Contribution ID: **35**

Type: **Oral**

Randomness Characterization through Bayesian Model Selection

Tuesday 22 October 2019 18:20 (20 minutes)

Random number generation currently plays a fundamental role due to its several applications in probabilistic algorithms (*e.g.* Monte Carlo methods, stochastic gradient descent, etc.), but mainly for its importance in cryptography. The most common methods for characterizing random numbers generators (RNG) either lack formality (*e.g.* the battery of tests provided by the NIST) or are not generally applicable, even in principle (*e.g.* the characterization developed by the Algorithmic Information Theory). In this work we present a method based on Model Selection using Bayesian Inference which turns out to be both rigorous and effective in assessing the randomness of bits sequences. We are able to obtain analytic expressions for a model's likelihood and our results shows that this new method is more stringent than both the NIST's set of tests and the Borel's Normality criterion. Additionally, given that Bayesian Inference entails the generalizability feature for the selected model, our scheme transcends single sequence analysis and provides a characterization of the *source* acting as a RNG. (More details and and experimental case are presented in Ref. [1].)

Authors: DIAZ HERNANDEZ ROJAS, Rafael (Sapienza University of Rome); SOLÍS, Aldo (UNAM); ANGULO MARTÍNEZ, Alí (UNAM); U'REN, Alfred (UNAM); HIRSH, Jorge (UNAM); MARSILI, Matteo (International Center of Theoretical Physics); PÉREZ CASTILLO, Isaac (UNAM)

Presenter: DIAZ HERNANDEZ ROJAS, Rafael (Sapienza University of Rome)

Session Classification: Submitted contributions

Track Classification: Artificial intelligence, data science, and machine learning