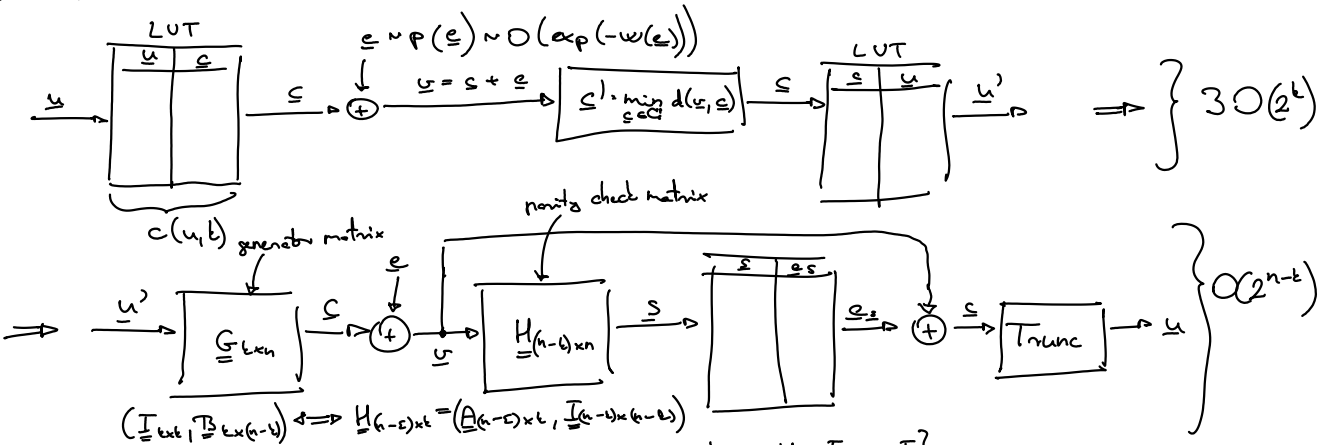
2016. szeptember 28., szerda 16:20



$(I_{k\times k} | B_{k\times(n-k)}) \Rightarrow H_{(n-k)\times n} = (A_{(n-k)\times k} | I_{(n-k)\times(n-k)})$

$E_s = \{ e : H e^T = s^T \}$

$e_s : \min_{e \in E_s} w(e)$

Lemma: if $e = H e^T = s^T$ then $e' = e + c = H e'^T = s^T = H e^T + H c^T = H e^T = s^T$

$C(5,2)$ $G_{2\times 5} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \Rightarrow H_{3\times 5} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

$s = (0\ 0\ 1)$

$E_s = \{(0\,0\,0\,0\,1), (0\,1\,1\,1\,0), (1\,0\,1\,1\,1), (1\,1\,0\,0\,0)\}$

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

$c^{(0)} = (0\,0\,0\,0\,0)$, $c^{(1)} = (0\,1\,1\,1\,1)$, $c^{(2)} = (1\,0\,1\,1\,0)$, $c^{(3)} = (1\,1\,0\,0\,1)$

Hamming codes - Constructing a code which can correct every single error
→ we need good channel in which the possibility of double errors are insignificant, so that single error detection is sufficient → wired MODEM connection

$e^{(i)} = (\ldots 0, 0, \underset{\uparrow}{1}, 0, 0 \ldots) \xrightarrow{??} "i"$
"i"-th bit

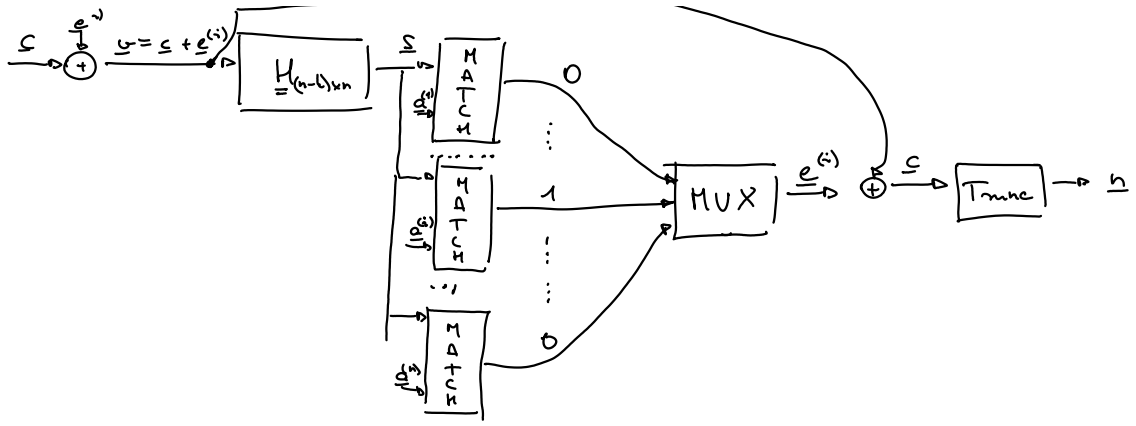
$H c^T = s$ ← computable → $H(c + e^{(i)})^T = s^T \Rightarrow \underbrace{H c^T}_{0^T} + H e^{(i)T} = s^T \Rightarrow H e^{(i)T} = s^T$
↑ given, ↑ observable

0^T ← column vector consists of only zeros

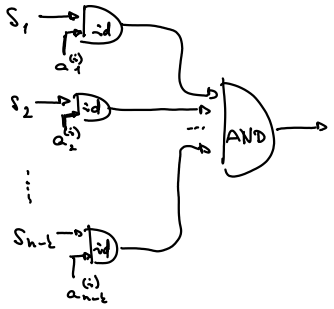
$\left(\begin{array}{c|c|c|c|c} e^{(1)T} & e^{(2)T} & \cdots & e^{(i)T} & \cdots & e^{(n)T} \end{array} \right) \cdot \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_1^{(i)} \\ a_2^{(i)} \\ \vdots \\ a_{n-k}^{(i)} \end{pmatrix} = a^{(i)T} = s^T$

$\dim(a^{(i)}) = n - k : \forall i = 1 \ldots n$

if they are equal, then we can identify "i" → so we can tell that there is an error on the bit in the "i"th position



Matcher circuit can be designed simply:



Criteria:

- $\underline{a}^{(i)} \neq \underline{0}$. $\forall i = 1 \dots n$
- $\underline{a}^{(i)} \neq \underline{a}^{(j)}$: $\forall i,j = 1 \dots n$, $i \neq j$

Length of code:

$C(n,k)$

$2^{n-k} - 1 = n$

$2^{n-k} = n + 1$

$\sum_{i=0}^{1} \binom{n}{i} = 2^{n-k}$

} for single-bit errors

General form: $\sum_{i=0}^{t} \binom{n}{i} = 2^{n-k}$ where t is the number of corrected bits

n	k
3	1
7	4
15	11
31	26

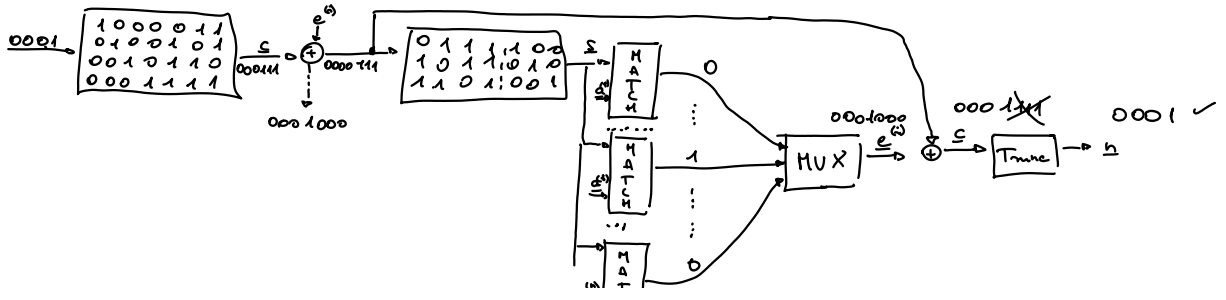
$C(7,4)$

$$\underline{\underline{H}}_{3\times 7} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \Rightarrow \underline{\underline{G}}_{4\times 7} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$1 < 2 < 3 < 4 < 5 < 6 < 7$

columns of parity check matrices are organized so that the decimal code is increasing

Example



Why do we love it so much?

$\frac{d_{min}-1}{2} = 1$

$d_{min} \geq 3$

$d_{min} \leq n-k+1 = 3-1+1$

$\Big\} \; d_{min} = 3 = n-k+1 \Rightarrow$ "This is my first MDS code!"