

abstract

MINI-WORKSHOP ON PSEUDORANDOMNESS

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

This talk will focus on the complexity of the cubic-residue (and higher-residue) characters over $GF(2^n)$, in the context of both arithmetic circuits and polynomials.

We show that no subexponential-size, constant-depth arithmetic circuit over $GF(2)$ can correctly compute the cubic-residue character for more than $1/3 + o(1)$ fraction of the elements of $GF(2^n)$. The key ingredient in the proof is an adaptation of the Razborov-Smolensky method for circuit lower bounds to setting of univariate polynomials over $GF(2^n)$.

As a corollary, we show 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 $d \ll n^{0.1}$. Classical approaches based on van der Corput differencing and the Weil bounds show this for $d \ll \log(n)$.