Shachar Lovett UC San Diego

Structure and Pseudo-Randomness in Coding Theory

Abstract:

The theory of structure and pseudo-randomness has been very influential in several areas of mathematics, such as number theory, graph theory and harmonic analysis. It is also been influential in theoretical computer science, with applications in complexity theory, cryptography and property testing. At a high level, it allows to analyze arbitrary objects by decomposing them to a "structural" component and a "pseudo-random" component. The pseudo-random component behaves in many ways like random noise, while the structural component has a concise representation which makes it amenable to analysis and algorithmic manipulation.

In this talk, I will describe applications of this paradigm to coding theory. I will describe a new general approach to list decoding, which follows by decomposing an arbitrary received word to a structural received word and pseudo-random noise. This allows for a simplified analysis of the list decoding problem. In particular, I will describe how this approach leads to a resolution of a conjecture by Gopalan, Klivans and Zuckerman [STOC 2008], that the list decoding radius of Reed-Muller codes (in certain regimes) is equal to the minimal distance of the code.

Based on joint work with Abhishek Bhowmick.