The Complexity of Powering in Finite Fields

Date Tuesday, January 31

Time 3:30 pm

Location 317 Mudd

Abstract: I will talk about the complexity of the cubic-residue (and higher-residue) characters over $GF(2^n)$, in the context of both arithmetic formulas and polynomials.

We show that no subexponential-size, constant-depth arithmetic formula over $GF(2)$ can correctly compute the cubic-residue character for more than $\frac{1}{3}+o(1)$ 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 $d << n^{0.1}$. Classical approaches show this kind of result for $d << log(n)$.