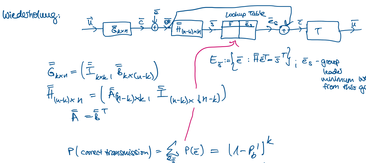
3. Lecture

Mittwoch, 13. September 2023 09:53

Wiederholung:



$\bar{G}_{kxn} = (\underset{k\times k}{\bar{I}} \; \underset{k\times(n-k)}{\bar{B}_{k\times(n-k)}})$

$\bar{H}_{(n-k)\times n} = (\underset{(n-k)\times k}{\bar{B}^T} \; \underset{(n-k)\times(n-k)}{\bar{I}})$

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

$E_{\bar{e}} := \{\bar{e} : \bar{H}\bar{e}^T = \bar{s}^T\}$, $\bar{e}_E$ - group leader minimum weight from this group

$P(\text{correct transmission}) = \sum_{\bar{e}\in E} P(E) = (1-p_b')^k$

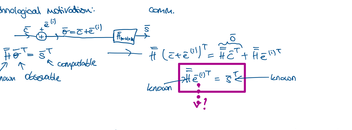
$\rightarrow$ BSC' $\rightarrow p_b'$

$p_b' \leq 10^{-\gamma} \quad \forall\, \gamma > 0{,}5$

DESIGN OF HAMMING CODE – BINARY LINEAR CODE FOR CORRECTING EVERY SIMPLE ERROR

$\bar{e}^{(i)} = (0\dots010\dots0) \rightarrow$? i ' what is „i"?

Technological motivation: comm.



$\bar{H}\bar{e}^T = \bar{s}^T$ ← computable

$\bar{H}(\bar{c}+\bar{e}^{(i)})^T = \bar{H}\bar{c}^T + \bar{H}\bar{e}^{(i)T}$

known decodable — known

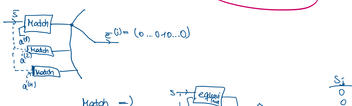
$\bar{H}\bar{e}^{(i)T} = \bar{s}^T$ known

$\bar{H}\bar{e}^{(i)T} = \bar{s}^T$ $\quad \dim(\bar{a}^{(i)}) = k-1$

$\begin{pmatrix} | & | & | & | & | \\ \bar{a}^{(1)} & \bar{a}^{(2)} & \bar{a}^{(3)} & \bar{a}^{(4)} & \bar{a}^{(5)} \\ | & | & | & | & | \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_1^{(i)} \\ a_2^{(i)} \\ a_3^{(i)} \\ a_{n-k}^{(i)} \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_{n-k} \end{pmatrix}$

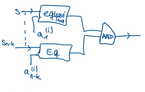
$\bar{s} = \bar{a}^{(i)}$ $\quad i = 1,\dots,n$

i determined by bijection



$\bar{e}^{(i)} = (0\dots010\dots0)$

Match ←



s_i	$a_i^{(i)}$	Eq
0	0	1
0	1	0
1	0	0
1	1	1

XOR

CONDITIONS:

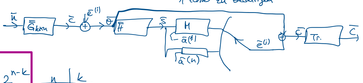
$\rightarrow \bar{a}^{(i)} \neq \bar{0}$

$\rightarrow \bar{a}^{(i)} \neq \bar{a}^{(j)}$

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

$n+1 = 2^{n-k}$ $\quad \sum_{i=0}^{1} \binom{n}{i} = 2^{n-k} \Rightarrow$ perfect code

$\Rightarrow$ code packt nicht lückenlos um Fehler zu korrigieren



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

n	k
3	1
7	4
15	11

Bsp: $c(7,4)$

$\bar{H}_{3\times7} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ ← not 0 vector & pairwise different columns

Standard $\Rightarrow \bar{G}_{4\times7} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

$P(\text{correct}) = (1-p_b)^n + n\, p_b (1-p_b)^{n-1} = (1-p_b')^k$

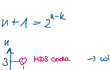
Given: p_b γ-GoS $\rightarrow$ find n,k mit $2^{n-k} = n+1 \rightarrow p_b' \leq 10^{-\gamma}$

(kann sich dass nicht ausreicht 1 Fehler zu finden/korrig)

$c(3,1)$ $\quad 3 \leq d_{min} \leq n-k+1 = 3 \Rightarrow d_{min} = 3$

$d_{min} = n-k+1$

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



Radio communication: $p_b \approx 10^{-2}$ need code of can correct multiple error

How to correct every double error?

$\bar{e}^{(ij)} = (0\dots0\overset{i}{1}0\dots0\overset{j}{1}0\dots0)$

$\bar{H}\bar{e}^T = \bar{s}^T \rightarrow \bar{H}(\bar{c}+\bar{e}^{ij})^T = \bar{s}^T \rightarrow \bar{H}\bar{e}^{(ij)T} = \bar{s}^T$

$\begin{pmatrix} | & | & | & | & | \\ \bar{a}^{(1)} & \bar{a}^{(2)} & \bar{a}^{(3)} & \bar{a}^{(4)} & \bar{a}^{(5)} \\ | & | & | & | & | \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \bar{a}^{(i)T} + \bar{a}^{(j)T}$

$\bar{s}^T$ Suchen in $\bar{H}$

conditions:
1) $\bar{s}^{(ij)} \neq 0$ ✓
2) $\bar{a}^{(i)} \neq \bar{a}^{(j)}$ ✓ von single error
3) $\bar{a}^{(i)} + \bar{a}^{(j)} \neq \bar{a}^{(k)}$ ✓ (nicht auftretende double error – single error)
4) $\bar{a}^{(i)} + \bar{a}^{(j)} \neq \bar{a}^{(k)}$ ✓

$\alpha_i \bar{a}^{(i)} + \alpha_j \bar{a}^{(j)} + \alpha_k \bar{a}^{(k)} + \alpha_m \bar{a}^{(m)} \neq 0$

$\Rightarrow$ linear unabh.

IF a code can correct "t" errors then 2t column vectors in $\bar{H}$ must be linearly independent.

$\bar{b} : w(\bar{b}) = 2t \qquad \bar{b} = (0\dots0\underset{i_1}{b_1}0\dots0\underset{i_{2t}}{b_{2t}}0\dots0)$

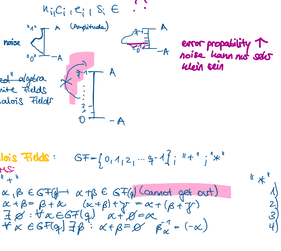
$\bar{b} \notin C \qquad 2t+1 = d_{min} = w_{min}$

$\bar{H}\bar{b} = \sum_{l=1}^{2t} b_{i_l} \bar{a}^{(i_l)T} \neq 0^T$

$\Rightarrow$ in binary codes nicht möglich

Lösung: $\Rightarrow q$-ary codes

$a_i, c_i, e_i, s_i \in$??



Galois Fields: $GF = \{0,1,2,\dots q-1\}$; i '+' j; '*'

AXIOMS:

'+'	'*'
1) $\alpha,\beta \in GF(q) \rightarrow \alpha+\beta \in GF(q)$ (cannot get out)	1) $\alpha,\beta \in GF(q) \rightarrow \alpha * \beta \in GF(q)$
2) $\alpha+\beta = \beta+\alpha$ $\quad (\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$	2) $\alpha*\beta = \beta*\alpha$ $\quad \alpha*(\beta*\gamma) = (\alpha*\beta)*\gamma$
3) $\exists\, 0 : \forall \alpha \in GF(q) : \alpha+0 = \alpha$	3) $\exists\, 1 : \forall \alpha \in GF(q) : \alpha*1 = \alpha$
4) $\forall \alpha \in GF(q) \exists \beta : \alpha+\beta = 0$ $\quad \beta = -\alpha$	4) $\forall \alpha \in GF(q) \setminus \{0\} \exists \beta : \alpha*\beta = 1 \Rightarrow \beta = \alpha^{-1} = \frac{1}{\alpha}$

Multiplik. Inverse

$(\alpha+\beta)*\gamma = \alpha*\gamma + \beta*\gamma$

MOD q algebra: 'q' is prime

$\alpha+\beta = p\cdot q+\gamma \Rightarrow \alpha+_p \beta \bmod q = \gamma$

↑ muss kleiner als q

$\alpha+\beta = p'\cdot q+\gamma' \rightarrow \alpha *_p \beta \bmod q = \gamma'$

$GF(7)$ $\quad 3*4 = 1\cdot7+5 \rightarrow 3\cdot4 \bmod 7 = 5$

$6+5 = 1\cdot7+4 \rightarrow 6+5 \bmod 7 = 4$

$2_M^{-1} = (-2)+5 \Rightarrow 2+\underline{5} = 1\cdot7+\emptyset$

$3_M^{-1} = \left(\frac{1}{3}\right) = \underline{5} \quad 3\cdot\underline{5} = 2\cdot7+1$

$5x+4 = 3$ $\quad GF(7)$ $\quad +1+\dots-1\cdot7+\emptyset$

$5x = -1$

$5x = 6$

$x = \left(\frac{1}{5}\right)6 \qquad 5\cdot\underline{3} = 2\cdot7+1$

$x = 3\cdot6$

$x = 18 \bmod 7$

$x = \underline{4}$

$\Rightarrow$ dass alle Elemente von $GF(7)$ entsprechen

Power table von $GF(7)$

	1	2	3	4	5	6
1	1	1	1	1	1	1
2	1	2	4	1	2	4
3	1	3	2	6	4	5
4	1	4	2	1	4	2
5	1	5	4	6	2	3
6	1	6	1	6	1	6

primitive Elemente

kann nur bei 3 & 5 aufgehen & alle Elemente von $GF(q)$ ausmachen

↑ mind. 1 primitive Element

1^1

2^1 $\quad 2^2$

$2^3 = 2^2\cdot2 = 3\cdot7+6$

3^1 $\quad 3^2 = 3\cdot3 = 2$

$3^3 = 3^2\cdot3 = 3\cdot2 = 6$

$3^4 = 3^2\cdot3^2 = 2\cdot2 = 4$

$3^5 = 3^4\cdot3^1$

$3^6 = 3^3\cdot3^3$