Automatic Sequences Along Polynomial Subsequences and Their Applications

Ísabel Pirsic and Domingo Gómez-Pérez
Universidad de Cantabria, Spain

30th Applications of Computer Algebra - ACA 2025

Pseudorandom sequences are crucial in various fields, particularly in cryptography. These sequences, which must exhibit high entropy and efficient implementation, are essential for generating nonces, session keys, and parameters in cryptographic systems, among other uses. Due to their deterministic nature, pseudorandom sequences can be analyzed to identify regularities and understand potential weaknesses in the form of patterns.

Automatic sequences are families of sequences generated by formal automata. This category includes, but is not limited to, Thue-Morse, Rudin-Shapiro and paper folding sequences. In this talk, we introduce a new general family, the CAP sequences, which encompasses many previously studied sequences. We then explore the problem of studying polynomial subsequences of these sequences, specifically when they become constant. Additionally, we consider the converse problem: given a polynomial, determine a nontrivial CAP sequence which becomes constant on that polynomial.

Thus we exhibit the necessity to understand well the automatic sequence family to which the polynomial subsequence paradigm is applied for cryptographic purposes.

We conclude the presentation with a software implementation and some open problems.