

Linear systems over composite moduli

Arkadev Chattopadhyay
University of Toronto
arkadev@cs.toronto.edu

Avi Wigderson
IAS, Princeton
avi@ias.edu

Abstract

We study solution sets to systems of *generalized* linear equations of the form

$$\ell_i(x_1, x_2, \dots, x_n) \in A_i \pmod{m}$$

where ℓ_1, \dots, ℓ_t are linear forms in n Boolean variables, each A_i is an arbitrary subset of \mathbb{Z}_m , and m is a *composite* integer that is a product of two distinct primes, like 6. Our main technical result is that such solution sets have exponentially small correlation, i.e. $\exp(-\Omega(n))$, with the boolean function MOD_q , when m and q are relatively prime. This bound is independent of the number t of equations.

This yields progress on limiting the power of constant-depth circuits with modular gates. We derive the first exponential lower bound on the size of depth-three circuits of type $\text{MAJ} \circ \text{AND} \circ \text{MOD}_m^A$ (i.e. having a MAJORITY gate at the top, AND/OR gates at the middle layer and *generalized* MOD_m gates at the base) computing the function MOD_q . This settles an open problem of Beigel and Maciél (Complexity'97), for the case of such modulus m .

Our technique makes use of the work of Bourgain (2005) on estimating exponential sums involving a *low-degree polynomial* and ideas involving matrix rigidity from the work of Grigoriev and Razborov (FOCS'98) on *arithmetic circuits* over finite fields.