If $u=(u_1,u_2,\dots,u_k)$ is an original message $u_i \in GF(q)$

Then encoding $Z_q^k \longrightarrow Z_q^n$ can be implemented as:

$$u \longmapsto uG = \sum_{i=1}^{k} u_i v_i$$

$$u_i \in GF(q),\ v_i \in Z_q^n$$

Since $v_i \in C$ and C linear

$$uG \in C$$

Let $G = \left[I \mid P \right]$

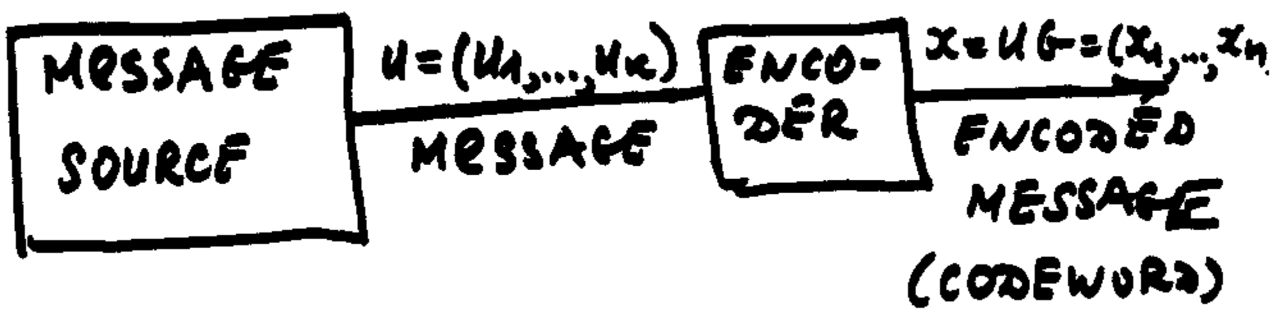
Then
$$x = uG = (x_1, x_2, \dots, x_k, x_{k+1}, \dots, x_n)$$

and
$$\boxed{x_i = u_i \qquad x_{k+i} = \sum_{j=1}^{k} p_{ij} u_j}$$

$x_1, \dots, x_k$ are <u>information</u> (message) digits

$x_{k+1}, \dots, x_n$ are <u>check</u> digits (redundancy)

$R = \frac{k}{n}$ is a transmission rate



Encoder $u \longmapsto x = uG$

$u \in \mathbb{Z}_q^k \longmapsto x \in \mathbb{Z}_q^n$

FOR A BINARY LINEAR

code C such that

$|C| = 2^k \qquad C \subseteq \mathbb{Z}_2^n$

ENCODING REQUIRES

$n-k$ ADDERS mod 2

(XOR gates)

with at most k inputs

ENCODER is a <u>LINEAR</u> NETWORK

(requires <u>XOR</u> <u>gates only</u>)

60 80

Example

$(7,16,3)$ code C

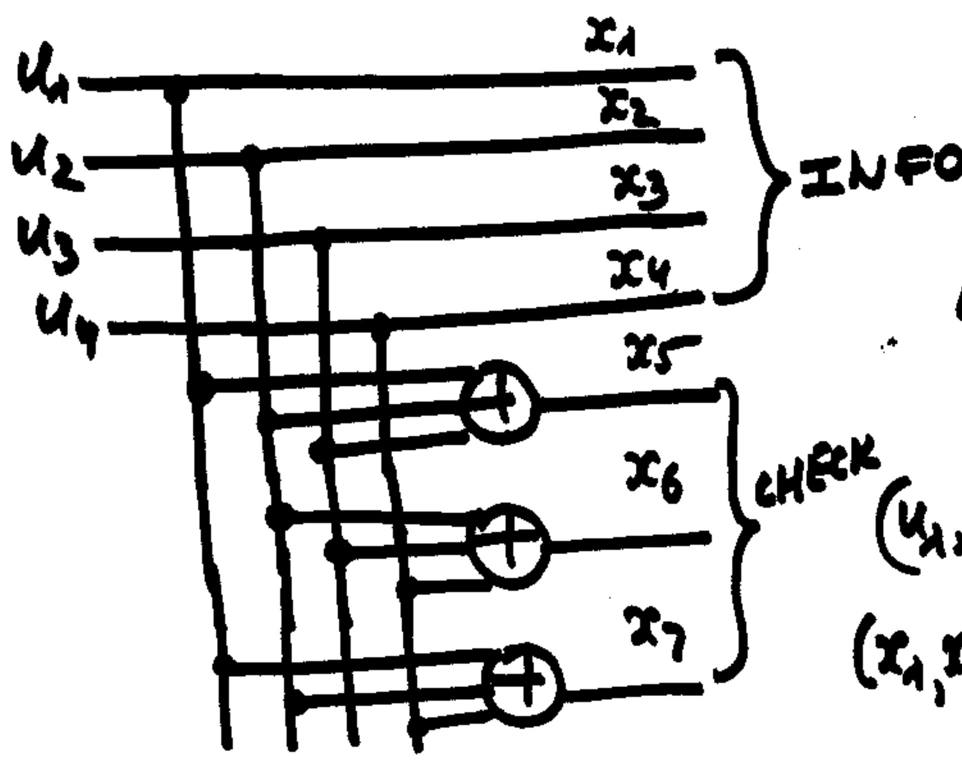
$$G=\begin{bmatrix}1000 & 101\\ 0100 & 111\\ 0010 & 110\\ 0001 & 011\end{bmatrix}$$

$k=4$

$\cancel{x=(u_1,u_2,\dots,u_7)}$

$$x=(u_1,u_2,u_3,u_4)\begin{array}{c}\quad I \qquad\quad P\\ \left[\begin{array}{cccc|ccc}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{array}\right]\end{array}=$$

$$=(u_1,u_2,u_3,u_4,u_1+u_2+u_3,u_2+u_3+u_4,u_1+u_2+u_4)$$



ENCODER for C

$(u_1,u_2,u_3,u_4)\longrightarrow$

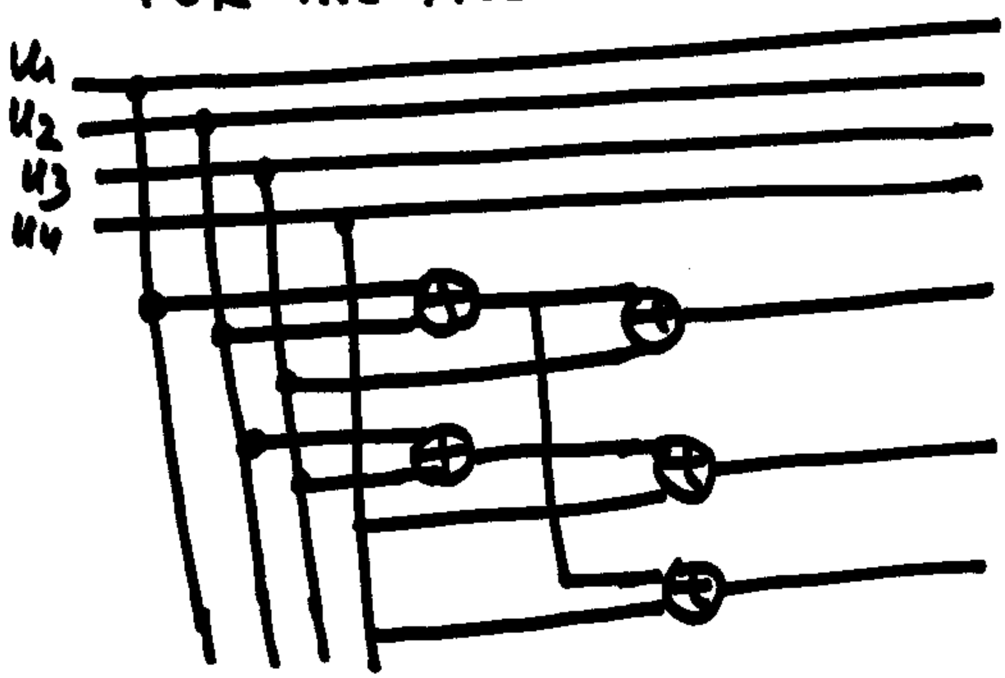
$(x_1,x_2,x_3,x_4,x_5,x_6,x_7)$

If only <u>two input</u> XOR gates are used for encoding then networks computing

$x_{K+1}, \dots, x_{K+r}$ $\quad K+r=n$

can be minimized by sharing gates.

FOR THE PREVIOUS EXAMPLE



DECODING WITH A LINEAR CODE

Let $\mathbb{C} \subseteq \mathbb{Z}_q^n$ is a linear code and $a \notin \mathbb{C}$

Consider

$$a+\mathbb{C} = \{a+x \mid x \in \mathbb{C}\}$$

$a+\mathbb{C}$ is a <u>coset</u> of $\mathbb{C}$

Take $b \notin \mathbb{C}$ and $b \notin a+\mathbb{C}$

Consider $b+\mathbb{C} = \{b+x \mid x \in \mathbb{C}\}$

$b+\mathbb{C}$ is another coset.