abstract

COMPUTER SCIENCE AND DISCRETE MATHEMATICS SEMINAR II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We study the complexity of computing some basic arithmetic operations over GF(2^n), namely computing q-th root and q-th residuosity, by constant depth arithmetic circuits over GF(2) (also known as AC^0(parity)). Our main result is that these operations require exponential size circuits.

We also derive strong average-case versions of these results. For example, we show that no subexponential-size, constant-depth, arithmetic circuit over GF(2) can correctly compute the cubic residue symbol for more than 1/3 + o(1) fraction of the elements of GF(2^n).

As a corollary, we deduce a character sum bound showing that the cubic residue character over GF(2^n) is uncorrelated with all degree-d n-variate GF(2) polynomials (viewed as functions over GF(2^n) in a natural way), provided d << n^{0.1}. Classical approaches based on van der Corput differencing and the Weil bounds show this only for d << log(n). Curiously, the proof of this character sum bound is almost entirely based on complexity-theoretic considerations.