1. (a) Let C be a binary $[n, k, d]$-code. Explain what is meant by the terms

   (i) generator matrix G for the code C

   (ii) standard form for G

   (iii) parity-check matrix H for C.

   (b) Let C consist of all binary even weight codewords of length $n = 4$. Determine all codewords of C and determine M, k and d.

   (c) Prove that the binary code E_n of all even weight codewords of length n is linear. Determine M, k and d.

   (d) Find for the code E_4 a standard form for

   (i) the generator matrix G and

   (ii) the parity check matrix H.

   (e) Construct, if possible, binary (n, M, d)-codes for each of the following parameter sets. When no such (n, M, d)-code exists, explain why.
   $(6, 2, 6), (3, 8, 1), (4, 8, 2), (5, 3, 4), (8, 30, 3)$.

2. Let C be a q-ary (n, M, d)-code.

(a) Define the Hamming distance $d(\vec{x}, \vec{y})$ between any two vectors $\vec{x}, \vec{y} \in V(n, q)$.

(b) (i) State and prove the sphere-packing-bound.

(ii) Define the term "perfect code".

(iii) Using $d(\vec{x}, \vec{y}) = w(\vec{x} - \vec{y})$ show that the minimum distance of a linear code C is given by the minimum weight of any non-zero codeword, (i.e. show that $d(C) = w(C)$).

(c) Let C be the binary $[7, 4]$ code with generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$.
Determine d, justifying your answer, and hence show that C is a perfect code.

(d) Show that for a binary perfect code d is odd.

(e) Give (without proof) two examples of families of binary perfect codes.

3. Let C be a q-ary $[n, k, d]$-code. Let G denote its generator matrix, and H its parity-check matrix, both given in standard form.

(a) Define the terms coset, coset leader and syndrome.

(b) Describe how to construct a standard array and a syndrome look-up table. Explain how the standard array and the syndrome look-up table can be used for decoding with error correction. Explain the advantage of using the syndrome look-up table over the standard array.

(c) Prove that two vectors $\vec{u}, \vec{v}$ are in the same coset if and only if they have the same syndrome $S(\vec{u}) = S(\vec{v})$.

(d) Explain why constructing the syndrome look-up table is particularly effective in the case of a perfect code with $d = 2t + 1$.

(e) Suppose C is a code with $d = 2t + 2$. Explain the idea of incomplete decoding on a channel, where retransmission is possible.

4. Define the term "binary symmetric channel" with cross-over probability p. Such a channel is used in one of the following two schemes.

a) Using a 3-repetition code, correcting one received error. ((((corrected version))))

b) For any pair of message bits a parity check bit is used. For any detected error retransmission is requested.

For each scheme

a) find the eventual probability of accepting an error.

b) find the expected number of bits that have to be transmitted per message bit.

Calculate the above quantities for both schemes a) and b) with $p = \frac{1}{10}$ and $p = \frac{1}{100}$.
Compare the relative merits of these schemes.
Which scheme do you suggest to use for $p = \frac{1}{100}$?

5. (a) Define the binary Hamming code $Ham(r, 2)$ by means of its parity-check matrix.

(b) Prove that $Ham(r, 2)$ is a $[2^r - 1, 2^r - r - 1]$-code.

(c) Prove that $Ham(r, 2)$ has minimum distance $d = 3$. (i.e. show that there are no codewords with weight 1 or 2, but that there is a codeword with weight 3).

(d) Give the parity-check matrix for $r = 2$ and $r = 3$ in standard form.

(e) Alice and Bob play the following game: Alice thinks of an integer $1 \leq a \leq 1,000,000$. Bob asks questions which Alice answers with yes or no.

Explain how $Ham(5, 2)$ can be used to to show that Bob can determine a in 25 questions, even if Alice is allowed to lie once.

Use the sphere-packing bound to show that generally 24 questions do not suffice.

(f) Prove the Singleton bound $A_q(n, d) \leq q^{n-d+1}$.

(g) Show that a latin square exists of any order q.

(h) Show that $A_q(4, 3) = q^2$ if and only if there exists two mutually orthogonal latin squares.

END **Christian Elsholtz**