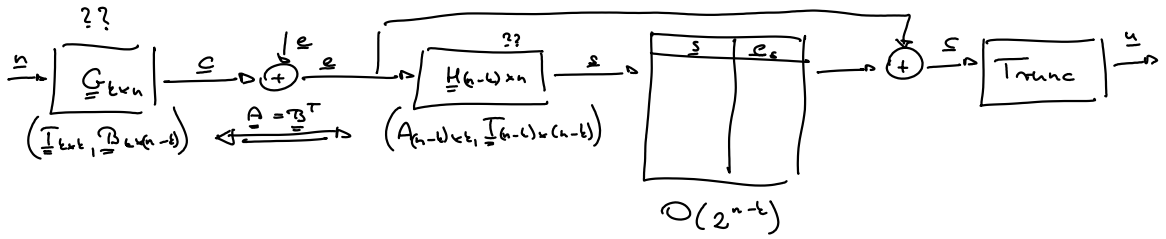
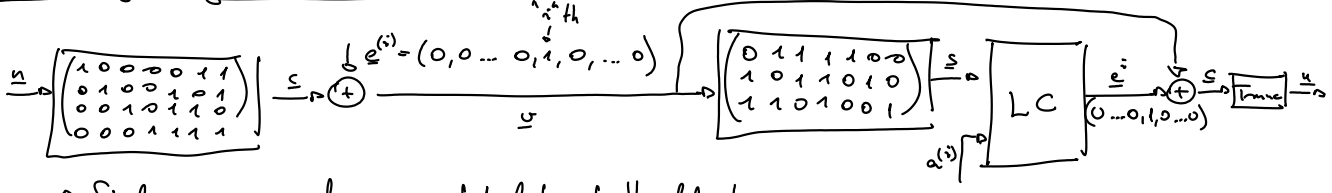
2016. szeptember 30., péntek 14:19

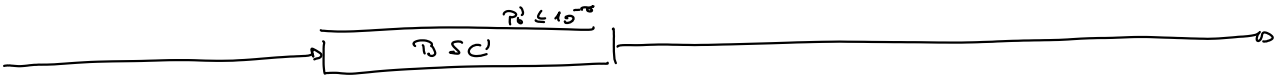


Correcting every single error (Hamming code)



$\Rightarrow$ Single error can be corrected, but not the block error

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



Given: P_b, γ (QoS - Quality of Service) $\Rightarrow P_b' < 10^{-\gamma}$ $\Rightarrow$ How to choose k and n?
bit error probability

$P_{\text{block error}} = P(\underline{s}\neq\underline{u}) = P(\underline{e}\neq\underline{c}) = \sum_{i=2}^{n} P_b^i (1-P_b)^{n-i}\binom{k}{i} = 1-(1-P_b)^k \le 10^{-\gamma}$

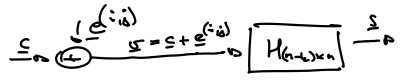
$\underline{e}=(\dots\underset{j_1}{1}\dots\underset{j_2}{1}\dots\underset{j_i}{1}\dots)$

$\Psi(P_b,\gamma) \Rightarrow n,k$ (we have to choose a k and n to fulfill the requirements above)

$\Rightarrow$ For example: $P_b \sim 10^{-2}$, $\gamma=5 \Rightarrow C(7,4)$

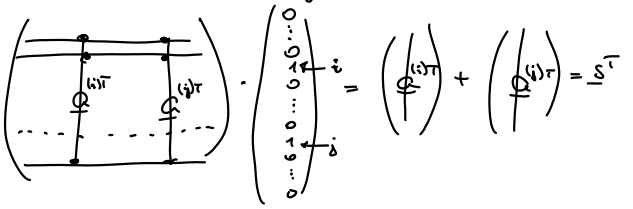
How to correct every double error?

$\underline{e}^{(i,j)}=(0\dots0\underset{i}{1}0\dots0\underset{j}{1}0\dots0) \rightarrow$ "i,j"



$\underline{H}\underline{v}^T=\underline{s}^T \Rightarrow \underline{H}(\underline{c}+\underline{e}^{(i,j)})^T=\underline{s}^T \Rightarrow \underline{H}\underline{c}^T+\underline{H}\underline{e}^{(i,j)}=\underline{s}^T \Rightarrow \underline{H}\underline{e}^{(i,j)T}=\underline{s}^T$

(given, given, given; given, given)



Criteria:

- $\underline{c}^{(i)}\neq 0 \quad \forall i=1\dots n$
- $\underline{c}^{(i)}\neq\underline{c}^{(j)} \quad \forall i,j=1\dots n,\ i\neq j$

} for single error

- $\underline{c}^{(i)}\neq\underline{c}^{(m)}+\underline{c}^{(l)} \quad \forall i,m,l=1\dots n,\ i\neq m\neq l$
- $\underline{c}^{(i)}+\underline{c}^{(j)}\neq\underline{c}^{(m)}+\underline{c}^{(l)} \quad \forall i,j,m,l=1\dots n,\ i\neq j\neq m\neq l$

} for double error

$\Rightarrow$ These 4 criteria can be substituted with one:

- 4 of the colum vectors of $\underline{A}$ must be linearly independent

Lemma: If a $C(n,k)$ linear code can correct "t" number of errors, then $\underline{H}_{(n-k)\times n}$

must have "2t" linearly independent column vectors

$t \rightarrow d_{min} = w_{min} = 2t+1$

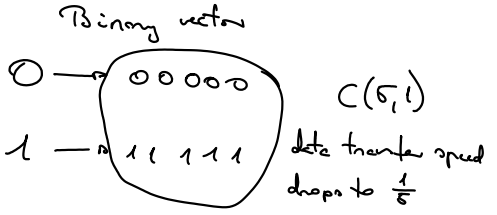
$\underline{b} \cdot w(\underline{b}) = 2t, \quad \underline{b} = (0 \dots 0\ b_{j_1} 0 \dots 0\ b_{j_2} 0 \dots 0\ b_{j_{2t}} 0 \dots 0)$

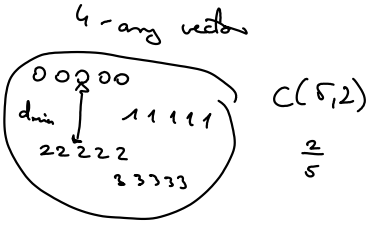
$\underline{\underline{H}}\, \underline{b}^T \neq \underline{0}^T$

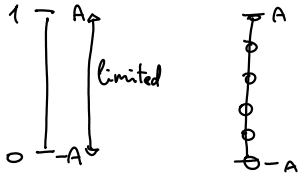
$\underline{\underline{H}}\, \underline{b}^T = \sum_{i=1}^{2t} b_{j_i} \alpha^{(j_i)^T} \neq \underline{0}^T$

⇒ Binary vectors are poor for being linearly independent

⇒ q-ary vectors are better for that $(n_i, c_i, v_i, e_i \in \{0, 1, \dots q\})$







Finite Algebra
Galois Fields