COROLLARY 2. If \( f \in \mathbb{R}[x_1, \ldots, x_n] \) and \( f(x) > 0 \) for any \( x \in \mathbb{R}^n \), then \( f(x') > 1/\gamma \).

Proof. The function \( f \) achieves local minima and, in particular, a global minimum at its critical points. If \( K \subset \mathbb{R}^n \) is the set of critical points of \( f \), then the set \( V = (K^c : \partial f/\partial x_i = \ldots = \partial f/\partial x_n = 0, f = x_{n+1}) \) is an algebraic variety, defined by the system \( \partial f/\partial x_i = \ldots = \partial f/\partial x_n = 0, f = \min_{x \in K^c} f(x) \) is an algebraic subvariety of the variety \( V \), and by Corollary 1, contains a point \( x' = (x'_1, \ldots, x'_{n+1}) \) such that \( |x'_{n+1}| > 1/\gamma \).

LITERATURE CITED


FACTORIZATION OF POLYNOMIALS OVER A FINITE FIELD
AND THE SOLUTION OF SYSTEMS OF ALGEBRAIC EQUATIONS

D. Yu. Grigor'ev

An algorithm is constructed for factoring polynomials in several variables over a finite field \( F_q \), which works in polynomial time in the size of the polynomial and \( q \). Previously this result was known in the case of one variable. An algorithm is given for the solution (over the algebraic closure \( \overline{F} \) of the field \( F \)) of systems of algebraic equations \( \hat{f}_1 = \ldots = \hat{f}_n = 0 \), where \( \hat{f}_1, \ldots, \hat{f}_n \in F[x_1, \ldots, x_n] \) with working time of order \( L^{n^k(n+l)}(q+1) \), where \( L \) is the size of a representative of the original system, \( l \) is the degree of transcendence of the field \( F \) over the prime subfield, \( q = \text{char}(F) \). Previously the estimate \( L^{n^k(q+1)} \) was known for \( l = 0 \).

INTRODUCTION

In the present paper we give algorithms for solving two problems of computational commutative algebra, the estimate of whose complexity is better in order of growth than those known previously. In Chapter I an algorithm is described for factoring polynomials in several variables into irreducible factors over a finite field, which works in polynomial time.

In Chapter II an algorithm is constructed for solving systems of algebraic equations of arbitrary degree, working in subexponential time.

The problem of constructing an algorithm for factoring polynomials into factors goes back all the way to Gauss. Up to now it has attracted the attention of many mathematicians. The Kronecker algorithm is widely known [1]. Unfortunately, Kronecker's algorithm, as well as all other algorithms known until most recently, required exponential time (in the length of the description of the original polynomial) in general. The first step was made by D. K. Faddeev and independently A. I. Skopin at the end of the fifties for factoring polynomials in one variable over a finite field $\mathbb{F} = \mathbb{F}_q$; in the literature this algorithm is known as Berlekamp's algorithm [5], which he published in the sixties. After this, in the course of nearly 20 years there was no essential progress. Only in 1982, Lenstra et al. [20] constructed a polynomial algorithm for factoring polynomials in one variable over the field of rational numbers $\mathbb{F} = \mathbb{Q}$. This reduced the factoring to the search for a vector of sufficiently small norm in a given lattice over the ring of integers $\mathbb{Z}$, with subsequent application of Berlekamp's algorithm and Hensel's lemma. Independently, in [15], the reduction of the factoring of polynomials in several variables over $\mathbb{F} = \mathbb{Q}$ to the factoring of polynomials in two variables was obtained, which was polynomial for a fixed number of variables, and, in addition, in [16] a polynomial reduction of the factoring of polynomials in two variables over $\mathbb{F} = \mathbb{Q}$ to the factoring of polynomials in one variable was found. Finally, an algorithm of polynomial complexity for factoring polynomials in several variables over a finite field was first given by the author in [8], and an account of it constitutes Chapter I of the present paper (cf. Theorem 1.4 of Sec. 3). Afterwards, Chistov constructed an algorithm of polynomial complexity for factoring polynomials in several variables over global fields [8] and extended this result to fields which are finitely generated over their prime subfields [4].

In Chapter I we consider a polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. Here we assume that $\deg_{x_i}(f) < r, 1 \leq i \leq n$. Then $f$ can be represented by the vector of length $r^n$ of its coefficients from the finite field $\mathbb{F}_q$. The bit length of the description of elements of the field $\mathbb{F}_q$ does not exceed $\log_2 q$. Hence, by the size of the polynomial $f$ in Chapter I we mean the quantity $r^nx \log_2 q$. In Chapter I an algorithm is described for factoring $f$ into factors which are irreducible over $\mathbb{F}_q$ in polynomial time in the size of $f$.

Section 1 of Chapter I is preparatory for Sec. 2, although it has independent interest. A polynomial algorithm is given for finding a minimal vector in a lattice over the ring $\mathbb{F}_q[x][t]$.

In Sec. 2 a polynomial algorithm is constructed for factoring polynomials from $\mathbb{F}_q[x_1, x_2]$.

In Sec. 3 the proof of the basic result of Chapter I is completed with the help of reduction to the case of two variables ($n = 2$).

The problem of solving systems of algebraic equations also has a long history. The fundamental possibility of solving systems over an algebraically closed field was already estab-