Problem sheet 2
2018

Codierungstheorie und Kryptographie

8. Let C be a linear $[n,k]$-code. Show that $C^\perp$ is a code of dimension $n-k$ and that $\left(C^\perp\right)^\perp = C$ holds.

9. A binary symmetric channel with symbol error probability p and a code C will be used for error detection only, i.e. not for automatic correction.

   Adapt the formula $\sum_{i=1}^{n} \alpha_i p^i (1-p)^{n-i}$ (that we found for error correction) for the probability of correct (incorrect) detecting an error.

   Now work out these probabilities for the $[7,4]$-code, depending on p.

10. The information 0101 shall be sent over a channel, with the $[7,4]$-code. Which codeword will be transmitted?.
    Suppose that 1010101 is received, what was (with high probability) the codeword originally sent, and what was the message before decoding? (Use syndrome decoding).

11. The $[7,4]$-code is extended to an $[8,4]$-code with a parity check bit. What is the minimum distance of teh code?

    If a word with distance 1 from a codeword is received, then maximum likelihood decoding would decode it as this codeword.

    What is the probability that this error correction does not lead to the codeword originally sent? Does the propability depend on the words considered?

    Whatever your answer, is this generally trues for other codes?

not to be handed in Recommended reading on combinatorial back ground to construct some nontrivial codes.
Lecture notes of Anderson and Honkola, (A Short Course in Combinatorial Designs.)
http://www.utu.fi/fi/yksikot/sci/yksikot/mattil/opiskelu/kurssit/Documents/comb2.pdf
In particular read Definition 3.1., which defines a $t-(v,k,\lambda)$ design. Designs can be used to construct codes.

12. Let C be the (linear) code over $\mathbb{F}_2^8$, defined by the generator matrix $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$. Prove that 14 words have weight 4, (all words apart from 00000000 and 11111111). ((You can use a computer if you like.))

    Show that these 14 words define a $3-(8,4,1)$ design .

not to be handed in Search at http://www.freepatentsonline.com/
for "Hamming code".

13. In this exercise we construct a quite large and interesting code. (Computer help recommended.)

    Let C be the (linear) code $C \subset \mathbb{F}_3^{12}$, defined by all $3^6 = 729$ linear combinations over the 6 rows of the generator matrix

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

    Prove (possibly by a computer check) that the minimal non-zero weight (of all codewords) is six. How many words have weight six? (Note that they come in pairs, c and $-c$, Now, from this one finds 132 codewords of wight six which are the blocks of a $5-(12,6,1)$ design, the so-called Mathieu 5-design on 12 points. (Using a computer it can be easily tested that each subset of 5 of the 12 positions occurs exactly once).

    How often do quadruples, triples, pairs, single elements occur, respectively?

    Do these 132 words form an e-error correcting code? If yes, for which e? Is it a perfect code?

    Now, delete the first column of G. What does it mean in terms of a code (linear?, minimum weight? how many codewords?). Does this give a $4-(11,5,1)$ design? Is the corresponding code perfect?

    ((For comparison, the quite similar matrix

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

    does not work, the minimum (non-zero) weight is 5 etc.))

Not to be handed in Study Theorem 4.9 of the lecture notes of Anderson and Honkola, (A Short Course in Combinatorial Designs.)
(Start reading on page 35.)

http://www.utu.fi/fi/yksikot/sci/yksikot/mattil/opiskelu/kurssit/Documents/comb2.pdf

14. If you search (in the mathematical literature) for perfect codes, you will find some information on (an) infinite family/ies) of codes, and a few further codes. Briefly list what is known.