# Infokód
# I

2016. 09. 14

BER : Bit Error Rate

SE: Spectral efficiency

[bit/sec/Hz] present 0.52 bit/sec/Hz

What is the data transmission rate available over 1 Hz physical spectrum

Source coding — channel coding — Data security

↓ Data compression

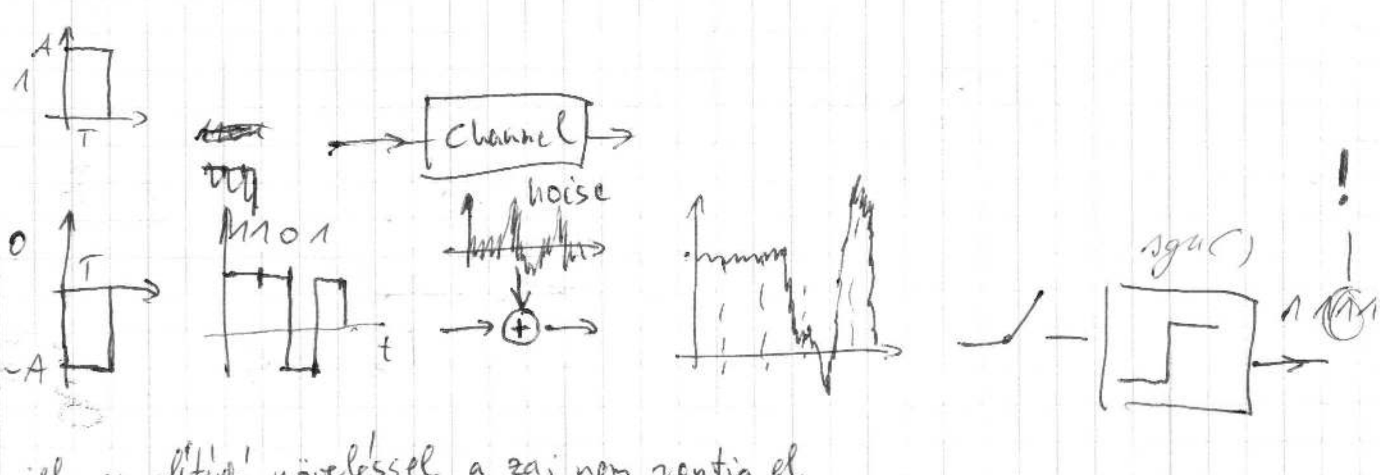
↓ unreliable channel Error correcting coding

↓ Cryptography

- How to communicate reliably over an unreliable channel
- How to ensure QoS communication

$$QoS \rightarrow P_B(BER) < 10^{-\gamma}$$ m "$\gamma$" QoS parameter

Comm. model:



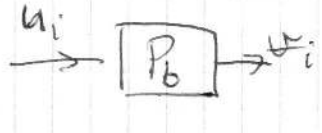
jel amplitúdó növeléssel a zaj nem rontja el

Errors are random events : $P_B \Longleftrightarrow$ SNR = Signal-to-Noise-Ratio

Transmission Power ↗ / ↙ $P_B$

↳ Limited

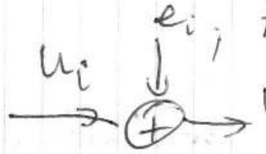
## Binary Symetric Channel (BSC)



$$P_b = P\left(v_i = 1 \,\middle|\, u_i = 0\right) = P\left(v_i = 0 \,\middle|\, u_i = 1\right)$$

$$1 - P_b = P\left(v_i = 0 \,\middle|\, u_i = 0\right) = P\left(v_i = 1 \,\middle|\, u_i = 1\right)$$ error free transmission

$e_i$ ; $P_b = P(e_i = 1)$ ; $1 - P_b = P(e_i = 0)$

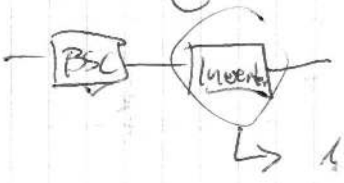


$v_i = u_i \oplus e_i$

| $u_i$ | $e_i$ | $v_i$ | |
|---|---|---|---|
| 0 | 0 | 0 | ← error free $v_i = u_i$ ← $1-P_b$ |
| 0 | 1 | 1 | ← error : $v_i \neq u_i$ ← $P_b$ |
| 1 | 0 | 1 | ← error free |
| 1 | 1 | 0 | ← error |

$0 \leq P_b < 0{,}5$ if $P_b > 0{,}5$

$\Downarrow$

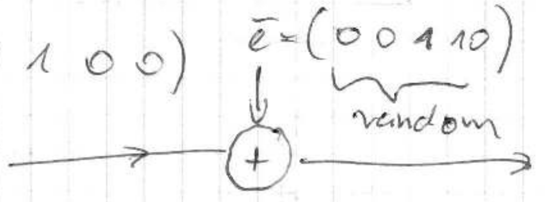


↳ $1 - P_b$

Infokód

## Vectorial Channel model

$\bar{u} = (0\ 1\ 1\ 0\ 0)$ $\quad \bar{e} = (\underbrace{0\ 0\ 1\ 1\ 0}_{\text{random}})$



$\bar{v} = \bar{u} \oplus \bar{e} = (\underset{1-P_b}{0}\ \underset{1-P_b}{1}\ \underset{P_b}{0}\ \underset{P_b}{1}\ \underset{1-P_b}{0})$

$$P(\bar{v}|\bar{u}) = P_b^2\,(1-P_b)^3 = P_b^{d(\bar{u},\bar{v})} \cdot (1-P_b)^{n-d(\bar{u},\bar{v})} =$$

n: total length

$$\left[\underset{\text{Hamming distance}}{d}(\bar{u},\bar{v}) = d((0 1 1 0 0),(0 1 0 1 0)) = 2\right]$$

$$= \left(\frac{P_b}{1-P_b}\right)^{d(\bar{u},\bar{v})} \cdot (1-P_b)^n$$

$$0 \le P_b < 0{,}5 \quad ; \quad 0 \le \frac{P_b}{1-P_b} < 1$$

$$P(\bar{e}) = P_b^{w(\bar{e})} \cdot (1-P_b)^{n-w(\bar{e})} = \left(\frac{P_b}{1-P_b}\right)^{w(\bar{e})} \cdot (1-P_b)^n \sim O(\exp(-w(\bar{e})$$

$$\left[\underset{\hookrightarrow \text{number of 1-s}}{w(0\ 0\ 1\ 1\ 0)}\right] \quad \cancel{P(w(\bar{e})=t)} \binom{n}{t} \left(= \frac{n!}{t!\,(n-t)!}\right)$$

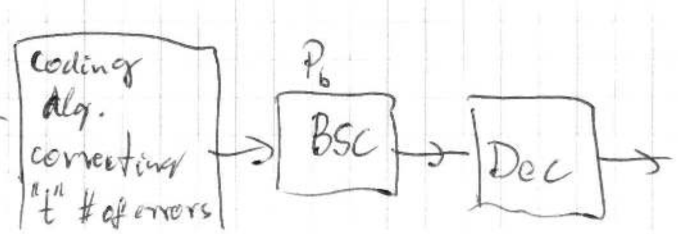
$$P(w(\bar{e})=t) = \binom{n}{t} P_b^t\,(1-P_b)^{n-t} \sim O(\exp(-t))$$

---

QoS: Given: $P_b \sim 10^{-2}$, $\gamma$

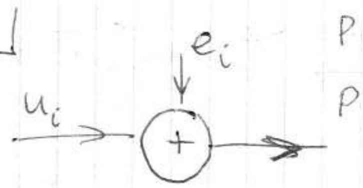
"t" # (number) of errors can be corrected

P(error) →



$$P(\text{error}) = \cancel{P(w(\bar{e}))}\, \underbrace{P(w(\bar{e}) > t)}_{\underline{\text{II}}\ \text{előadás}} = \sum_{i=t+1}^{n} \binom{n}{t} \left(\frac{P_b}{1-P_b}\right)^{i} (1-P_b)^{n} < \overset{\overset{\text{QoS}}{\downarrow}}{10^{-\gamma}}$$

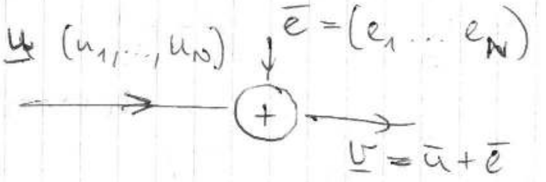
**BSC**



$P(e_i = 1) = P_b$

$P(e_i = 0) = 1 - P_b$

$0 \leq P_b < 0{,}5$



$$P(\bar{e}) \sim \exp(-w(\bar{e}))$$

$$P(w(\bar{e}) = k) = \binom{n}{k} P_b^{k} (1-P_b)^{n-k}$$

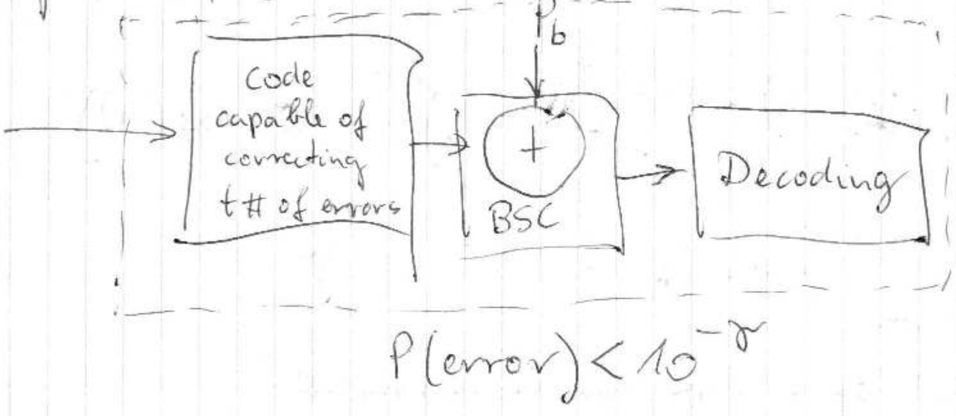
QoS Let us assume, that "t" # of errors we can correct

$$P(\text{error}) = \sum_{i=t+1}^{n} \binom{n}{i} \left(\frac{P_b}{1-P_b}\right)^{i} (1-P_b)^{n} < 10^{-\gamma}$$

$\gamma$: QoS parameter

Design:

Given $\gamma$, $P_b$

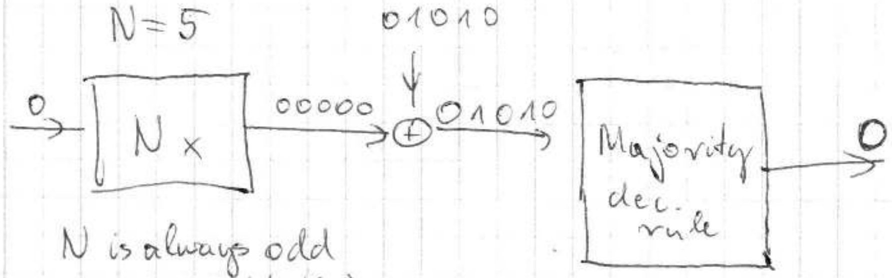


$$P(\text{error}) < 10^{-\gamma}$$

Infokód 1

2016.09.21.

## Repeater code



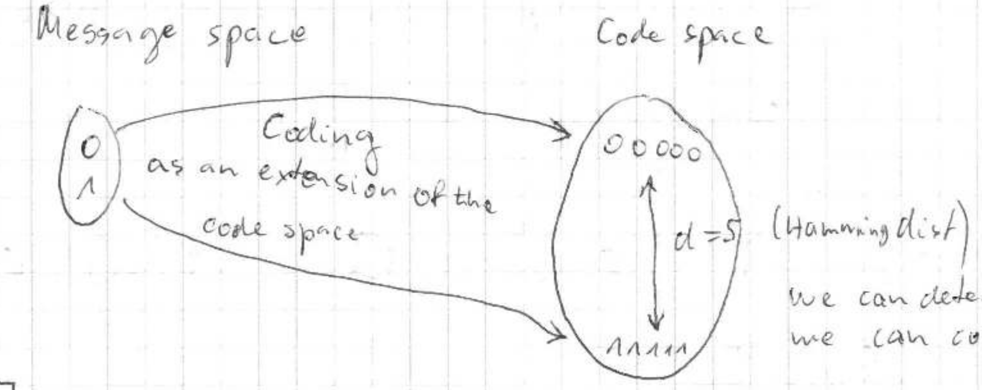
N is always odd (páratlan)

Given $P_b, \gamma$ $$P(\text{error}) = \sum_{i=\left\lceil \frac{n}{k} \right\rceil}^{N} \binom{N}{i} P_b^{i} (1-P_b)^{N-i} < 10^{-\gamma}$$

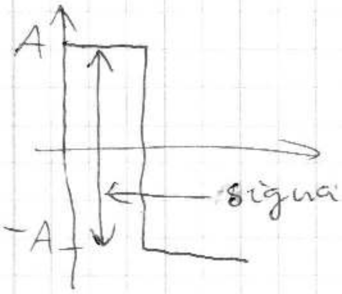
$i = \left\lceil \frac{n}{k} \right\rceil$

Great loss in dataspeed $\frac{1}{N}$ !!!

## Geometric interpretation



we can detect errors
we can correct errors

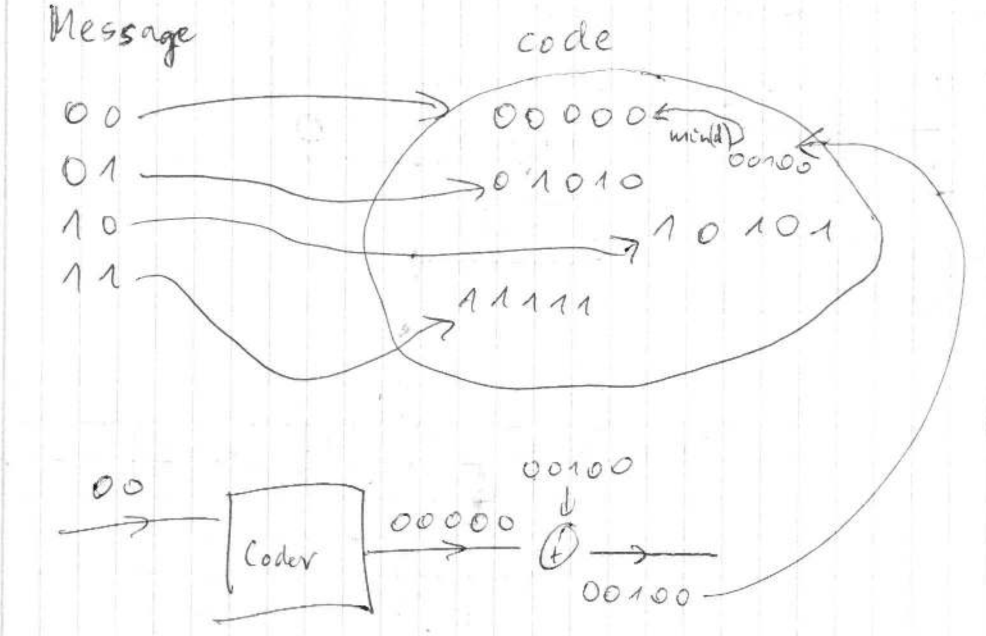


signal distance limited by the transmission power

⇕ ?

code distance limited by the tolerable loss in data speed

## Another example



## Formal description

$\bar{u} = (u_1 \dots u_k)$ $C(n,k,$

- Messages $\bar{u} \in \{0,1\}^k$ ; $\dim(\bar{u}) = k$ , $M = 2^k$
  ↳ # of messages

- Code $C = \{\bar{c}_1 \dots \bar{c}_M\}$ ; $\dim(\bar{c}) = n$ $n > k$, ~~redunda~~

  redundancy: $n-k$ ; $\frac{k}{n}$

- Coding: $\Psi : \{0,1\}^k \rightarrow C$ ; $\Psi(\bar{u}) = \bar{c}$

  $\xrightarrow{\bar{c}} \overset{\downarrow \bar{e}}{\oplus} \xrightarrow{} \bar{v} = \bar{c} + \bar{e}$

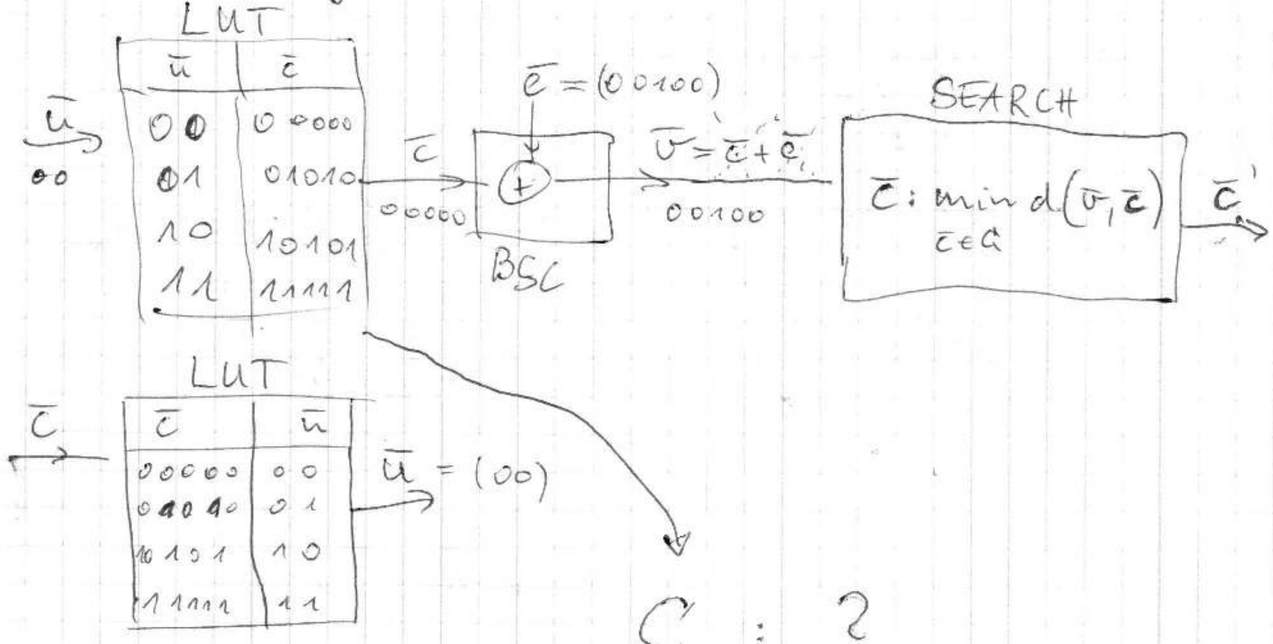
- Received vectors $\bar{v} \in \{0,1\}^n$ ; $\dim(\bar{v}) = n$

- Detection $\varphi : \{0,1\}^n \rightarrow C$ $\varphi(\bar{v}) = \bar{c}$

- Decoding $\Psi^{-1} : C \rightarrow \{0,1\}^k$ ; $\Psi^{-1}(\bar{c}) = \bar{u}$

nfokód)

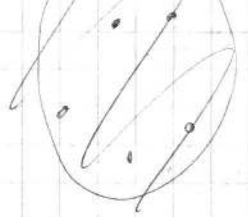
## Generic Coding scheme



| $\bar{u}$ | $\bar{c}$ |
|---|---|
| 00 | 00000 |
| 01 | 01010 |
| 10 | 10101 |
| 11 | 11111 |

| $\bar{c}$ | $\bar{u}$ |
|---|---|
| 00000 | 00 |
| 01010 | 01 |
| 10101 | 10 |
| 11111 | 11 |

$C_{opt}$: ?



$$d_{min}: \min_{\substack{\bar{c},\bar{c}' \in C \\ \bar{c} \neq \bar{c}'}} d(\bar{c}, \bar{c}')$$

$$\Downarrow$$

$$C_{opt}: \max_{C} d_{min}$$

problem I: too complex

Complexity: $\sim 3O(2^k)$   On-line compl.

problem II:

$C_{opt}$: calculating this is impossible

---

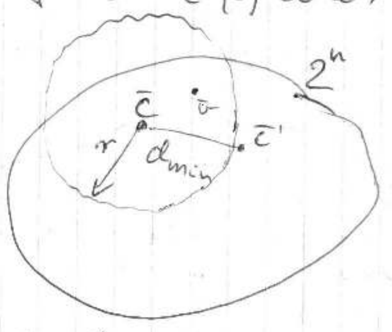
Challenge:

How to replace this scheme with a real-time scheme ("p" complexity operations) and find the optimal code to upload.

Code performance:

$$d_{min}: \min_{\substack{\bar{c},\bar{c}' \in C \\ \bar{c} \neq \bar{c}'}} d(\bar{c},\bar{c}')$$

Error detection capability of a $C(n,k)$ code: $d_{min}-1$

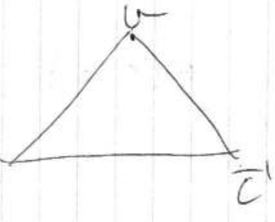


$r = d_{min} - 1$

Error correction capability.

Correct detection

$d(\bar{v},\bar{c}) < d(\bar{v},\bar{c}') \quad \forall \bar{c}' \in C;\ \bar{c} \neq \bar{c}'$



$$d(\bar{c},\bar{c}') \le d(\bar{v},\bar{c}) + d(\bar{v},\bar{c}')$$

$$d(\bar{c},\bar{c}') - d(\bar{v},\bar{c}) \le d(\bar{v},\bar{c}')$$

$$d(\bar{v},\bar{c}) < d(\bar{c},\bar{c}') - d(\bar{v},\bar{c})$$

$$d(\bar{v},\bar{c}) < d_{min} - d(\bar{v},\bar{c})$$

$$2\, d(\bar{v},\bar{c}) < d_{min}$$

## III ea

2016. 09. 23

Generic scheme is non Real-Time

How to develop a Real-Time scheme?

("P" complexity in each box)

2016. 09. 23.

## Code Performance

Singliton bound $d_{min} \leq n-k+1$

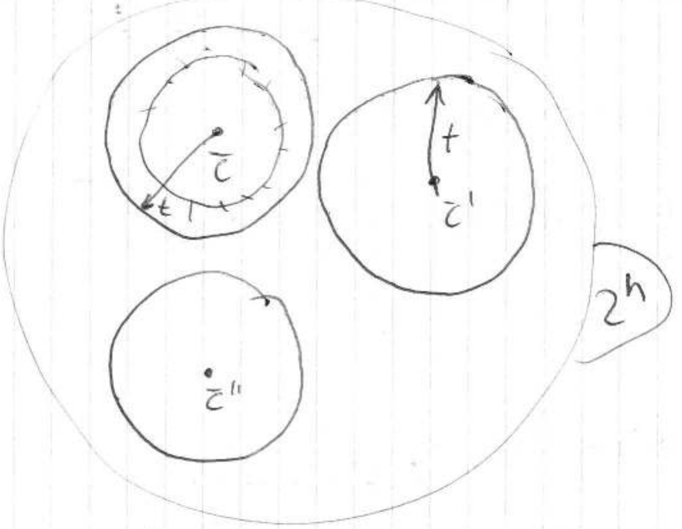
Systematic codes

$$\bar{c} = (\overbrace{u_1, \dots, u_k}^{k\text{-bit}}, \overbrace{p_{k+1} \dots p_n}^{n-k \text{ bit}}) = (\bar{u}, \bar{p})$$

$$\bar{c}' = (u'_1 \dots u'_k \ p'_{k+1} \dots p'_n)$$

MDS codes (Maximum distance Separability) if $d_{min} = n-k+1$

Hamming bound: correcting "t" errors $\rightarrow \sum_{i=0}^{t} \binom{n}{i} \leq 2^{n-k}$



$$2^k \sum_{i=0}^{t} \binom{n}{i} \leq 2^n$$

$$\sum_{i=0}^{t} \binom{n}{i} \leq 2^{n-k}$$

$$\sum_{i=0}^{t} \binom{n}{i} = 2^{n-k}$$

## Binary Linear Codes $C(n,k)$

$G = \{\bar{g}^{(1)} \dots \bar{g}^{(k)}\}$, $\dim(\bar{g}^{(i)}) = n$; $C = \mathcal{L}_c\{G\}$

$$\bar{c} = \sum_{i=1}^{k} u_i \bar{g}^{(i)}; \quad (\underbrace{\quad \bar{c} \quad}_{n}) = u_1 (\underbrace{\quad \bar{g}^{(1)} \quad}_{n}) + u_2 (\underbrace{\quad \bar{g}^{(2)} \quad}_{n}) + \dots + u_k (\underbrace{\bar{g}^{(k)}}_{n})$$

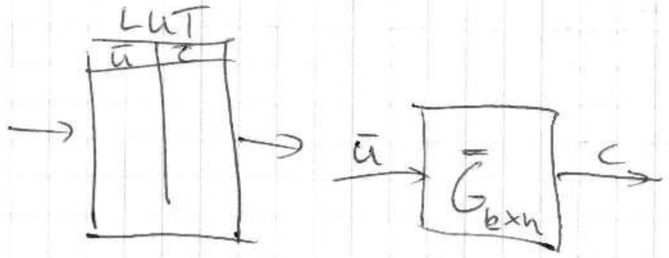
Generator Matrix:

$$\bar{G}_{k \times n} = \begin{pmatrix} \bar{g}^{(1)} \\ \hline \bar{g}^{(2)} \\ \hline \vdots \\ \hline \bar{g}^{(k)} \end{pmatrix}$$

Coding: $\bar{c} = \bar{u}\,\bar{\bar{G}} \rightarrow \left(\xrightarrow{\bar{c}}\right) = (\ldots m\,\bar{u} \ldots) \cdot \begin{pmatrix} \bar{\bar{G}}_{k\times n} \end{pmatrix}$

Technological message

LUT helyett mátrixszorzás



$$\underset{\text{compl. LUT}}{2^k(k+n)} \gg \underset{\text{Compl. gen matrix}}{k \times n}$$

E.g

$$G = \{(10110),\ (01111)\} \qquad \begin{matrix} k=2 \\ n=5 \end{matrix} \Rightarrow C(5,2)$$

$$\bar{\bar{G}}_{2\times5} = \begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1 \end{pmatrix} \qquad d_{min} = ?$$

$$\bar{c}^{(0)} = (0\ 0)\begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1 \end{pmatrix} = (0\,0\,0\,0\,0)$$

$$\bar{c}^{(1)} = (0\ 1)\begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1 \end{pmatrix} = (0\,1\,1\,1\,1)$$

$d_{min} = 3$

error detection = 2

—||— correction: ~~ta~~

$$: t = \left\lfloor \frac{3-1}{2} \right\rfloor = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 1$$

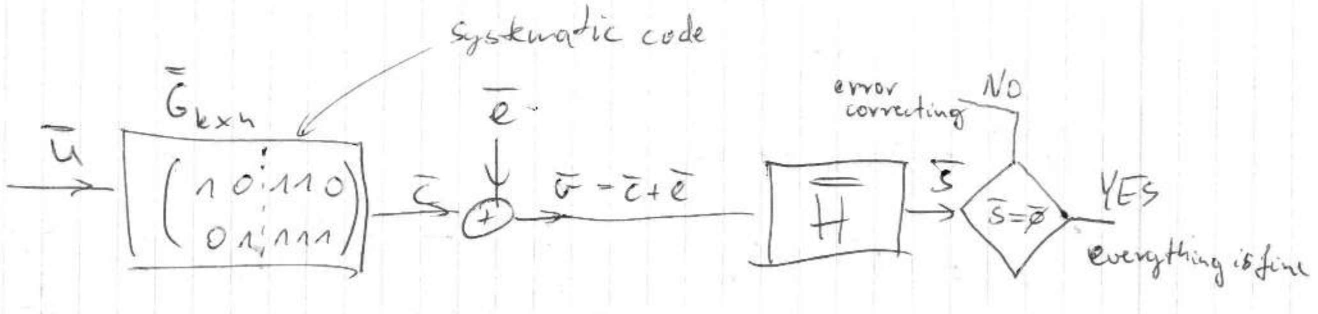
$$\bar{c}^{(2)} = (1\ 0)\begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1 \end{pmatrix} = (1\,0\,1\,1\,0)$$

$$\bar{c}^{(3)} = (1\ 1)\cdot\begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1 \end{pmatrix} = (1\,1\,0\,0\,1)$$

infokód

$$d_{min} \sim \min_{\substack{\bar{c},\bar{c}' \in C \\ \bar{c}\neq\bar{c}'}} d(\bar{c},\bar{c}') \sim \min_{\substack{\bar{c},\bar{c}' \in C \\ \bar{c}\neq\bar{c}'}} w(\underbrace{\bar{c}+\bar{c}}_{\bar{c}''}) \sim \min_{\substack{\bar{c}'' \in C \\ \bar{c}''\neq\bar{0}}} w(\bar{c}'')$$

Linear codes: $d_{min} = w_{min}$



Parity check matrix $\bar{\bar{H}}_{(n-k)\times n}$: $\bar{\bar{H}}\bar{c}^T = \bar{0}^T \ \forall \bar{c} \in C$

$$\bar{\bar{H}}\bar{v}^T = \bar{s}^T \qquad \bar{\bar{H}}(\bar{u}\bar{\bar{G}})^T = \bar{0}^T \ \forall \bar{u} \in \{0,1\}^k$$

$$\bar{\bar{H}}\bar{\bar{G}}^T\bar{u}^T = \bar{0}^T$$

$$\Downarrow$$

$$\bar{\bar{H}}\bar{\bar{G}}^T = \bar{\bar{0}}^T$$

Systematic Code

$$\bar{\bar{G}}_{k\times n} = (\bar{\bar{I}}_{k\times k}, \bar{\bar{B}}_{k(n-k)}|$$

$$\bar{\bar{H}}_{(n-k)\times n} = (\bar{\bar{A}}_{(n-k)\times k} | \ \bar{\bar{I}}_{(n-k)\times(n-k)})$$

$$\bar{\bar{A}} = \bar{\bar{B}}^T$$

↳ egységmátrix

⑥

$$\overline{\overline{H}}_{3\times 5} = \left(\begin{array}{cc|ccc} \multicolumn{2}{c|}{B^T=A} & \multicolumn{3}{c}{I} \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right) \cdot \begin{pmatrix}0\\1\\1\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix} \Big\} n-k=3$$

$$\Uparrow \begin{pmatrix}1 & 1 & 0\\ 1 & 1 & 1\end{pmatrix}^T$$

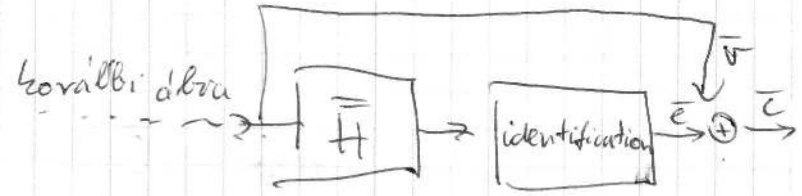
The "Key" Equation"

$$\underset{\text{given}}{\overline{\overline{H}}}\;\underset{\text{observable}}{\bar{v}} = \underset{\text{computable}}{\bar{s}^T} \leftarrow \text{syndrome vector} \Rightarrow \overline{\overline{H}}(\bar{c}+\bar{e})^T = \bar{s}^T \rightarrow \underbrace{\overline{\overline{H}}\bar{c}^T}_{\bar{0}^T} + \overline{\overline{H}}\bar{e}^T = \bar{s}^T$$

$\dim(\bar{s}) = n-k$

$$\boxed{\underset{\text{given}}{\overline{\overline{H}}}\,\bar{e}^T = \underset{\text{given}}{\bar{s}^T}}$$

we can identify e



$\overline{\overline{H}}$ nem invertálható mert nem négyzetes

e meghatározása search algorythm

$$E_{\bar{s}} = \left\{ \bar{e} : \overline{\overline{H}}\bar{e}^T = \bar{s}^T \right\}$$

pl:

$$E_{(001)} = \left\{ \boxed{(00001)}, (01110), (11000), (10111) \right\}$$

$\Downarrow$ legnagyobb valószínű

$$\bar{e}_s \quad \min_{\bar{e} \in E_{\bar{s}}} w(\bar{e})$$

| $\bar{s}$ | $\bar{e}_s$ |
|---|---|
| 000 | |
| 001 | 00001 |
| 010 | |
| 11 | |

$\overline{c} = \overset{?}{\overline{u}}\, \overline{G}_{k\times n}$

known　　given

Systematic

$\overline{c} = (\underbrace{u_1, \dots, u_k}_{\overline{u}}, p_{k+1}, \dots, p_n)$