1. (a) Let E_n denote the binary even weight code of length n.

   (i) Prove that E_n is a linear code.

   (ii) Determine M, k, and d (in terms of n).

   (iii) Give the generator matrix G and the parity check matrix H. (Clearly state the dimension of the matrices).

   (iv) List all codewords of the dual code $E_n^{\perp}$.

   (b) Prove that in a binary linear code either all codewords have even weight, or exactly half of the codewords have even weight and half have odd weight. Also show that in a non-linear code this is not necessarily the case.

2. (a) Let $q = 11$ and $n = 10$. Consider the ISBN-code with

$$C_1 = \{x_1 x_2 \cdots x_{10} \in \mathbb{Z}_{11}^{10} : \sum_{i=1}^{10} i x_i \equiv 0 \bmod 11\}.$$

   (i) Show that $x_{10} = \sum_{i=1}^{9} i x_i \bmod 11$.

   (ii) Show that this code can be used to detect any single error.

   (iii) Show that this code can be used to detect any transposition, i.e. any swap of two symbols;
   e.g. 0123456789 $\leftrightarrow$ 0**4**23**1**56789.

   (iv) What is the minimum distance?

   (v) Can the code be used to correct an arbitrary single error?

   (vi) Can the code be used to detect an arbitrary pair of two errors?

   (b) Consider two other codes defined by

$$C_2 = \{x_1 x_2 \cdots x_{10} \in \mathbb{Z}_{15}^{10} : \sum_{i=1}^{10} i x_i \equiv 0 \bmod 15\}$$

and

$$C_3 = \{x_1 x_2 \cdots x_{10} \in \mathbb{Z}_{11}^{10} : \sum_{i=1}^{10} x_i \equiv 0 \bmod 11\}.$$

What are the disadvantages of these codes, compared with C_1?

3. (a) Define $A_q(n,d)$.

(b) Construct, if possible, binary (n,M,d)-codes with the parameters below. If no such code exists, state why.

(i) (7,2,7)

(ii) (2,4,1)

(iii) (6,3,5)

(iv) (12,400,5)

(c) (i) Prove the existence of a linear $[7,4,3]$ code.

(ii) From this show that $A_2(7,3) = 16$.

(iii) Prove the following theorem:
Let d be odd. A binary (n,M,d)-code exists
if and only if a binary $(n+1,M,d+1)$-code exists.

(iv) From (ii) and (iii) determine $A_2(8,4)$.

4. (a) Let the binary codes C_1, C_2, C_3 be defined by the following generator matrices:

$$G_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \text{ and } G_3 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

(i) Give generator matrices in standard form for these three codes.

(ii) Construct standard arrays for the three codes. Using the 3rd array decode 1101.

(b) (i) Assume the above codes and standard arrays are used for decoding. Let the error probability of a binary symmetric channel be p. For each of the three codes determine the probability $p_{\text{err}}(C)$ that any received vector is incorrectly decoded.

(ii) Assume that p is small. Compare the three codes: distinguish two applications, where in one of these high accuracy is most important, and in the other one a good rate is more important.

(c) The binary repetition code of length 3 is used for communication on a binary symmetric channel with error probability p in the following way: whenever an error is detected one asks for retransmission. Evaluate the overall probability of accepting an error.

5. (a) State the Singleton bound on $A_q(n, d)$.

(b) Prove the Gilbert-Varshamov bound

$$A_q(n, d) \geq \frac{q^n}{\sum_{r=0}^{d-1} (q-1)^r \binom{n}{r}}.$$

(c) (i) Define a Hadamard matrix of order m.

(ii) Prove: If a Hadamard matrix of order m exists, then also one of order $2m$ exists. Deduce that a Hadamard matrix of order $2m$ exists, for each $m = 2^k$, $(k = 0, 1, 2, \ldots)$.

(d) Prove that $A_q(4, 3) = q^2$ if and only if there exists a pair of orthogonal Latin squares of order q.

END **Christian Elsholtz**