IV054 Coding, Cryptography and Cryptographic Protocols
2012 - Exercises II.

1. Decide which of the following codes are linear. Find the standard form of generator matrix for codes that are linear.

   (a) binary code $C_1 = \{00000, 00110, 00101, 10111, 10010, 10001, 10100, 00011\}$

   (b) ternary code $C_2 = \{000, 001, 110, 111\}$

   (c) quinary (5-ary) code $C_3 = \{000, 224, 132, 444, 312\}$

2. Consider the binary linear code C generated by the matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

   (a) Show that C is able to correct any one-bit error.

   (b) The set $\{11001011, 01110101, 10101010\}$ consists of exactly one codeword, one word obtained by making an error in exactly one bit and one word obtained by making an error in exactly two bits. Decide which word has which property. Explain.

3. Consider the 5-ary code C such that

$$a_1a_2a_3a_4 \in C \Leftrightarrow a_1 + 2a_2 + 3a_3 + 4a_4 \equiv 0 \pmod 5$$

   . Show that C is a linear code and find its generator matrix in standard form.

4. Given a linear code prove that the minimum distance equals the minimal weight among all non-zero codewords.

5. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for an $[n, k]$ code C. How many information sets are there for the binary repetition code of length n?

6. Let C_1 and C_2 be linear codes of the same length. Decide whether the following statements hold.

   (a) If $C_1 \subseteq C_2$, then $C_2^\perp \subseteq C_1^\perp$.

   (b) $(C_1 \cap C_2)^\perp = C_1^\perp \cup C_2^\perp$.

7. Show that there exists a $[2k, k]$ self-dual code over $\mathbb{F}_q$ if and only if there is a $k \times k$ matrix P with entries from $\mathbb{F}_q$ such that $PP^T = -I_k$.

8. Let M_i be the family of all binary linear codes with weight equal to m_i where m_i is the ith Mersenne prime (a prime of the form $2^j - 1$ for some $j \in \mathbb{N}$). For all $i \in \mathbb{N}$, decide whether there exists a self-dual code in M_i.