abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In this work we study the correlation between low-degree GF(2) polynomials and explicit functions, where the correlation between two functions f,p : {0,1}^n -> {+1,-1} is defined as Correlation(p,f) := | E_x [f(x) p(x)] | = | P_x[f(x) = p(x)] - P_x[f(x) != p(x)] |. The study of correlation bounds is motivated, in large part, by their applications to proving lower bounds on the size of important classes of circuits with parity and majority gates. For example, exhibiting an explicit function which has negligible correlation with every GF(2) polynomial of polylogarithmic degree would solve the famous open problem of establishing a superpolynomial lower bound on the size of constant-depth circuits with parity gates and one majority gate (using a result by Razborov; Mat. Zametki, '87). An additional motivation for studying correlation bounds is that functions with negligible correlation with low-degree GF(2) polynomials can be used to construct pseudorandom generators that fool GF(2) polynomials, and more generally constant-depth circuits with few parity gates (using the pseudorandom generator construction by Nisan and Wigderson; JCSS, '88). Finally, our ability to prove correlation bounds is a fundamental benchmark for our understanding of complexity theory: Currently no explicit function on n bits is known to have negligible correlation with GF(2) polynomials of degree log_2 n. In this work we obtain the following results: (I) We present a new proof that the Mod(3) function, i.e. the function that equals 1 iff the sum of the input bits is divisible by 3, has correlation exp(-n/4^d) with any GF(2) polynomial of degree d. Such a result was recently obtained in a breakthrough work by Bourgain (C. R. Acad. Sci. Paris, 2005). Our proof appears to be more modular and achieves a slightly better bound. (II) We exhibit a polynomial-time computable function on n bits that has correlation at most exp(-n/2^d) with any GF(2) polynomial of degree d. Previous to our work the best correlation bound for an explicit function was exp(-n/(d 2^d)), which follows from a result by Babai, Nisan, and Szegedy (JCSS, '92). (III) We derive an `XOR Lemma' for low-degree GF(2) polynomials. We

abstract

show that if a function f on n bits has correlation at most .5 with any degree-d GF(2) polynomial then the product of m copies of f on disjoint inputs (i.e., f(x_1) f(x_2) ... f(x_m)) has correlation at most exp(-m/4^d) with any degree-d GF(2) polynomial. Previous to our work such a result was not known for any degree d > 1. Our results rely on a measure of the `complexity' of a function due to Gowers (Geom. Funct. Anal., 1998 & 2001). Our work seems to be the first use of this measure to prove correlation bounds. A write-up of these results is available at http://eccc.hpi-web.de/eccc-reports/2006/TR06-097/index.html. These results are part of a larger work (in preparation) which is joint with Avi Wigderson.