abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We consider the problem of bounding the absolute value of the correlation between parity and low-degree polynomials modulo q, for odd q >= 3. The boolean function corresponding to the polynomial is 0 on an input iff the polynomial evaluates to 0 modulo q on this input.

Exponentially small upper bounds on the correlation implies exponential lower bounds on the size necessary to compute parity by depth-3 circuits with a "majority" gate at the top, "divisibility by q" gates at the middle level and AND gates of small fan-in at the input level. Proving exponential lower bounds for such circuits which have poly-log fan-in ANDs against a function from ACC0 is an interesting and important question in complexity theory. We show exponentially small upper bounds on the correlation for polynomials which satisfy certain linear algebraic properties. Although our techniques come short of bounding the correlation for all low-degree polynomials, the class of polynomials for which we obtain exponentially small upper bounds include polynomials of large degree and with a large number of terms that previous techniques did not apply to. Our technique is based on a general representation of the correlation using exponential sums that allows us to take advantage of a linear algebraic structure derived from the polynomial.

Our work includes the result of Goldmann on the correlation between parity and degree one polynomials. Using ideas from the proof of Cai, Green, and Thierauf, and a result of Voloch on the representation of the elementary symmetric polynomials by power-sum polynomials in prime fields, we extend the result of Cai, Green, and Thierauf to functions of a small number of certain generalized symmetric polynomials.

This is a joint work with Prof. Anna Gal.