
Below we use the following notation:
Txbk – "Codinig theory and Cryptography" by Hankerson & others.

We may also use notations:
♢ – the proof is not obligatory,
♦ – an important topic, the proof in particular.

Content of lectures 5-6.

Lecture 5.

Constructing a code from its parity check matrix H: main steps.
♦ How the minimal distance of the code can be determined from H ?
The "singleton bound" theorem.
Equivalent codes.
♦ The "Varshamov-Gilbert bound" theorem.
†Txbk: 2.7, 2.9, 2.8, 3.1.
‡. See also [Pless]: 2.3, 1.2.

Lecture 6.

MDS codes. Orthogonal codes (are called dual codes sometimes).
♦ If a code is MDS then its orthogonal is MDS too.
Syndrom decoding: cosets, coset leaders.
Cyclic codes (beginning of the topic).
♦ Cyclic codes correspond (bijectively) with ideals.
†Txbk: 2.2, 2.5, 3.1, 2.10-2.11, 4.1-4.2.
‡See also [Pless]: 2.3, 2.1, 5.1.