Linear Codes

Definition: A block code $C \subseteq \{0,1\}^*$ is called a linear code, if the elements from C form a linear vector space over the field $\{0,1\}$.

A linear code $C \subseteq \{0,1\}^n$ has as a vector space a dimension $dim(C)$
C is an $[n, dim(C)]$-code

Definition: Let C be an $[n,k]$-code.
i) A (k,n)-matrix G is called a base matrix for C, if the k rows of G form a base for C (as vector space).
ii) An $(n-k,n)$-matrix H is called a check matrix for C, if

$$C = \{c \mid c \in \{0,1\}^n, Hc^T = (0^{n-k})^T\}$$

holds.

Example

x_3	x_5	x_6	$x_3e_3(3) + x_5e_3(5) + x_6e_3(6)$	x_1	x_2	x_4	X
0	0	0	$(0,0,0)$	0	0	0	000000
0	0	1	$(1,1,0)$	0	1	1	010101
0	1	0	$(1,0,1)$	1	0	1	100110
0	1	1	$(0,1,1)$	1	1	0	110011
1	0	0	$(0,1,1)$	1	1	0	111000
1	0	1	$(1,0,1)$	1	0	1	101101
1	1	0	$(1,1,0)$	0	1	1	011110
1	1	1	$(0,0,0)$	0	0	0	001011

$$H_6 = \{000000, 010101, 100110, 110011, 111000, 101101, 011110, 001011\}$$

base matrix $G = \begin{pmatrix} 1\,0\,0\,1\,1\,0 \\ 0\,1\,0\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1 \end{pmatrix}$ check matrix $H = \begin{pmatrix} 1\,1\,0\,1\,0\,0 \\ 1\,0\,1\,0\,1\,0 \\ 0\,1\,1\,0\,0\,1 \end{pmatrix}$

Weight of a code

Definition: i) As the weight $w(c)$ of a word $c \in \{0,1\}^+$, we take the number of the symbols 1 occurring in c.
ii) The weight $w(C)$ of a block code $C \subseteq \{0,1\}^n$ is defined by

$$w(C) = \min\{w(c) \mid w \in C \setminus \{0^n\}.$$

Theorem: Let C be a linear $[n,k]$-code and H be a check matrix for C. Then, we have

$$\begin{aligned} w(C) &= \min\{r \mid \text{there are } r \text{ linear dependent columns in } H\} \\ &= \max\{r \mid \text{each } r-1 \text{ columns of } H \text{ are linear independent}\} \end{aligned}$$

Theorem: For a linear code C, we have $d(C) = w(C)$.

Some Estimations I

$$k(n,d) = \max\{dim(C) \mid C \subseteq \{0,1\}^n \text{ is a linear code with } d(C) \geq d\}$$

$$\begin{aligned}
k(n,d) &\leq k(n-1,d)+1\,,\\
k(n,d) &= k(n+1,d-1) \text{ for odd } d\,,\\
k(2n,2d) &\geq k(n,d)+k(n,2d)\,,\\
n(k+1,d) &> n(k,d) \quad \text{and} \quad n(k,d+1) > n(k,d)\,.
\end{aligned}$$

Some Estimations II

Theorem: For $k > 1$: $n(k,d) \geq n\left(k-1, \lceil \frac{d}{2} \rceil\right) + d$.

Corollary: For $k \geq 1$, we have

$$n(k,d) \geq \sum_{i=1}^{k-1} \lceil \frac{d}{2^i} \rceil \, .$$

Corollary: We have

$$k(n,d) \leq \max\{k \mid \sum_{i=1}^{k-1} \lceil \frac{d}{2^i} \rceil \leq n\} \, .$$

A method for constructing linear codes

Lemma: Let two linear codes C_1 and C_2 be given with the dimensions k_1 and k_2 and the code distances d_1 and d_2, respectively. Then

$$C = C_1 \alpha C_2 = \{(c_1, c_1 \oplus c_2) \mid c_1 \in C_1, c_2 \in C_2\}$$

is a linear code with

$$C \subseteq \{0,1\}^{2n}, \quad dim(C) = k_1 + k_2 \quad \text{and} \quad d(C) = \min\{2d_1, d_2\}\,.$$

Existence of linear codes with certain parameters

Theorem: If three natural numbers n, k, and d satisfy the conditions

$$k \leq n \quad \text{and} \quad 2^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i}$$

, then a linear code C exists with

$$C \subseteq \{0,1\}^n, \quad dim(C) = k \quad \text{and} \quad d(C) \geq d$$

(hence, $k(n,d) \geq k$).