Problem sheet 2
2005, Jan. 20

MT361 Error correcting codes

Ex. 1
Construct, if possible, binary (n, M, d) codes, with the parameters below. If no such code exists, explain why.

a) (6,2,6)

b) (3,8,1)

c) (4,8,2)

d) (5,3,4)

e) (8,30,3)

Ex. 2
Show that $A_2(8, 5) = 4$.

Ex. 3
Show that $A_2(8, 4) = 16$.

Ex. 4
State and prove the sphere-packing bound.

Ex. 5
Given a binary code. State and prove a connection between the distance between two code words and the weights of the codewords.

Ex. 6
Let $E_n \subset F_2^n$ denote the set of all vectors with even weights. Deduce that E_n is the code that is obtained by adding a parity check to the code $C = F_2^{n-1}$. Deduce that E_n is an $(n, 2^{n-1}, 2)$-code.

Ex. 7
Prove that $A_q(3, 2) = q^2$.

Ex. 8
Show: If binary (n, M, d)-code exists, with d even, then there also exists a binary (n, M, d)-code in which all the codewords haven even weight.

Ex. 9
(Not to be handed in!)
Work through this example.
$C = \{(00000, 01101, 10110, 11011)\}$ defines a $(5, 4, 3)$-code. So, $A_2(5, 3) \geq 4$. We want to show that no code with $n = 5, M = 5, d = 3$ exists. An exhaustive search would be possible, with a computer. But the following procedure is much more effective:
Let C be a $(5, M, 3)$-code with $M \geq 4$.
By our discussion on equivalent codes we may assume w.l.o.g. that $00000 \in C$. C can contain at most one codeword with weight 4 or 5, since any two such codewords would have distance at most 2. Also, because of $d = 3$ there cannot be any codeword with just one or two ones, since the distance to 00000 would be at most 2. Since $M \geq 4$, there must be at least 2 codewords containg exactly 3 ones. By rearranging the positions we can assume that one of these is 11100. The other one can have at most one of its three ones in the first three position, (otherwise the distance to 11100 would be ≤ 2. So we can assume w.l.o.g. that the third codeword is 00111.
Now, after some trial and error attempts we find that the only possible fourth codeword is 11011. This proves that $A_2(5, 3)$.
This type of argument reduces any exhausting search considerably!
It also proves that there is, up to equivalence, exactly one $(5, 4, 3)$-code.

Ex. 10
(Not to be handed in!)
We had considered a non-trivial perfect binary $(7, 16, 3)$-code. Make yourself familiar with this example.

$$
\begin{array}{ccccccccc}
\vec{0} & = & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\vec{a_1} & = & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
\vec{a_2} & = & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
\vec{a_3} & = & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
\vec{a_4} & = & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
\vec{a_5} & = & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
\vec{a_6} & = & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
\vec{a_7} & = & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
\vec{b_1} & = & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
\vec{b_2} & = & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
\vec{b_3} & = & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
\vec{b_4} & = & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
\vec{b_5} & = & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
\vec{b_6} & = & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
\vec{b_7} & = & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
\vec{1} & = & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}
$$

When evaluating the minimum distance you would need to compare $16 \times 15/2$ pairs. By the cyclical construction this can be much reduced;

Compare $\vec{0}$ with $\vec{1}$ and $\vec{a_1}, \vec{b_1}$. (3)
Compare $\vec{1}$ with $\vec{a_1}, \vec{b_1}$. (2)
Compare $\vec{a_1}$ with $\vec{a_i}$, $i = 2, 3, \ldots, 7$. (6)
Compare $\vec{a_1}$ with $\vec{b_i}$, $i = 1, \ldots, 7$. (7)
Compare $\vec{b_1}$ with $\vec{b_i}$, $i = 2, 3, \ldots, 7$. (6)
These 24 comparisions suffice, (this number can be further reduced by methods that we learn at a later stage in the course). Note that the minimum distance is $d = 3$. Check that the sphere packing bound is sharp here.

Hand in solutions at the beginning of the lecture on Thursday 27th January.
I've put some books in the restricted loan section of the library. Recommended reading is R. Hill: A First course in coding theory. (001.539 Hil)
An electronic version of the problem sheets is available:
http://www.ma.rhul.ac.uk/~elsholtz/WWW/lectures/0405mt361/lecture.html