Abstract

We consider the problem of solving *systems of multivariate polynomial equations of degree k* over a finite field. For every integer $k \geq 2$ and finite field $\mathbb{F}_q$ where $q = p^d$ for a prime p, we give, to the best of our knowledge, the first algorithms that achieve an exponential speedup over the brute force $O(q^n)$ time algorithm in the worst case. We present two algorithms, a randomized algorithm with running time $q^{n+o(n)} \cdot q^{-n/O(k)}$ time if $q \leq 2^{4ekd}$, and $q^{n+o(n)} \cdot (\frac{\log q}{dek})^{-dn}$ otherwise, where $e = 2.718\ldots$ is Napier's constant, and a deterministic algorithm for *counting* solutions with running time $q^{n+o(n)} \cdot q^{-n/O(kq^{6/7d})}$. For the important special case of quadratic equations in $\mathbb{F}_2$, our randomized algorithm has running time $O(2^{0.8765n})$. For systems over $GF(2)$ we also consider the case where the input polynomials do not have bounded degree, but instead can be efficiently represented as a $\Sigma\Pi\Sigma$ circuit, i.e., a sum of products of sums of variables. For this case we present a deterministic algorithm running in time $2^{n-\delta n}$ for $\delta = 1/O(\log(s/n))$ for instances with s product gates in total and n variables. Our algorithms adapt several techniques recently developed via the polynomial method from circuit complexity. The algorithm for systems of $\Sigma\Pi\Sigma$ polynomials also introduces a new *degree reduction* method that takes an instance of the problem and outputs a subexponential-sized set of instances, in such a way that feasibility is preserved and every polynomial among the output instances has degree $O(\log(s/n))$.