On Lattice Constructions from Codes over Finite Fields

Franciele do Carmo Silva

francielecs@ime.unicamp.br

Abstract

Lattices are discrete additive subgroups of the n-dimensional Euclidean space which are also described as all integer linear combinations of a set of linearly independent vectors. Some efficient lattice constructions in coding for reliable transmissions, such as Construction A, D and D', are based on linear codes over integer residue rings. Recently, it has been proposed generalizations of Construction A and D of complex lattices over number fields and also over principal ideal domains due to perspective applications to compute-and-forward schemes and block fading wiretap coding. In this presentation, we extend this approach to Construction D' from a family of nested linear codes over finite fields. This construction enables a natural use of low-density parity-check codes (LDPC), known for efficient decoding performance.

This is a work in progress supervised by Prof. Sueli Costa aiming the study of properties and possible applications of these lattice constructions to coding for different channels and in cryptography.