CURVAS ALGÉBRICAS E TEMAS AFINS

Construction of sequences with high nonlinear complexity from Hermitian function fields

Guilherme Chaud Tizziotti
Universidade Federal de Uberlândia
01/11/2019 - Sexta-Feira
15h00 - Sala 121

Resumo: The theory of algebraic functions of one variable over the finite fieldFq 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 H. This sequence was obtained using a function with pole divisor in ` collinear rational places P1,...,P` on H.