

The questions which will appear in exam tickets are presented below. The ticket will include two questions and a problem. The first question will be devoted to information theory, the second question will be devoted to coding theory. You are allowed to use any literature. Good luck!

1. Measures of information. Entropy, joint entropy, conditional entropy, relative entropy (or Kullback-Leibler divergence). Mutual information, connection to entropy. Jensen's, log sum, data processing and Fano's inequalities.
2. Data compression. Uniquely decodable and prefix codes. Kraft inequality. Source coding theorem. Huffman coding. Universal source coding.
3. Noisy transmission channels. Discrete memoryless channel, symmetric channel. Channel capacity. Channel coding theorem (Shannon's theorem and converse).
4. Differential entropy. Gaussian channel and its capacity. Parallel Gaussian channels and water filling.
5. Multi-user channels. Multiple access channel (MAC), broadcast channel and their capacities.
6. Block codes. Boolean cube as a metric space: Hamming distance, ball, sphere, layer. Code, minimal code distance. Maximum likelihood decoding and bounded minimum distance decoding. Detection and correction of errors, geometric interpretation.
7. Bounds on the code parameters. Definition of $A_q(n, d)$. Hamming, Gilbert, Singleton and Plotkin bounds. Asymptotic regime.
8. Linear codes. Definition and main parameters. Generator and parity-check matrices. Theorem on the parity-check matrix of linear code and its minimum distance. Varshamov–Gilbert bound. Syndrome and syndrome decoding.
9. Dual code, weight enumerator and MacWilliams identity.
10. Binary Hamming codes, extended Hamming codes. Perfect codes. Syndrome calculation and decoding of Hamming codes. Non-binary Hamming codes.
11. Reed-Muller codes and their parameters. Plotkin construction.
12. MDS codes and their properties. Reed–Solomon codes and Discrete Fourier Transform. Decoding algorithm: key equation, Euclidean algorithm, Chien search and Forney's algorithm.
13. Reed–Solomon codes. List decoding. Polynomial reconstruction and Sudan's algorithm.
14. Polynomial codes. Cyclic codes. Equivalence of polynomial and cyclic codes. Generator and check polynomials. Generator and parity-check matrices. Non-systematic and systematic encoding. Definition of cyclic code with use of roots of generator polynomial. Cyclic codes and bursts of errors. CRC codes.
15. BCH codes and their parameters. Design distance and parity-check matrix. BCH codes as subcodes of Reed–Solomon codes, Euclidean decoding algorithm.
16. Asymptotically good family of codes, asymptotic properties of Hamming, Reed-Muller and BCH codes.
17. Concatenated codes and their parameters. Zyablov bound. Decoding algorithm. Generalized minimum distance (GMD) decoding. GMD for concatenated codes.
18. Convolutional codes. Definition and main properties. Soft decoding. Code tree, finite state machine and trellis representations. Free distance. Dynamic programming principle and Viterbi decoding algorithm.

19. LDPC codes, Tanner graph representation. Graph codes. Bit-flipping decoding algorithm. Expander graph, expander mixing lemma. Sipser–Spielman and Zemor codes.
20. Factor graph. Marginalization via message-passing for trees (Sum-Product algorithm). Decoding of LDPC codes via message-passing.
21. Construction of LDPC codes. Waterfall and error-floor regions. Irregular LDPC codes. Density evolution for BEC, threshold. Trapping sets, cycles and progressive-edge grows algorithm. Protograph-based and quasi-cyclic LDPC codes.
22. Polar codes. Polarization, “virtual” channels. Encoding, frozen bits. Successive-cancellation decoding algorithm.