The Expansion Complexity of Ultimately Periodic Sequences over Finite Fields

Yi Zhang
Xi'an Jiaotong-Liverpool University, China

30th Applications of Computer Algebra - ACA 2025

The expansion complexity is a new figure of merit for cryptographic sequences. In this paper, we present an explicit formula of the (irreducible) expansion complexity of ultimately periodic sequences over finite fields. We also provide improved upper and lower bounds on the N-th irreducible expansion complexity when they are not explicitly determined. In addition, for some infinite sequences with given nonlinear complexity, a tighter upper bound of their N-th expansion complexity is given. This a joint work with Zhimin Sun, Xiangyong Zeng, Chunlei Li, and Lin Yi.