NP-Hardness of Reed-Solomon Decoding and the Prouhet-Tarry-Escott Problem

Elena Grigorescu, Purdue University

Establishing the complexity of Bounded Distance Decoding in Reed-Solomon is a fundamental open problem in coding theory, and its study is motivated by the current large gap between the regime when it is NP-hard, and the regime when it is efficiently solvable (i.e., the Johnson radius).

We show the first NP-hardness results for asymptotically smaller decoding radii than the maximum likelihood decoding radius of Guruswami and Vardy. Our results follow from the NP-hardness of a generalization of the classical Subset Sum problem to higher moments, which has been a known open problem, and which may be of independent interest. We further reveal a strong connection with the well-studied Prouhet-Tarry-Escott problem in Number Theory, which turns out to capture a main barrier in extending our techniques to smaller radii.

This is a joint work with Venkata Gandikota (Purdue) and Badih Ghazi (MIT).