An overview of asynchronous delay iterations: mathematical analysis and algorithms

Christophe Guyeux

12th CHAOS 2019 International Conference

Abstract

Asynchronous delay iterations from discrete mathematics have long been used to accelerate convergence in high-performance computing. They have the particularity of being defined on an infinite (discrete) set that can be seen as a Cartesian product: at each iteration, a vector of fixed-size bits is updated from a function whose return also depends on a parameter, itself obtained from the first term of a sequence that is iterated at each iteration. The resulting product space is infinite but only handles bounded integers. In addition, only the bit vector must be stored in the finite state machine, a new term of the infinite sequence can be read at each iteration. In doing so, we obtain a discrete dynamic system that can be implemented as is on our computers, but which, from the moment they receive new data at each clock stroke, iterates over an infinite set.

Any algorithm performing the function mentioned above, and iterating in such a way as to update the machine's memory (the bit vector) from a new input provided to it, is therefore ultimately a discrete dynamic system iterating over an infinite discrete set, and whose chaos can be studied and measured. Such an approach has proved to be rich in perspectives. Indeed, provided that the above framework is respected, it is possible to design algorithms whose realization on the machine corresponds exactly to the discrete dynamic system studied mathematically: the Cartesian product mentioned above corresponds to all the bit vectors that can be stored in the memory coupled to all the bit sequences that can be provided at the input of the machine, which is indeed an infinite set.

This exact framework therefore makes it possible to define and design concretely, and without any shenanigans, programs that have been mathematically proven to be chaotic, and fine-state systems such as Turing's machines that have been proven to be just as precisely chaotic. This framework has been used over the past decade to design algorithms in computer security and hazard generation, for the Internet of Things, and more recently to design new artificial intelligence algorithms. The purpose of this arti! cle is to review the various theoretical advances in these asynchronous iterations, and in such concepts as the characterization of Devaney's chaos, topological or metric

entropy, Lyapunov's exponent and ergodicity, and the concrete algorithmic applications that have been published over the past ten years.

References:

1. H. Noura, C. Guyeux, A. Chehab, M. Mansour, and R. Couturier. An Efficient, Flexible, and Practicable Cipher Scheme with Study of OFB dynamics. International Journal of Bifurcation and Chaos. *, ***_***. 2018.

2. M. Bakiri, C. Guyeux, J.-F. Couchot, L. Marangio, and S. Galatolo. A Hardware and Secure Pseudorandom Generator for Constrained Devices. IEEE Transactions on Industrial Informatics. Special Issue on Applied Cryptography, Security, and Trust Computing for Industrial Internet-of-Things. 14(8), 3754-3765. 2018.

3. M. Bakiri, C. Guyeux, J.-F. Couchot, and A. Oudjida. Survey on Hardware Implementation of Random Number Generators. Computer Science Review, Elsevier. 27, 135-153. 2018.

4. M. Bakiri, J.-F. Couchot, and C. Guyeux. CIPRNG: A VLSI Family of Chaotic Iterations Post-Processings for F2-Linear Pseudorandom Number Generation Based on Zynq MPSoC. IEEE Transactions on Circuits and Systems I: Regular Papers. 65(5), 1628-1641. 2018.

5. Z. Lin, C. Guyeux, S. Yu, Q. Wang, and S. Cai. On the use of chaotic iterations to design keyed hash function. Cluster computing. *, ***_***. 2017.