

CONSTRUCTION OF SEQUENCES WITH HIGH NONLINEAR COMPLEXITY FROM HERMITIAN FUNCTION FIELDS

GUILHERME CHAUD TIZZIOTTI

JOINT WORK WITH ALONSO S. CASTELLANOS AND LUCIANE QUOOS

ABSTRACT. The theory of algebraic functions of one variable over the finite field \mathbb{F}_q of cardinality q has several applications in distinct areas of mathematics such as coding theory, permutation polynomials and sequences. Sequences over finite fields from the complexity-theoretic standpoint can also be applied on cryptography and pseudorandom generation, one of the requirements of such sequences is that it should be very hard to replicate the entire sequence from the knowledge of a part of it, that is, its complexity should be large. Many different complexity measures are available in the literature, the most usual being the *linear complexity*. In recent years paper researchers have constructed sequences with large *nonlinear complexity* measure.

We provide a sequence with high nonlinear complexity from the Hermitian function field \mathcal{H} . This sequence was obtained using a function with pole divisor in ℓ collinear rational places P_1, \dots, P_ℓ on \mathcal{H} .