Ex. 1
To determine the minimum distance of a general code one needs $\binom{M}{2}$ comparisons. Show that for a linear code the minimum distance is given by the minimum weight of any non-zero codeword.
Further show that C has distance d if and only if any $d-1$ rows of a parity check matrix H are linearly independent but there exist d rows which are dependent.

Ex. 2

a) Alice and and Bob play the following game: Alice thinks of a number $n \in \{1, 2, \ldots, 1\ 000\ 000\}$. Bob is allowed to ask questions. Alice will answer them truthfully with yes or no, only, but is allowed to lie at most once.

   What is the minimum number of questions Bob has to ask that *guarantees* that he correctly finds the number (i.e. even if Alice thinks of a difficult number and is very clever with her answers).

   Use the Hamming-code Ham$(5, 2)$ to show that 25 questions will suffice. But also show by the sphere packing bound that 24 questions do not suffice in general.

   Describe the procedure to ask the questions.

b) Since it may be tedious to write down the generator and parity check matrix in a): Explain with Ham(3,2) and a suitable parity-check matrix H (and generator matrix G) how to formulate the questions, and to correct the lie, as explicit as possible.
   You can describe it with an example but it should be clear that this is a typical general case.
   Does your method work if Alice did not lie at all?

c) What happens, if Alice changes her number during the game(!!??) (according to the rule that still at most one answer is wrong)?