Abstract

Consider the following setting. Suppose we are given as input a "corrupted" truth-table of a polynomial $f(x_1,..,x_m)$ of degree $r = o(\sqrt{m})$, with a random set of $1/2 - o(1)$ fraction of the evaluations flipped. Can the polynomial $f$ be recovered? Turns out we can, and we can do it efficiently!

The above question is a demonstration of the reliability of Reed-Muller codes under the random error model. For Reed-Muller codes over $\mathbb{F}_2$, the message is thought of as an $m$-variate polynomial of degree $r$, and its encoding is just the evaluation over all of $\mathbb{F}_2^m$.

In this talk, we shall study the resilience of RM codes in the *random error* model. We shall see that under random errors, RM codes can efficiently decode many more errors than its minimum distance. (For example, in the above toy example, minimum distance is about $1/2^{\sqrt{m}}$ but we can correct close to $1/2$-fraction of random errors). This builds on a recent work of [Abbe-Shpilka-Wigderson-2015] who established strong connections between decoding erasures and decoding errors. The main result in this talk would be constructive versions of those connections that yield efficient decoding algorithms.

This is joint work with Amir Shpilka and Ben Lee Volk.