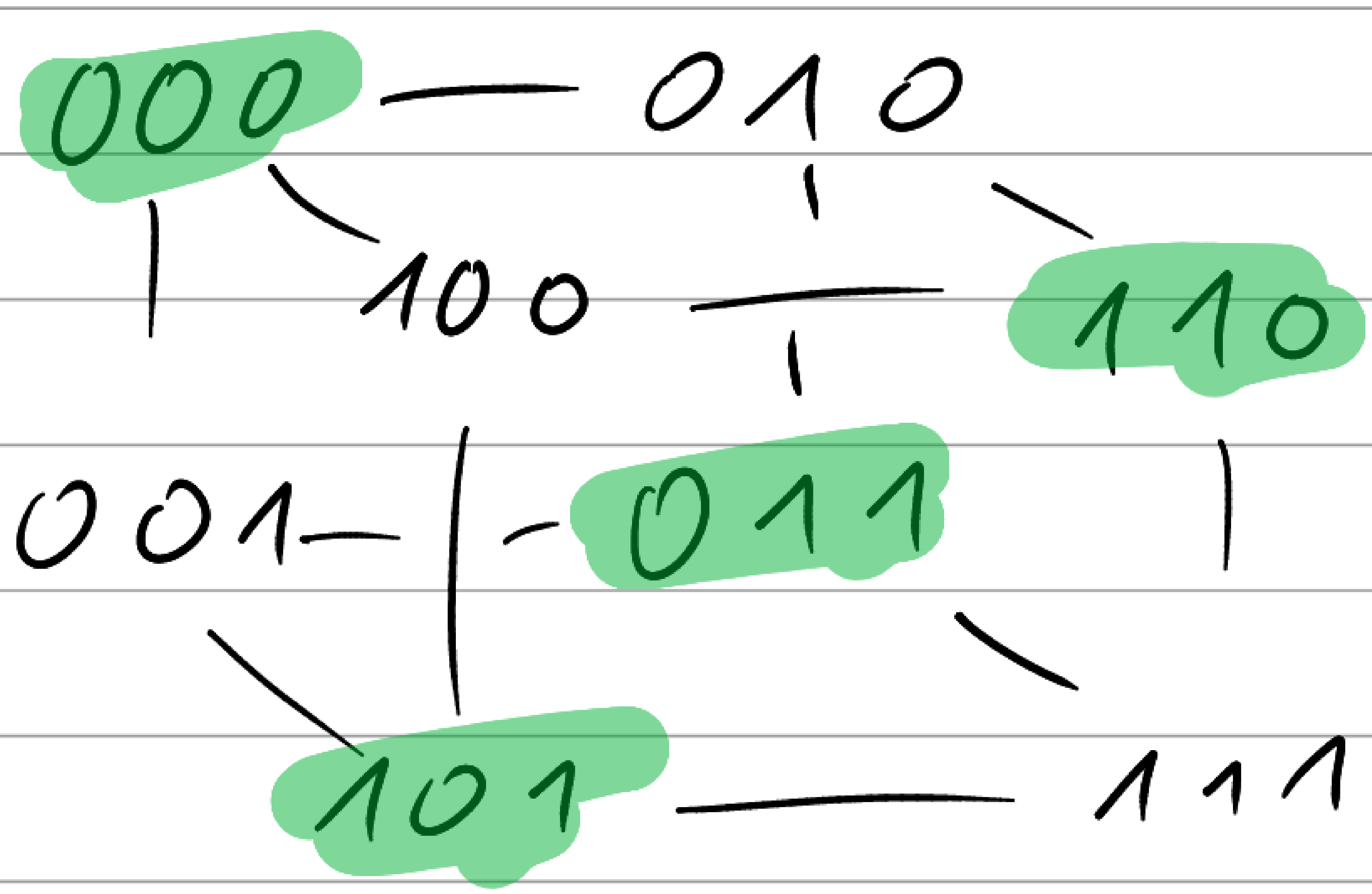
$\mathbb{Z}_2 = \{\text{zbytkové třídy modulo } 2\}$

$0, 1$

$0 + 1 = 1$

$1 + 1 = 0$

$(\mathbb{Z}_2)^n \ni \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

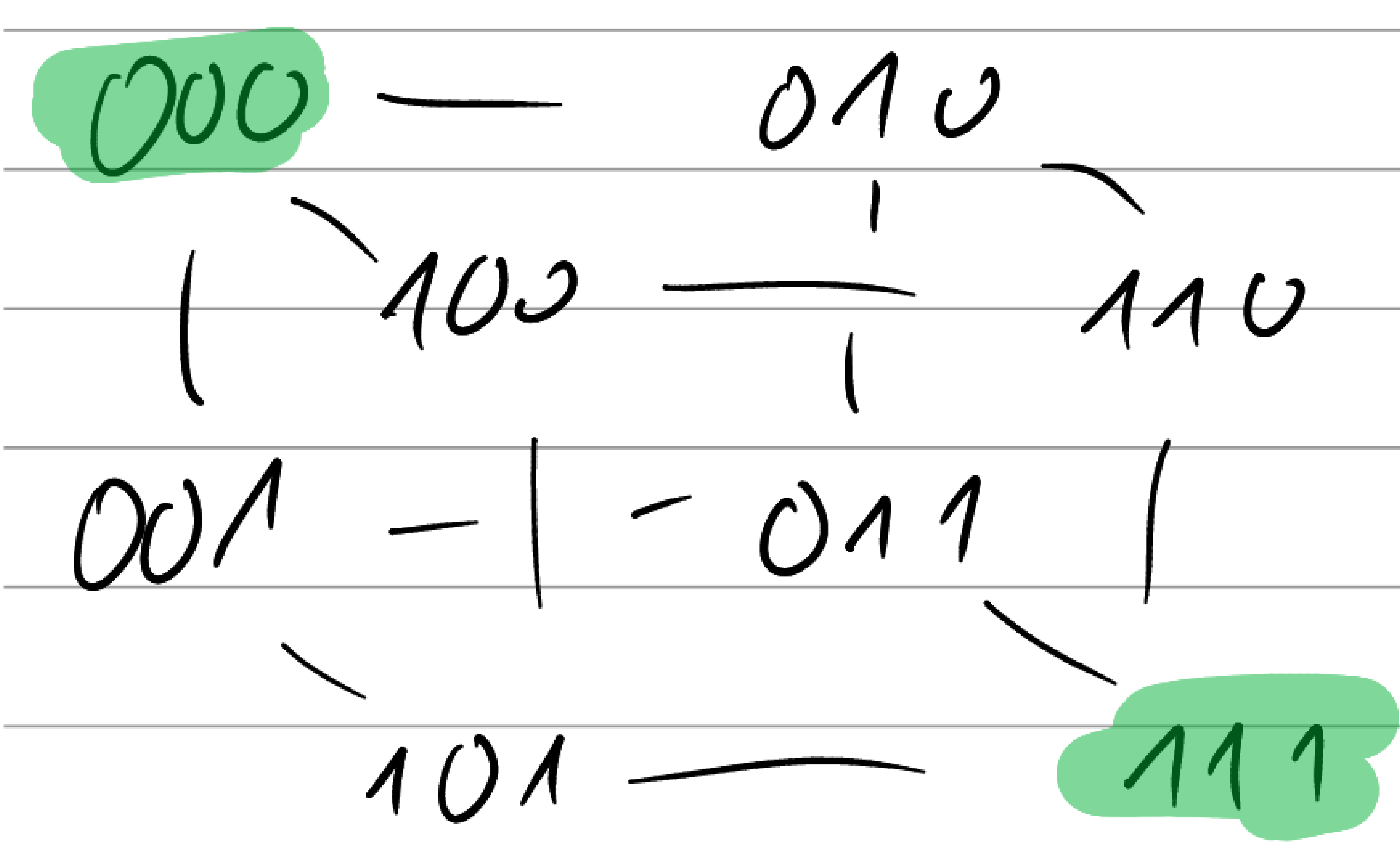


$00 \mapsto 000$

$01 \mapsto 101$

$10 \mapsto 110$

$11 \mapsto 011$



V $\mathbb{Z}_2$ je $\underline{\underline{x = -x}}$

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

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

$$(\mathbb{I} \mid P)\begin{pmatrix} x \\ y \end{pmatrix} = \mathbb{I} \cdot x + P \cdot y$$
$$= x + Py$$

$H \cdot v = 0 \iff v$ kódové slovo

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} ; \quad H \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$H \cdot (v + e) = H \cdot v + H \cdot e$$

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_k \end{pmatrix} = 1 \cdot x_0 + 1 \cdot x_1 + \cdots + 1 \cdot x_k$$
$$= x_0 + x_1 + \cdots + x_k$$
$$= h(x)$$

$$H = \left(\overbrace{1}^{\mathbb{I}_1} \middle| \overbrace{1 \; \cdots \; 1}^{P} \right)$$

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

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ \hline 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad G \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ \hline 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

$$\mathbb{Z}_2[x] \ni b_0 + b_1 x + \cdots + b_{k-1} x^{k-1}$$
$$b_0, b_1, \ldots, b_{k-1} \in \mathbb{Z}_2$$

$p(x) = 1+x$

$v(x) = 1+x^2$ ... co je $h(v(x))$

$$
\begin{array}{l}
(x^2+1):(x+1) = x-1 \\
-(x^2+x) \\
\hline
\quad -x+1 \\
\quad -(-x-1) \\
\hline
\qquad 2
\end{array}
$$

$h(v(x)) = 2 = 0$

$h(v(x)+v'(x)) \overset{?}{=} h(v(x)) + h(v'(x))$

$v(x) = q(x) \cdot p(x) + r(x)$

$v'(x) = q'(x) \cdot p(x) + r'(x)$

$v(x)+v'(x) = (q(x)+q'(x)) \cdot p(x) + (r(x)+r'(x))$

$h(1) = 1 \quad h(x) = x, \ldots, h(x^{n-k-1}) = x^{n-k-1}$

$$1+x+x^3 = p(x)$$

$$x^i$$

$$H = \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right) \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \text{i-tý sloupec } H$$

$1 \bmod p(x) = 1+0x+0x^2$

$x = 0+1x+0x^2$

$x^2 \quad 0+0x+1x^2$

$x^3 \bmod p(x) = 1+x$

$x^4 = x+x^2$

$$x^3 = 1\cdot(1+x+x^3) + 1 + x$$

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

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

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

$$x^6 \equiv x+x^2+x^3 \equiv x+x^2+1+x \equiv 1+x^2$$

$$\left(1 \,\middle|\, 1 \; 1 \; \cdots \; 1\right) = H$$

zb.1 zb.1

$$x = 1 \cdot (1+x) + 1$$

$$x = 1$$

$$x^2 = x = 1$$

$$x^3 = x = 1$$

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

$$\left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right) = H$$

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

$$G \cdot (0) = \begin{pmatrix} 0 \\ 0 \\ \hline 0 \end{pmatrix}$$

$$G \cdot (1) = \begin{pmatrix} 1 \\ 1 \\ \hline 1 \end{pmatrix}$$

$v(x)$ $\qquad\qquad$ $v(x)+e(x)$

kódové $\qquad$ ne-kódové

$e(x)$ málo členů

$e(x)=x^i$

$e(x)=x^i+x^j$

$p(x) \mid v(x) \Rightarrow p(x) \nmid v(x)+e(x)$

! $p(x) \nmid e(x)$