On Polynomial Approximations Over Z/2kZ

Abhishek Bhrushundi
Dept. of Computer Science

2/28/2017 at 03:15 pm
CoRE A (301)

Abstract

We study approximation of Boolean functions by low-degree polynomials over the ring Z/2kZ. More precisely, given a Boolean function F : {0,1}n {0,1}, define its k-lift to be F : {0,1}n {0,2k-1} by Fk(x) = 2k-F(x) mod 2k$. We consider the fractional agreement (which we refer to as d,k(F)) of Fk(x) with degree d polynomials from Z/2kZ[x1,...,xn].

Our results are the following: 1. Increasing k can help: We observe that as k increases, d,k(F) cannot decrease. We give two kinds of examples where d,k(F) actually increases. The first is an infinite family of functions F such that 2d,2(F) 3d-1,1(F) (1). The second is an infinite family of functions F such that d,1(F) 1/2 + o(1) – as small as possible – but d,3(F) 1/2 +(1). 2. Increasing k doesn't always help: Adapting a proof of Green[Comput. Complexity, 9(1):16-38, 2000], we show that irrespective of the value of k, the Majority function Majn satisfies d,k(Majn) 1/2 + O(d/n). In other words, polynomials over Z/2kZ for large k do not approximate the majority function any better than polynomials over Z/2Z.

We observe that the model we study subsumes the model of non-classical polynomials in the sense that proving bounds in our model implies bounds on the agreement of non-classical polynomials with Boolean functions. In particular, our results answer questions raised by Bhowmick and Lovett [In Proc. 30th Computational Complexity Conf., pages 72-87, 2015] that ask whether non-classical polynomials approximate Boolean functions whether non-classical polynomials approximate Boolean functions better than

Examination Committee: Prof. Swastik Kopparty (Advisor), Prof. Eric Allender (Advisor)Prof. Mario Szegedy, Prof. Gerard de Melo