IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises II.

1. Decide which of the following codes are linear.
   a) binary code $C_1 = \{0000, 0011, 0110, 1001, 1010, 1100, 1111, 0101\}$
   b) quaternary code $C_2 = \{000, 312, 220, 132\}$
   c) ternary code $C_3 = \{0000, 0101, 1000, 1101\}$
2. Consider a binary $[n, k]$-code C with a parity check matrix
$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$
   a) Find $n, k, h(C)$ and $|C|$.
   b) Find the standard form generator matrix for C.
   c) Prove that $C^{\perp} \subset C$.
   d) Find coset leaders and the corresponding syndromes.
3. Consider a binary linear code. Prove that either all of the codewords begin with 0 or exactly half of the codewords begin with 0.
4. Compare P_{corr} when sending 16 messages unencoded to encoding using a Hamming code $\mathcal{H}_3$. Assume communication is over a binary symmetric channel with error probability p. Compare results for $p = 0.01$.
5. Let C be an $[n, k, d]$ code over $\mathbb{F}_q$. Prove that
   a) $A_0(C) + A_1(C) + \ldots + A_n(C) = q^k$.
   b) $A_0(C) = 1$ and $A_1(C) = A_2(C) = \ldots = A_{d-1}(C) = 0$.
   c) If C is a binary code containing the codeword $1 = 11\ldots1$, then $A_i(C) = A_{n-i}(C)$ for $0 \leq i \leq n$.
6. Let P_i be the set of all binary linear codes with weight equal to p_i, where p_i is the ith prime. Decide whether there exists a self-dual code ($C = C^{\perp}$) in P_i for all $i \in \mathbb{N}$.
7. Show that two vectors y_1 and y_2 are elements of the same coset if and only if
$$Hy_1^{\top} = Hy_2^{\top}.$$
8. a) How many cosets is contained in the Reed-Muller code R(1, m)? Explain your reasoning.
   b) Determine the lower bound for the number of cosets that have a unique leader in R(1, m). Explain your reasoning.