Ex. 1
Alice 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 and Alice will answer them by yes or no, but is allowed to lie once.
So far we know: there is a strategy that allows to find the number in 41 questions. Generally, one certainly needs 20 questions. Model this question in terms of error correcting codes. Use your existing knowledge on correction of one bit to find better lower and upper bounds on the number of questions in the worst case, given the optimal strategy. Describe your procedure, describe the questions.

Ex. 2
Let C be the binary linear code with generator matrix $\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$.
Find a generator matrix for C in standard form. Is this the same code as that in example 5.8 of the lecture? (Or is it equivalent to that code?)

Ex. 3
Construct standard arrays for codes having each of the following generator matrices:

$$G_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad G_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Using the third array decode the received vectors 11111 and 01011. Give two examples of
a) two errors in a codeword and being corrected and
b) two errors in a codeword and not being corrected.

Ex. 4
If the error probability of a binary symmetric code is p, calculate the probabilities for each of the three codes from the previous exercise that any received vector will be decoded as the codeword which was sent. Evaluate these probabilities for $p = 0.01$.
Now suppose each code is used purely for error detection. Calculate the respective probabilities that the received vector is a codeword different from that sent, and evaluate this for $p = 0.01$. Comment on the merits of these three codes.

Ex. 5
We have assumed that, for a binary symmetric channel, the symbol error probability p is less than $1/2$. Can an error correcting code be used to reduce

the number of messages received in error if
a) $p = 1/2$
b) $p > 1/2$?

Ex. 6
Suppose C is a binary $[n, k]$ code with minimum distance $2t + 1$ (or $2t + 2$). Given that p is very small, show that an approximate value of $P_{\text{err}}(C)$ is

$$\left(\binom{n}{t+1} - \alpha_{t+1} \right) p^{t+1},$$

where α_{t+1} is the number of coset leaders of C of weight $t + 1$.

Ex. 7
Suppose the perfect binary $[7, 4]$ code (see problem sheet 2 and examples in the lectures!) is used for error detection and suppose that $p = 0.01$. Evaluate the probability that a retransmission needs to be requested and evaluate the probability that an error is undetected in the first step, and evaluate that overall probability an error is undetected, even after retransmission.

Ex. 8
(Exam question 2000)
Define the term "binary symmetric channel with cross-over probability p". Such a channel is used to send a message using one of two possible schemes as follows:-
A. using a 4-repetition code, and requiring retransmission as often as necessary when any errors are detected;
B. using a 5-repetition code, correcting one received error but requiring retransmission as often as necessary when two errors are detected;
For each of these schemes,

1. find the overall probability of accepting an error;
2. find the expected number of bits that have to be transmitted per message bit.

Calculate the above quantities for $p = 0.01$ and $p = 0.1$.
Explain the relative merits of these methods under various circumstances.
Suggest a possible scheme if retransmission is not possible.