Докл. Акад. Наук СССР
Том 275 (1984), № 6

Soviet Math. Dokl.
Vol. 29 (1984), No. 2

FAST DECOMPOSITION OF POLYNOMIALS INTO IRREDUCIBLE ONES AND THE SOLUTION OF SYSTEMS OF ALGEBRAIC EQUATIONS

UDC 518.5+513.46

D. YU. GRIGOR'EV AND A. L. CHISTOV

In this note results are presented which show that polynomials in several variables can be decomposed in polynomial time into irreducible factors over a field finitely generated over a primitive field, and, moreover, that an algebraic variety can be decomposed in subexponential (in fact approximately polynomial) time into irreducible components. All previously known algorithms have had exponential bounds on the operating time for solving these problems.

1. Let $f \in F[X_1, \dots, X_n]$ be a polynomial with coefficients in the field

$$F = H(T_1, \dots, T_l)[\eta],$$

where either $H = \mathbf{Q}$ of $H = \mathbf{F}_{q^\kappa}$, $q = \operatorname{char}(F)$, the elements $T_1, \dots, T_l$ are algebraically independent over H, and the element η is separable and algebraic over $H(T_1, \dots, T_l)$; we denote by

$$\varphi = \sum_{0 \le i \le \deg_Z(\varphi)} (\varphi_i^{(1)}/\varphi_i^{(2)}) Z^i \in H(T_1, \dots, T_l)[Z]$$

its minimal polynomial over $H(T_1, \dots, T_l)$ with leading coefficient $\operatorname{lc}_Z(\varphi) = 1$, where $\varphi_i^{(1)}, \varphi_i^{(2)} \in H(T_1, \dots, T_l)$ are relatively prime. The element f has a unique representation as

$$f = \sum_{\substack{0 \le i < \deg_Z(\varphi) \\ 0 \le i_1, \dots, i_n \le d}} \frac{a_{i,i_1,\dots,i_n}}{b_{i,i_1,\dots,i_n}} \eta^i X_1^{i_1} \cdots X_n^{i_n},$$

where $a_{i,i_1,\dots,i_n}$, $b_{i,i_1,\dots,i_n} \in H(T_1, \dots, T_l)$ are relatively prime. In addition, let

$$\deg(\varphi) = \max_i \{\deg_Z(\varphi), \deg(\varphi_i^{(1)}), \deg(\varphi_i^{(2)})\} < d_1; \quad \deg_{X_j}(f) < d;$$

$$\deg_{T_j}(f) = \max_{i,i_1,\dots,i_n} \{\deg_{T_j}(a_{i,i_1,\dots,i_n}), \deg_{T_j}(b_{i,i_1,\dots,i_n})\} < d_0$$

for arbitrary j. By the length $l(h)$ of a record h when $h \in H$ we understand its bit length (see [1]), and when $h \in \mathbf{F}_{q^\kappa}$ the length is $\kappa \log(q)$. Suppose that the record length of every coefficient in H of the polynomials $a_{i,i_1,\dots,i_n}$ and $b_{i,i_1,\dots,i_n}$ ($\varphi_i^{(1)}$ and $\varphi_i^{(2)}$, respectively) is not greater than M (than M_1). The we take the record length to be $l(f) = 2d_0^l d_1 d_M^n$, i.e., f is represented as a vector of $2d_0^l d_1 d^n$ components in H, and similarly $l(\varphi) = 2d^{l+1})M_1$.

2. The problem of decomposition of f into finite irreducible polynomials has a long history (cf. [1] and [4]). All previously known algorithms for the decomposition of f have had an exponential upper bound on the complexity, as, for example, the classical algorithm of Kronecker [2] (see [5] also), even for the case $F = H$. When F is a finite field, $n = 1$, a decomposition algorithm, polynomial in $l(f)$ and q, was finally obtained after 50 years (see, e.g., [1]). Following were the essential steps: the $l(f)$-polynomial

1980 *Mathematics Subject Classification*. Primary 12E05, 68C05, 68C25; Secondary 14A10.

algorithm for the case $F = \mathbf{Q}$, $n = 1$ was proposed in [4]. In [6] an algorithm for the case $F = \mathbf{Q}$ was constructed having processing time polynomial in $(l(f))^n$. The authors in [7] obtained an algorithm polynomial in $l(f)$ and q for global fields F.

THEOREM 1. *A polynomial f can be decomposed into factors irreducible over F in time that is polynomial in $l(f)$, $l(\varphi)$ and q.*

In the proof of the theorem an essential use is made of an efficient version, proposed by the authors [7], of Hilbert's theorem on irreducibility for fields of nontrivial characteristic.

For every polynomial f the *absolute decomposition* $f = \prod_i f_i^{e_i}$ is its decomposition into factors that are not reducible over the algebraic closure $\overline{F}$ of the field F. If f is not reducible over F, then all the f_i are conjugate over F with $e_i = q^\nu$ for all i and some $\nu \geq 0$ when $q > 0$, and $e_i = 1$ when $\mathrm{char}(F) = 0$. We denote by F_i the decomposition of F induced by the coefficients of the polynomial $f_i^{q^\nu}$.

COROLLARY 1. *For every polynomial f irreducible over F we can find a time for its absolute decomposition that is polynomial in $l(f)$, $l(\varphi)$ and q, i.e., a polynomial $\psi \in F[Z]$, irreducible over F, such that $F_i \simeq F[Z]/(\psi)$, and a polynomial $f_i^{q^\nu} \in F_i[X_1, \ldots, X_n]$ for all i.*

3. We proceed now to a brief description of the algorithm for solving systems of algebraic equations $f_0 = f_1 = \cdots = f_{k-1} = 0$. Since we are actually proposing an algorithm for decomposing manifolds in projective space into irreducible components, we can assume that $f_0, f_1, \ldots, f_{k-1} \in F[X_0, X_1, \ldots, X_n]$ are homogeneous polynomials with degrees $\delta_0 \geq \delta_1 \geq \cdots \geq \delta_{k-1}$, respectively, and we let $V \subset \mathbf{P}^n(\overline{F})$ denote the manifold of the roots of the system $f_0 = f_1 = \cdots = f_{k-1} = 0$. We shall, moreover, assume that $\delta_0 < d$ and that, for the polynomials $f_0, f_1, \ldots, f_{k-1}$ satisfying the same bounds as the polynomial f in §1,

$$\deg_{T_1,\ldots,T_l}(f) = \max_{i,i_1,\ldots,i_n} \{\deg(a_{i,i_1,\ldots,i_n}), \deg(b_{i,i_1,\ldots,i_n})\} < d_2.$$

The problem of solving systems of algebraic equations also has a long history. Algorithms based on the theory of elimination [2] have a processing time bound even greater than exponential. The complexity bound for this problem has been improved in a sequence of articles, and the best estimate known to date [5] is polynomial in k, M and d^{2^n} in the case $F = H$.

In [8] an algorithm was constructed for finding the roots of a system when $\dim V = 0$ (we emphasize that it is essential here that V be in projective space). The construction in [8] is based on an effective version of the Hilbert theorem on zeros for homogeneous polynomials. This algorithm requires a number of arithmetic operations over the elements of F that is polynomial in kd^n. The result is an algorithm polynomial in the input length and d^n only in the case of a finite field F where, as before, $\dim V = 0$ (we note that the number of output elements of the algorithm, i.e., the number of roots of the system, is $\mathrm{card}(V) \leq (d-1)^n$, and in the general case equality occurs according to Bézout's theorem). To construct an algorithm for the arbitrary field in §1, it was necessary to modify the method of [8]. The modification for arbitrary fields F requires for the case considered below that V be of arbitrary dimension, even when the coefficients of the input system of equations belong to H. Let $D = \delta_0 + \delta_1 + \cdots + \delta_{n-1}$, $r = \binom{D+n}{n}$. We will assume that the field H contains a sufficient number of elements, enlarging it if necessary.

THEOREM 2. *We can construct an algorithm that tells us whether $\dim V = 0$ and whether it will find all the roots (with multiplicities) of the input system. In fact, all the roots are partitioned into conjugate classes over F for each of which the algorithm constructs a polynomial $\Phi \in F[Z]$, separable and irreducible over F, such that $\mathrm{lc}_Z(\Phi) = 1$.*

Moreover, the algorithm determines a j_0, $0 \leq j_0 \leq n$, *such that for each root* $(\xi_0 : \cdots : \xi_n) \in \mathbf{P}^n(\overline{F})$ *of this class,* $\xi_{j_0} \neq 0$, *and* $\xi_j = 0$ *for* $0 \leq j < j_0$. *In addition, the algorithm finds those* $\gamma_{j_0}, \ldots, \gamma_n \in H$ *(if* $\operatorname{card}(H) > (rd_1)^2$*) and the* q^ν, $1 \leq q^\nu \leq r$ *(in case* $\operatorname{char}(F) = 0$ *we stipulate that* $q^\nu = 1$*) for which the element* $\theta = \sum_{j_0 \leq j \leq n} \gamma_j (\xi_j/\xi_{j_0})^{q^\nu}$ *satisfies* $\Phi(\theta) = 0$. *Here*

$$F[(\xi_{j_0+1}/\xi_{j_0})^{q^\nu}, \ldots, (\xi_n/\xi_{j_0})^{q^\nu}] = F[\theta] = F[Z]/(\Phi),$$

and the algorithm constructs an expression for $(\xi_j/\xi_{j_0})^{q^\nu} \in F[\theta]$ *for* $j_0 < j \leq n$. *The number of conjugate roots in the class is equal to* $\deg_Z(\Phi) \leq \operatorname{card}(V)$.

The degrees

$$\max_{1 \leq i \leq l} \deg_{T_i}(\Phi), \qquad \max_{1 \leq i \leq l} \{\deg_{T_i}((\xi_j/\xi_{j_0})^{q^\nu})\}$$

(they are determined as in §1) are bounded above by a certain polynomial in r, d_1 *and* d_2. *The lengths of the records* $l(\Phi)$ *and* $l((\xi_j/\xi_{j_0})^{q^\nu})$ *(they are also determined as in §1) are bounded above by a certain polynomial in* r^l, d_1^l, d_2^l, M *and* M_1 *which is linear in* M *and* M_1. *Finally, the operating time of the algorithm is polynomial in* $r^l, d_1^l, d_2^l, M, M_1, k$ *and* q.

4. We now proceed to a discussion of the case in which V is of arbitrary dimension. Since V is defined over the field $F^{q^{-\infty}}$ (the maximal purely nonseparable purely nonseparable decomposition of F [3]), we can expand V in the form $V = \bigcup_\alpha W_\alpha$, where the W_α are defined and irreducible over $F^{q^{-\infty}}$. Furthermore, $W_\alpha = \bigcup_\beta W_{\alpha\beta}$, where the components $W_{\alpha\beta}$ are defined and irreducible over $\overline{F}$. The proposed algorithm finds all the W_α and then the $W_{\alpha\beta}$ (in fact, the W_α and $W_{\alpha\beta}$ are defined over certain finite extensions of F [3] which the algorithm also finds).

Let $W \subset \mathbf{P}^n(\overline{F})$ be a manifold, $\operatorname{codim}_{\mathbf{P}^n} W = m$, defined and irreducible over some field F_1 which is a finite extension of F, and let F_2 be the maximal subfield of F_1, a separable extension of F. Let $t_1, \ldots, t_{n-m}$ be algebraically independent over F. We can define a generic point of W by the following field isomorphism:

$$(1) \quad F_2(t_1, t_2, \ldots, t_{n-m})[\theta]$$
$$\simeq F_2\left(\sum_{0 \leq j \leq n} \lambda_{1j} \frac{X_j}{X_{j_0}}, \ldots, \sum_{0 \leq j \leq n} \lambda_{n-m,j} \frac{X_j}{X_{j_0}}, \left(\frac{X_0}{X_{j_0}}\right)^{q^\nu}, \ldots, \left(\frac{X_n}{X_{j_0}}\right)^{q^\nu}\right) \subset F_1(W)$$

for some q^ν, where θ is an algebraic and separable element over $F_2(t_1, \ldots, t_{n-m})$ and $\Phi(z)$ is its minimal polynomial, $\det_Z(\Phi) \leq \deg W$, $\operatorname{lc}_Z(\Phi) = 1$; the elements X_j/X_{j_0} are considered here as rational functions on W, where W does not lie in the hyperplane defined by the equation $X_{j_0} = 0$; and $\lambda_{sj} \in H$.

Let $c = c(V) = \min\{\max_\alpha \dim W_\alpha, \max_\alpha \operatorname{codim} W_\alpha\}$ and let L denote the length of the input data record (see below).

THEOREM 3. 1) *One can construct an algorithm which defines for each component* W_α *its generic point and constructs a family of homogeneous manifolds* $\psi_1^{(\alpha)}, \ldots, \psi_N^{(\alpha)} \in F[X_0, \ldots, X_n]$ *such that the set of roots of the system* $\psi_1^{(\alpha)} = \cdots = \psi_N^{(\alpha)} = 0$ *is identical with* W_α. *Let* $m = \operatorname{codim} W_\alpha$, $\theta_\alpha = \theta$ *and* $\Phi_\alpha = \Phi$.

Then $q^\nu \leq d^{2m}$ *and* $\deg_Z(\Phi_\alpha) \leq \deg W_\alpha \leq d^m$; *for all* i *and* j *the degrees*

$$\deg_{T_i} \Phi_\alpha, \quad \deg_{t_i}(\Phi_\alpha), \quad \deg_{T_i}((X_j/X_{j_0})^{q^\nu}), \quad \deg_{t_i}((X_j/X_{j_0})^{q^\nu})$$

(the last two are defined in accordance with the isomorphism of (1)) are bounded above by a certain polynomial in $d^m d_1 d_2$; *and the lengths of the records* $l(\lambda_{sj})$, $l(\Phi_\alpha)$ *and* $l((X_j/X_{j_0})^{q^\nu})$ *are bounded above by a polynomial in* M_1, M *and* $(d^m d_1 d_2)^{n-m+l+1}$. *The number of equations is* $N \leq m^2 d^{4m}$ *and the degrees* $\deg_{X_i}(\psi_j^{(\alpha)})$ *and* $\deg_{T_i}(\psi_j^{(\alpha)})$ *are*

bounded above by a polynomial in $d^m d_1 d_2$; the algorithm displays each $\psi_j^{(\alpha)}$ in the form $\psi_j^{(\alpha)} = \tilde{\psi}_j^{(\alpha)}(Z_{j,0}, \dots, Z_{j,n-m+2})$, where the $Z_{j,i}$ are linear forms in $X_0, X_1, \dots, X_n$ with coefficients in the field H; the record length $l(\tilde{\psi}_j^{(\alpha)})$ does not exceed a certain polynomial in M_1, M and $(d^m d_1 d_2)^{n-m+l+1}$; and $l(Z_{j,i})$ does not exceed a certain polynomial in n and $\log(dd_1d_2)$. The overall operating time of the algorithm is bounded above by a polynomial in

$$MM_1 d^{n(c+l+1)}(d_1d_2)^{n+l}k(q+1).$$

The last value obviously does not exceed

$$O(L^{c+l+1}(q+1)) \le O(L^{\log L}(q+1))$$

when $n, d_1, d_2 = 0(d^{\Omega})$, $\Omega = \text{const}$.

2) *One can construct an algorithm which finds for each component $W_{\alpha\beta}$ the maximal separable subfield $F_2 = F[\mu]$ of the minimal field of definition of F_1 (containing F) of the manifold $W_{\alpha\beta}$. The algorithm constructs a generic point of $W_{\alpha\beta}$ as well as a system of equations with coefficients in F_2 defining $W_{\alpha\beta}$. For the parameters of the generic point and of the system of equations the same bounds are satisfied as in 1). Let $\varphi_{\alpha\beta} \in F[Z]$ be the minimal variety for μ and $\mathrm{lc}_Z(\varphi_{\alpha\beta}) = 1$; then $\deg_Z(\varphi_{\alpha\beta}) \le \deg W_{\alpha\beta}$; the $\deg_{T_i}(\varphi_{\alpha\beta})$ are bounded above by a polynomial in $d^m d_1 d_2$; and the record lengths $l(\varphi_{\alpha\beta})$ are bounded above by a polynomial in $MM_1(d^m d_1 d_2)^{l+1}$. The processing-time bound is the same as in §1).*

Theorem 3 generalizes Theorem 1 ($\operatorname{codim} V = 1$) and Theorem 2 ($\dim V = 0$) to the case of arbitrary dimension of V, and its proof is essentially based on them. We also mention that the upper bound to the output length of the algorithm of Theorem 3 is of the same order as the processing-time bound cited in the theorem, and therefore the greatest reduction in the processing time can be expected only when the representation of the manifold component is different from what we have presented here.

Leningrad Branch
Steklov Institute of Mathematics
Academy of Sciences of the USSR

Leningrad Scientific-Research Computing Center
Academy of Sciences of the USSR

Received 13/JUNE/83

BIBLIOGRAPHY

1. Donald E. Knuth, *The art of computer programming*. Vol. 2, Addison-Wesley, 1969.
2. B. L. van der Waerden, *Moderne Algebra*. Vols. I, II, Springer-Verlag, 1930, 1931; English transl. of later eds., Ungar, New York, 1970.
3. Oscar Zariski and Pierre Samuel, *Commutative algebra*. Vols. I, II, Van Nostrand, Princeton, N.J., 1958, 1960.
4. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, Math. Ann. **261** (1982), 515–534.
5. A. Seidenberg, Trans. Amer. Math. Soc. **197** (1974), 273–313.
6. Erich Kaltofen, 23rd Annual Sympos. Foundations of Computer Sci. (Chicago, 1982), IEEE Computer Soc. Press, Los Angeles, Calif., 1982, pp. 57–64.
7. A. L. Chistov and D. Yu. Grigoryev [Grigor'ev], Preprint E-5-82, Leningrad Branch Steklov Inst. Math. Acad. Sci. USSR, Leningrad, 1982. (English)
8. Daniel Lozard, Theoret. Computer Sci. **15** (1981), 77–110.

Translated by R. N. GOSS