Solvability of polynomial equations over finite fields.

Neeraj Kayal

Abstract

We investigate the complexity of the following polynomial solvability problem - given a finite field $F_q$ and a set of polynomials $f_1, f_2, \ldots, f_m \in F_q[x_1, x_2, \ldots, x_n]$ of total degree at most $d$, determine the existence of an $F_q$-solution to the system of equations

$$f_1(x) = f_2(x) = \ldots = f_m(x) = 0.$$ 

That is determine if there exists a point $a \in F_q^n$ such that

$$f_1(a) = f_2(a) = \ldots = f_m(a) = 0.$$ 

The problem is easily seen to be NP-complete even when the field size is 2 and the degree $d$ of each polynomial is also bounded by 2. Here we investigate the deterministic complexity of this problem when the number $n$ of variables in the input is bounded. We show that for any fixed $n$, there is a deterministic algorithm for this problem whose running time is bounded by a polynomial in $(d \cdot m \cdot \log q)$. Moreover the algorithm can be implemented parallely to get a family of P-uniform circuits of size $\text{poly}(d \cdot m \cdot \log q)$ and depth $\text{poly}(\log d \cdot \log m \cdot \log q)$ for this problem.