Kolmogorov One-way Functions

Filipe Casal

Dep. Matemática, Instituto Superior Técnico, U Lisboa, Portugal and
Centro de Matemática, Aplicações Fundamentais e
Investigação Operacional (CMAF-CIO), U Lisboa, Portugal

One-way functions are polynomially computable functions that are hard to invert, meaning that given an image it should not exist an efficient algorithm to compute its pre-image. One-way functions are not know to exist. However their existence has major consequences in mathematics, as well as in everyones daily lives: on one hand their existence implies that $\mathsf{P} \neq \mathsf{NP}$ (see [3]); on the other hand, if they do not exist, then most cryptographic protocols and pseudo-random generators are not secure since their security is based on the hardness of several one-way function candidates.

In Algorithmic Information Theory the central notion is Kolmogorov complexity, $\mathsf{K}(x)$, proposed in [4], [6] and [2], that measures the information contained in a string x by means of the length of its shortest description. The computational hardness is easily encoded in this information measure by considering its time-bounded version, $\mathsf{K}^t(x)$, where the restriction is that the program describing it must run within time $t(|x|)$.

Here, we are interested in the connection between Kolmogorov complexity and the study of one-way functions, a line of work first considered in [7] and [1]. In these works, the authors provided a characterization of strong and weak one-way functions based on the expected value of $\mathsf{K}_f^{t \log t}(x|f(x), r, n)$. Furthermore, based on the difference between $\mathsf{K}_f^t(x|n)$ and $\mathsf{K}_f^t(x|f(x), n)$ they propose an individual approach characterization to one-way functions. We show that the expected value approach cannot be used to fully characterize the class of strong one-way functions. Moreover, we provide a sufficient condition under which Kolmogorov one-way functions (as defined in [1]) are weak one-way functions.

Pursuing the idea of having a full classification of classes of one-way functions using Kolmogorov based measures, we give alternative characterizations of one-way functions based on time-bounded Kolmogorov complexity. We define several classes of functions, namely Kolmogorov strong and weak one-way functions and show that these are equivalent to the usual notions of strong and weak one-way functions.

Joint work with João Rasga, Dep. Matemática, Instituto Superior Técnico, U Lisboa, Portugal and CMAF-CIO, U Lisboa, Portugal and André Souto at Dep. Matemática, Instituto Superior Técnico, U Lisboa, Portugal and SQIG at Instituto de Telecomunicações.

References

1. F. Casal, J. Rasga and A. Souto. Kolmogorov One-way Functions Revisited *Submitted for publication.*
2. L. Antunes, A. Matos, A. Pinto, A. Souto, and A. Teixeira. One-way functions using algorithmic and classical information theories. *Theory of Computing Systems*, 52(1):162–178, 2013.
3. G. Chaitin. On the length of programs for computing finite binary sequences. *Journal of ACM*, 13(4):547–569, 1966.
4. O. Goldreich. *Foundations of Cryptography.* Cambridge University Press, 2001.
5. A. Kolmogorov. Three approaches to the quantitative definition of information. *Problems of information transmission*, 1(1):1–7, 1965.
6. J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of Symp. on Theory of Computing '90*, pages 387–394. ACM, 1990.
7. R. Solomonoff. A formal theory of inductive inference, part I. *Information and Control*, 7(1):1–22, 1964.
8. A. Souto, A. Pinto and A. Teixeira, A. One-way functions using Kolmogorov complexity. In *Proceedings of CiE 2010*, Açores, Portugal, 2010.