Two Applications of Number Theory to Information Theory

Giacomo Micheli

The University of South Florida
and
The Center for Cryptographic Research at USF

Abstract. In the first part of the talk, we will see how to capture information of polynomial maps over finite fields using group theory. With the developed framework, we will mention how to construct interesting information theoretical structures, such as codes for distributed storage systems. In the second part of the talk we will use the theory of multiplicative character sums to construct binary linear codes having relative distance asymptotic to $1/2$, and large dimension.