Regularities Lemmas for Polynomials and Applications

Pooya Hatami
IAS

10/28/2015 at 11:00 am
Core A (Room 301)

Abstract

In analogy with the regularity lemma of Szemeredi, regularity lemmas for polynomials over finite fields shown by Green and Tao (Contrib. Discrete Math. 2009) and by Kaufman and Lovett (FOCS 2008) allow one to “refine” a given collection of polynomials to a new collection of polynomials that are “pseudorandom”.

We discuss algorithmic versions of these regularity lemmas and give two applications. We show that Reed-Muller codes can be globally decoded at any error rate (even beyond list-decoding radius) if we assume that the noise is “structured”. As another application, we give an efficient algorithm for finding prescribed decompositions of low-degree polynomials.

Lastly, we discuss structure theorems for low-degree polynomials. Let \( \mathbb{F}=\mathbb{F}_p \) be a prime field. Haramaty and Shpilka [STOC 2010] proved that a biased cubic or quartic polynomial \( f \in \mathbb{F}[x_1,\ldots,x_n] \) can be written in the form \( f = g_1 h_1 + \ldots + g_t h_t \) (as a function), where \( t \) depends only on the bias of \( f \), and \( g_i, h_i \) are degree < \( \deg(f) \) polynomials satisfying \( \deg(g_i)+\deg(h_i) \leq \deg(f) \). Using regularity lemmas for polynomials, we prove that such a strong structure theorem holds for degree five polynomials as well. This structure theorem implies that every biased degree five polynomial is constant on an \( \Omega(n) \) dimensional subspace of \( \mathbb{F}^n \).

Organizer(s): Eric Allender, Michael Saks and Mario Szegedy