Nonexhaustive list of questions for the exam of Information Theory and Application (Part 1: Information Theory and Theoretical Security)

Giorgio Taricco

2019/2020

1. Illustrate the basic concepts on probability: probability spaces, events, outcomes, probability function, σ-algebra assumptions.
2. Illustrate the basic properties of probabilities.
3. Define random variables, expectation, and their basic parameters.
4. Introduce the basic concepts on information sources.
5. Define the basic concepts from information theory until the definition of entropy.
6. Prove in detail all the entropy inequalities.
7. Define the joint and conditional entropies and show that the entropy of a function of a discrete random variable is lower than the entropy of the random variable itself.
8. Define the mutual information and the relative entropy with their relationships and inequalities.
9. Define the entropy rate of a general information source and a Markovian source.
10. Explain in detail the meaning of fixed-to-fixed and fixed-to-variable source coding.
11. Describe in detail the classification of source codes.
12. Illustrate the Kraft and McMillan inequalities with detailed proofs and applications.
13. Illustrate the Shannon Theorem for source coding and its proof.
14. Describe in detail the Huffman coding algorithm.
15. Describe in detail the MAP rule.
16. Illustrate the concept of channel codes and Shannon's Theorem for channel coding (theoretical statement and practical application).
17. Illustrate the channel capacity in general and when the channel matrix has rows permutations of each other.
18. Illustrate and derive in detail the capacity of a strictly symmetric discrete channel and of the binary symmetric channel.
19. Derive in detail the capacity of a binary input symmetric output channel and of the binary erasure channel.
20. Derive in detail the capacity of the binary asymmetric channel and of the Z channel.
21. Illustrate the Blahut-Arimoto Theorem and prove the basic result supporting this theorem.
22. Illustrate in detail the data-processing inequality.
23. Illustrate the concept of discretization for continuous random variables and its detailed application leading to the differential entropy.

24. Illustrate in detail the properties of the mutual information between continuously-distributed random variables.

25. Derive in detail the capacity of the additive Gaussian channel and the differential entropy inequality for Gaussian random variables.

26. Illustrate in detail the weighted water-filling algorithm.

27. Illustrate in detail the concepts of perfect secrecy and "one-time pad" for a secure communication system.

28. Illustrate the concept of "one-time pad" and the Maurer scheme along with their connection.

29. Derive the output of an LFSR with N cells and connection coefficients $c_0, c_1, \dots, c_{N-1}$ (general case).

30. Derive the period and the output of an LFSR with N cells and given connection coefficients $c_0, c_1, \dots, c_{N-1}$ (specific case with numerical data).

31. Illustrate in detail if and how an LFSR can be used as a stream cipher.

32. Illustrate the A5/1 algorithm and its properties.

33. Illustrate the concept of unicity distance and apply it to the following encryption scheme (to be specified).

34. Illustrate the wiretap channel and derive the secrecy capacity of a binary symmetric wiretap channel.