IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises II.

1. How many different binary linear $[6,3]$ codes C fulfill the condition $C = C^{\perp}$?
2. Determine the number of k-dimensional subspaces of the vector space $V(n,q)$. Explain your reasoning.
3. Let C be a binary code of length n. Consider a binary code C' of length $n+1$ such that $x_1 \cdots x_n x_{n+1} \in C'$ if $x_1 \dots x_n \in C$ and $x_{n+1} = \bigoplus_{i=1}^{n} x_i$. Show that if C is a linear code, then C' is also a linear code.
4. Consider the binary linear code C spanned by the codewords 01111, 10111, 11011 and 01100.
   (a) Find a generator matrix of C.
   (b) Determine how many cosets C has and how many words each of them contains.
   (c) Construct a Slepian array for C and use it to decode 11111 and 00011.
5. Show that the set E_n of all vectors from $\mathbb{Z}_2^n$ which have even weight is a binary linear code. Find a generator matrix in a standard form for this code.
6. Let C be a binary linear $[n,k]$ code with a parity check matrix H. Consider a binary code C' of length $n+1$ such that $x_1 \cdots x_n x_{n+1} \in C'$ if $x_1 \cdots x_n \in C$ and $x_{n+1} = \bigoplus_{i=1}^{n} x_i$. Show that the matrix

   $$G = \begin{pmatrix} H & r^T \\ s & 1 \end{pmatrix},$$

   where $r = (00 \cdots 0)$ of length $n-k$ and $s = (11 \cdots 1)$ of length n, is a parity check matrix of the code C'.
7. Show that weight of any non-zero word of code $C^{\perp}$, where $C = Ham(r,2)$, is 2^{r-1}.
8. Suppose that the matrix

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

   is a parity check matrix of a linear code C. Find the distance of C and the non-zero word of minimum weight in C.