Université de Montpellier, Autumn 2019.
The program of the course *Information theory.*

Section 1, weeks 1-5.

1.1 Measure of information in a finite set (Hartley's information).

1.2 Problems of optimal search: the "guess a number" game; search of a fake coin; sorting algorithm. Techniques of lower bounds: the counting argument and the adversarial argument.

1.3 Shannon's entropy for a distribution with a finite range: definition and basic properties.

1.4 The average number of questions in the "guess a number" game with a non-uniform distribution on possible answers. Shannon's bounds for the average length of a prefix code.

1.5 Uniquely decodable codes and lossless data compression. Kraft's inequality. Equivalence of prefix codes and uniquely decodable codes.

1.6 Expectation and variance of a random variable distributed on real numbers. The Bienaymé–Chebyshev inequality.

1.7 Stirling's formula for the factorial; approximation for binomial coefficients. Shannon's theorem on the block coding for a sequence of independent identically distributed random variables.

1.8 Classical coding techniques: the Shannon–Fano codes and Huffman's codes.

1.9 Shannon's entropy as a heuristic rule in search problems (by the example of the search of a fake coin).

1.10 Conditional entropy and of the mutual information, their basic properties. Universal inequalities for Shannon's entropy.

1.11 Symmetric encryption schemes and the optimal size of the secret key.

1.12 The problem of secret sharing. Threshold access structures and Shamir's scheme.

Section 3, weeks 11-13.

3.1 The simplest mathematical model of a communication channel with a random noise: discrete memoryless noisy channel. Shannon's definition of the capacity of a random noisy channel.

3.2 Shannon's coding theorem for a discrete memoryless noisy channel [excluded from the final exam].

3.3 Simple Kolmogorov complexity: the definition, existence of an optimal decompressor.

3.4 Basic properties of Kolmogorov complexity. Non-computability of the function of Kolmogorov complexity.

3.5 Kolmogorov complexity of a pair; proofs of the inequalities

$$C(x,y) \leq C(x) + C(y) + O(\log C(x))$$

and

$$C(x,y) \not\leq C(x) + C(y) + O(1).$$

3.6 Conditional Kolmogorov complexity: the main definition and existence of an optimal decompressor.

3.7 Basic properties of the conditional Kolmogorov complexity.

3.8 Algorithmic mutual information (mutual information for Kolmogorov complexity): the Kolmogorov–Levin theorem

$$C(x,y) = C(x) + C(y\,|\,x) + O(\log(C(x) + C(y)))$$

and symmetry of the mutual information.

3.9 An example of application of Kolmogorov complexity: duplicating a word on a one tape Turing machine requires quadratic time.

3.10 Deterministic and randomized communication protocols for two parties; a formal definition of deterministic communication complexity. Deterministic communication complexity of the predicate $\mathit{Equality}_n$ (for two n-bit strings) is $n+1$. Randomized communication protocol of logarithmic complexity for the predicate $\mathit{Equality}_n$ is $O(\log n)$.

References

[1] T.M. Cover, J.A. Thomas. Elements of information Theory. John Wiley & Sons.

[2] A. Shen, V. Uspensky, and N. Vereshchagin. Kolmogorov complexity and algorithmic randomness. AMS.

http://www.lirmm.fr/~ashen/kolmbook-eng.pdf

Supplementary literature:

[3] D. MacKay. Information Theory, Inference, and Learning Algorithms. Cambridge University Press.

https://www.inference.org.uk/itprnn/book.pdf

[4] M. Li and P. Vitányi. An introduction to Kolmogorov complexity and its applications. Springer.

[5] L. Fortnow, Kolmogorov complexity.

http://people.cs.uchicago.edu/~fortnow/papers/kaikoura.pdf

[6] E. Kushilevitz and N. Nisan. Communication Complexity. Cambridge University Press, NY, USA.

[7] A. Beimel. Secret-sharing schemes: a survey. International Conference on Coding and Cryptology 2011, pp. 11-46.

https://www.cs.bgu.ac.il/~beimel/Papers/Survey.pdf

[8] W. Feller An introduction to probability theory and its applications. Vol. 1. John Wiley & Sons.

[9] Y. Ollivier. Aspects de l'entropie en mathématiques. 2002.

http://www.yann-ollivier.org/entropie/entropie.php

[10] N. Sendrier. Introduction à la théorie de l'information. 2007.

https://www.rocq.inria.fr/secret/Nicolas.Sendrier/thinfo.pdf

[11] B. Durand, Alexandr Zvonkin, Complexité de Kolmogorov.

https://www.labri.fr/perso/zvonkin/Research/kolmogorov.pdf

[12] Н.К. Верещагин, Е.В. Щепин. Информация, кодирование и предсказание. МЦНМО, 2012.