Definitions of Conditional Rényi entropies: a review

Andreia Teixeira

CINTESIS - Center for Health Technology and Services Research

Abstract. The Rényi entropy [9], a generalization of Shannon entropy [10,2] has been used in several ways in Computer Science, Cryptography and Information Theory. There are however several proposals for an appropriate definition of conditional Rényi entropy (see for instance [1,3,4,5,6,7,8]) and there is no general agreement on the most appropriate definition. This is an important problem deserving some further study as the application of the conditional Rényi entropy can be found in many areas such as biomedical engineering [12], cryptography [1], fields related to statistics [11] and economics [13]. Recently, entropy measure has been used in healthcare to quantify the amount of information/complexity carried by a physiological signal such as heart rate (HR) and its deterministic dynamics. The Gaussianity of HR is a complementary measure of the physiological complexity of the underlying signal and conditional Rényi entropy can be used as Gaussianity measuring the extent to which the signal deviates from a stationary linear Gaussian [12]. In cryptography, the ability to guess the value of a random variable is an important measure of the variable's quality. This ability is captured by the Rényi entropy when $\alpha = \infty$, called min-entropy. Usually, the adversary has some additional information that is correlated with the secret and this clearly shows that conditional Rényi entropy should be well defined. For $\alpha = 2$, it is called the collision entropy, a measure relevant for various hashing schema and cryptographic protocols. Given the raising number of applications of conditional Rényi entropy it is important to study all the existing proposals and its properties in order to reach an agreement on the best definition. Otherwise we risk that by not using the same measure different researchers reach contradictory conclusions. We list, study and compare three definitions of conditional Rényi entropy considering in particular the case of min-entropy.

References

1. C. Cachin, *Entropy Measures and Unconditional Security in Cryptography*, PhD thesis, Swiss Federal Institute of Technology Zürich, 1997.
2. T. Cover and J. A. Thomas, *Elements of Information Theory*, Second Edition, Wiley Series in Telecommucations.
3. I. Csiszár, *Generalized cuttof rates and Rényi information measures*, IEEE Transactions on Information Theory, **41**, pp 26-34, 1995.

4. L. Golshani, E. Pasha, and G. Yari, *Some properties of Rényi entropy and Rényi entropy rate*, Information Sciences, 2009, pp 2426 2433.
5. P. Jizba and T. Arimitsu, *The world according to Rényi: thermodynamics of multifractal systems*, Annals of Physics **312**, pp 17-59, 2004.
6. P. Jizba and T. Arimitsu, *Generalized statistics: yet another generalization*, Physica A, **340**, pp 110-116, 2004.
7. C. Hsiao, C. Lu and L. Reyzin, *Conditional Computational Entropy, or Toward Separating Pseudoentropy from Compressibility*, EUROCRYPT 2007, pp 169-186.
8. R. Renner and S. Wolf, *Smooth Rényi entropy and applications*, Proceedings of the IEEE International Symposium on Information Theory, pp 233, June 2004.
9. A. Rényi, *On measures of entropy and information*, Mathematical Institute, Hungarian Academy of Sciences, 1961.
10. C. E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal, **27**, pp 379–423 and 623–656, 1948.
11. F. Kanaya and T.S. Han, *The asymptotics of posterior entropy and error probability for Bayesian estimation*, IEEE Transactions on Information Theory, **41**, pp. 1988–1992, 1995.
12. D.E. Lake, *Rényi entropy measures of heart rate gaussianity*, IEEE Transactions on Biomedical Engineering, **53**, pp. 21–27, 2006.
13. S.R. Bentes and R. Menezes and D.A. Mendes *Long memory and volatility clustering: is the empirical evidence consistent across stock markets?*, Physica A, **387**, pp. 3826–3830, 2008.