Problem sheet 3
2018

Codierungstheorie und Kryptographie

12. In this exerice we construct a quite interesting code! Let us start with the $[24, 12, 8]$ Golay-code G_{24} generated by.

$$G = \begin{pmatrix} 1,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,1,1,0,0,0,1,0,1 \\ 0,1,0,0,0,0,0,0,0,0,0,0,1,0,1,1,1,0,0,0,1,0,1,1 \\ 0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,0,1,0,1,1,1 \\ 0,0,0,1,0,0,0,0,0,0,0,0,1,1,1,0,0,0,1,0,1,1,0,1 \\ 0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,0,0,1,0,1,1,0,1,1 \\ 0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,1,0,1,1,0,1,1,1 \\ 0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1,1,0,1,1,1,1 \\ 0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,1,1,0,1,1,1,0,1 \\ 0,0,0,0,0,0,0,0,1,0,0,0,0,1,0,1,1,0,1,1,1,0,0,1 \\ 0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,1,0,1,1,1,0,0,0,1 \\ 0,0,0,0,0,0,0,0,0,0,1,0,0,1,1,0,1,1,1,0,0,0,1,1 \\ 0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,0 \end{pmatrix}$$

(I would suggest that you programme some of the following so that you can do some experiments, I can provide G in mathematica or tex code). reorder the columns so that the word 111111110000000000000000 of weight 8 exists. Why does $d = 8$ in G_{24} imply that there is some generator matrix whose first 8 columns are?

$$G' = \begin{pmatrix} 1,0,0,0,0,0,0,1 \\ 0,1,0,0,0,0,0,1 \\ 0,0,1,0,0,0,0,1 \\ 0,0,0,1,0,0,0,1 \\ 0,0,0,0,1,0,0,1 \\ 0,0,0,0,0,1,0,1 \\ 0,0,0,0,0,0,1,1 \\ 0,0,0,0,0,0,0,1 \\ 0,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0 \\ 0,0,0,0,0,0,0,0 \end{pmatrix}$$

Show that there are 32 codewords (of length 24) starting with 00000000. Similarly with $10000001, 01000001, 00100001, 00010001, 00001001, 00000101, 00000011$. This gives 256 words. Now delete the first 8 positions of these 256 words. Show that these new 256 words of length 256 define a $(16, 256, 6)$ code. Deduce that a $(15, 256, 5)$ code exists.

Compare the last parameters with the sphere packing bound.

The parameters are amazingly good. From this $(15, 256, 5)$-code you can obtain a $(12, 32, 5)$ code. Even this code still has optimal parameters!

Now, is the $(16, 256, 6)$-code linear? Have a guess...

13. Prove that there is no linear $[13, 6, 5]$-code. Suppose there is one, then start with a generator matrix of type $\begin{pmatrix} 11111 & * * * * * * ** \\ G_1 & G_2 \end{pmatrix}$. Show that G_2 would define a linear $[8, 5, 3]$-code. Why does this give a contradiction? Show that this implies that there are no $[15, 8, 5]$ and $[16, 8, 6]$-codes.

14. Prove the Plotkin bound $A_2(2d, d) \leq 4d$ in case d is even.

15. A Hadamard matrix H_n is an $n \times n$-matrix with entries in $\{-1, 1\}$ and the property that $HH^t = nI_n$. Try to construct some small Hadamard matries $n = 2, 3, 4, 5, 6, 8, 12$. Prove: If Hadamard matrices of order n and m exist, then also of order nm. Conclude that they do exist for $n = 2^k$. Use a Hadamard matrix H with $n = 2^k$ to construct a good code, (which parameters?) For which of the general code bounds are the codes constructed by Hadamard matrices sharp?

16. 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).

    (Describe the procedure to ask the questions, in case that is very difficult, choose a samller example.) Does your method work if Alice did not lie?

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