

Information Theory (Teoria informacji)
Cele kształcenia
The student will acquire basic knowledge in the field of application of the main concepts of information theory such as entropy, mutual information or relative entropy and their properties. He will also learn the capacities of communication channels and methods of estimating them. Acquiring this knowledge will result in understanding of the possibilities and limitations of communication as well as will provide an introduction to other courses of quantum information theory. The student will be able to apply the knowledge learned in whatever context it can be used, including physics, statistics and cryptography.
Treści programowe
The course contents includes presentation of the following concepts (lecture and exercises will be devoted to the same topics): <ol style="list-style-type: none"> 1. Shannon entropy function, its interpretation and properties, 2. Entropy functions of many variables, including conditional entropy, mutual information, relative entropy, conditional mutual information and their properties, including data processing inequality and the chain principle for conditional mutual information, 3. "Asymptotic Equipartition Property" theorem, compression codes (including Huffman's), Lempel-Zif compression algorithm, 4. Error correction codes (Huffman, CSS, other line codes), 5. The concept of typical and total typical sequences, Shannon's theorem on the capacity of a communication channel, random code technique 6. Capacities of selected communication channels (among others, broadcast channel, multiple access channel, erasure channel) and Slepian-Wolf theorem on joint coding, 7. Interpretation of relative entropy in the context of betting, 8. Kolmogorov complexity and Kraft and Mc Millan inequality, 9. The use of IT in cryptography (secure key agreement) including the Csisar & Koerner theorem and the protocol increasing security by means of two-way communication by U. Maurer and non-increasing (so-called monotonous) security functions. 10. Application of IT in quantum communication: von-Neumann entropy versus Shannon entropy similarities and differences; quantum conditional entropy versus Shannon's conditional entropy - comparison.
Wykaz literatury
A. Literature required to pass the course <ul style="list-style-type: none"> • E. Shannon, W. Weaver, The Mathematical Theory of Communication • Thomas M. Cover, Joy A. Thomas, Elements of Information theory • R. W. Yeung, A First Course in Information Theory • chapters of M. Nielsen, I. Chuang, Quantum Information and Computation, concerning IT B. Extracurricular readings <ul style="list-style-type: none"> • other chapters of M. Nielsen, I. Chuang, Quantum Information and Computation