Effective Hilbert Irreducibility*

Erich Kaltofen†

University of Toronto
Department of Computer Science
Toronto, Ontario M5S1A4, Canada

Abstract

In this paper we prove by entirely elementary means a very effective version of the Hilbert Irreducibility Theorem. We then apply our theorem to construct a probabilistic irreducibility test for sparse multivariate polynomials over arbitrary perfect fields. For the usual coefficient fields the test runs in polynomial time in the input size.

Keywords. Hilbert Irreducibility Theorem, Probabilistic Algorithms, Polynomial Factorization, Sparse Polynomials.

1. Introduction

The question whether a polynomial with coefficients in a unique factorization domain is irreducible poses an old problem. Recently, several new algorithms for univariate and multivariate factorization over various coefficient domains have been proposed within the framework of polynomial time complexity, see e.g. Berlekamp (1970), Lenstra et al. (1982), Kaltofen (1985a), Chistov and Grigoryev (1982), Landau (1985). All algorithms in the references just given are polynomial in $l(n+1)^v$, where l is the number of bits needed to represent the coefficients of the polynomial to be factored, n is its total degree, and v is the number of its variables. The algorithms for finite fields are probabilistic (Las Vegas – always correct and probably fast.) If v is not fixed, $l(n+1)^v$ may not represent the input size since the input polynomial may only consist of a few monomials. In this sparse case, J. von zur Gathen (1985a) has developed a probabilistic irreducibility test and factorization algorithm, the former of the Monte Carlo kind and polynomial in the degree and the number of non-zero monomials of the polynomial to be tested for irreducibility. His algorithm is based on the Hilbert Irreducibility Theorem, as was our older multivariate to bivariate reduction (cf. Kaltofen (1985a), §7), and a

* This research was partially supported by the National Science and Engineering Council of Canada under grant 3-643-126-90.

† Author's current address: Department of Computer Science, Rensselaer Polytechnic Institute, Troy, New York 12181.

This paper appears in *Information and Control*, **66**, pp. 123--137 (1985).

generalized version of the sparse Hensel lifting scheme of Zippel (1981).

In §3 we shall prove a new very effective Hilbert Irreducibility theorem, which, applied to the rational coefficient case, states roughly the following: If a polynomial $f(x_1, \ldots, x_v)$ is irreducible then the probability that $f(x_1+w_1, c_2x_1+w_2, \ldots, c_{v-1}x_1+w_{v-1}, x_2)$ becomes reducible for randomly chosen integers $c_2, \ldots, c_{v-1}, w_1, \ldots, w_{v-1}$ of $O(\deg f + \log 1/\varepsilon)$ digits is less than ε. In von zur Gathen (1985a), Lemma 4.3, the integers have $O(\deg^2 f + \log 1/\varepsilon)$ digits and the substitutions are somewhat more complicated ($c_i x_1 + u_i x_2 + w_i$ for x_i.) We also use elementary methods to prove our result whereas von zur Gathen follows the algebraic geometric approach of Heintz and Sieveking (1981) which is based on Bertini's theorem.

In §4 we then use our effective Hilbert Irreducibility Theorem to establish Monte-Carlo irreducibility tests for sparse multivariate polynomials. The tests are similar to probabilistic primality testing except that they definitely establish irreducibility but compositeness only with a small failure probability. For rational coefficients the test runs in time polynomial in the number of non-zero monomials of the input polynomial, its total degree, and its coefficient length. Our theorem also applies to coefficients from a field of positive characteristic p provided the p-th root of any element can be taken within this field. Therefore our theorem includes the important case in which the coefficients lie in a finite field. We propose a different irreducibility test in this case, which, unlike the algorithms by Chistov and Grigoryev (1982) and von zur Gathen (1985a), does not require one to work in an algebraic extension of the coefficient domain. All irreducibility tests rely on polynomial-time irreducibility tests for polynomials in two or three variables.

Notation: By $\mathbf{Z}$ we denote the integers, by $\mathbf{Q}$ the rationals and by $\mathbf{C}$ the complex numbers. $\mathbf{Z}_p$ denotes the field of residues modulo the prime p. D shall denote an integral domain, $\mathrm{QF}(D)$ its field of quotients, $\mathrm{char}(D)$ its characteristic. $D[x_1, \ldots, x_v]$ denotes the polynomials in $x_1, \ldots, x_v$ over D, $D(x_1, \ldots, x_v)$ the corresponding field of quotients; $\deg_{x_1}(f)$ denotes the highest degree of x_1 in $f \in D[x_1, \ldots, x_v]$, $\deg_{x_1,x_2}(f)$ the highest total degree of f in the variables x_1 and x_2, and $\deg(f) = \deg_{x_1,\ldots,x_v}(f)$ the total degree of f. The coefficient of the highest power of x_v in f is referred to as the leading coefficient of f in x_v and will be denoted by $\mathrm{ldcf}_{x_v}(f)$. We call f monic in x_v if $\mathrm{ldcf}_{x_v}(f)$ is a unit of D. As is well-known, $D[x_1, \ldots, x_v]$ is a unique factorization domain (UFD) provided that D is a UFD. In this case the content of $f \in D[x_1, \ldots, x_v]$ in x_v, $\mathrm{cont}_{x_v}(f)$, is the greatest common divisor (GCD) of all coefficients of $f(x_v)$ as elements in $D[x_1, \ldots, x_{v-1}]$. The primitive part of f in x_v is defined as

$$\mathrm{pp}_{x_v}(f) = \frac{1}{\mathrm{cont}_{x_v}(f)}\, f$$

and we call f primitive in x_v if $f = \mathrm{pp}_{x_v}(f)$. We also note that the total degree of a factor of f with respect to any variable set is less than or equal to the total degree of f in that variable set. The infinity norm of $f \in \mathbf{Q}[x_1, \ldots, x_v]$, the maximum of the absolute values of the rational coefficients of f, will be denoted by $| f |$. The squareroot of the sum of squares of the coefficients of f, the square norm of f, will be denoted by $| f |_2$.

Let $f(x_v) = a_l x_v^l + a_{l-1} x_v^{l-1} + \cdots + a_0$ and $g(x_v) = b_m x_v^m + \cdots + b_0$ with $a_i, b_j \in D[x_1 ,\ldots, x_{v-1}]$, $a_l b_m \neq 0$. By $\mathrm{res}_{x_v}(f, g)$ we denote the resultant of f and g with respect to x_v. As is well-known, $\mathrm{res}_{x_v}(f, g) \neq 0$ if and only if $\mathrm{GCD}(f, g)$ over $D(x_1 ,\ldots, x_{v-1})[x_v]$ is a constant.

The probability of an event E will be denoted by $P(E)$, the cardinality of a set S by $\mathrm{card}(S)$. The vertical stroke $|$ stands for the divisibility relation.

2. Preliminary Results

First we prove a lemma stating that the set of zeros of a multivariate polynomial over an integral domain D is of small measure. (Measure 0 if $\mathrm{card}(D) = \infty$.)

Lemma 1 (cf. Schwartz (1980)): Assume that $t(y_1,\ldots,y_v) \in D[y_1 ,\ldots, y_v]$ is a non-zero polynomial of total degree d and let $S \subseteq D$. Then the probability

$$P(t(c_1,\ldots,c_v) = 0 \mid c_i \in S,\ 1 \le i \le v) \le \frac{d}{\mathrm{card}(S)}.$$

Proof: Induction on v. For $v = 1$, $t(y_1)$ has at most d roots in D, hence the probability

$$P(t(c_1) = 0 \mid c_1 \in S) \le \frac{d}{\mathrm{card}(S)}$$

Assume, the statement is true for $v-1$. Let $l(y_1,\ldots,y_{v-1}) = \mathrm{ldcf}_{y_v}(t)$, $n = \deg_{y_v}(t)$. Then $\deg(l) \le d-n$ and by induction hypothesis

$$P(l(c_1,\ldots,c_{v-1}) = 0 \mid c_i \in S,\ 1 \le i \le v-1) \le \frac{d-n}{\mathrm{card}(S)}$$

In case $l(c_1,\ldots,c_{v-1}) \neq 0$ there are at most n roots for $t(c_1 ,\ldots, c_{v-1}, y_v)$. Therefore,

$$\begin{aligned} P(t(c_1,\ldots,c_v) = 0) &= P(t = 0 \mid l = 0)\, P(l = 0) + P(t = 0 \mid l \neq 0)\, P(l \neq 0) \\ &\le P(l(c_1,\ldots,c_{v-1}) = 0) + P(t(c_1,\ldots,c_v) = 0 \mid l(c_1,\ldots,c_{v-1}) \neq 0) \\ &\le \frac{d-n}{\mathrm{card}(S)} + \frac{n}{\mathrm{card}(S)} = \frac{d}{\mathrm{card}(S)}. \quad \square \end{aligned}$$

Secondly, we prove that squarefreeness of an irreducible multivariate polynomial is likely to be preserved by evaluation.

Lemma 2: Let $f(y_1,\ldots,y_v,x) \in F[y_1,\ldots,y_v,x]$ be irreducible in $F(y_1 ,\ldots, y_v)[x]$, F a field, and assume further that $\partial f / \partial x \neq 0$. Let $n = \deg_x(f)$, $d = \deg_{y_1,\ldots,y_v}(f)$ and $a_n(y_1 ,\ldots, y_v) = \mathrm{ldcf}_x(f)$. We now select $w_1 ,\ldots, w_v$ randomly from a subset $S \subseteq F$. Then the probability

$$P(a_n(w_1,...,w_v) = 0 \text{ or } f(w_1,...,w_v,x) \text{ not squarefree}) \le \frac{(2n+1)\,d}{\mathrm{card}(S)}.$$

Proof: Since f is irreducible and $\partial f/\partial x \ne 0$, $\mathrm{GCD}(f, \partial f/\partial x) = 1$. Therefore the resultant

$$\Delta_f(y_1,\ldots,y_v) = \mathrm{res}_x\left(f, \frac{\partial f}{\partial x} \right) \ne 0.$$

Notice that $\deg(\Delta_f) \le (2n-1)d$. Now let $\partial f/\partial x = k\,a_k x^{k-1} + \cdots + a_1$ with $k\,a_k \ne 0$, $1 \le k \le n$, where $a_i \in F[y_1, \ldots, y_v]$ are the coefficients of x^i in f, $\deg(a_i) \le d$, $1 \le i \le n$. If we select $w_1, \ldots, w_v$ such that $(a_n a_k \Delta_f)(w_1, \ldots, w_v) \ne 0$, then $\bar{f}(x) = f(w_1, \ldots, w_v, x)$ is squarefree. For were it not, then $\mathrm{GCD}(\bar{f}, \mathrm{d}\bar{f}/\mathrm{d}x) \ne 1$ implying that $\Delta_{\bar{f}} = \mathrm{res}(\bar{f}, \mathrm{d}\bar{f}/\mathrm{d}x) = 0$. But $\Delta_{\bar{f}} = \Delta_f(w_1, \ldots, w_v) \ne 0$, a contradiction.

Since $\deg(a_n a_k \Delta_f) \le (2n+1)d$, by lemma 1 we conclude that randomly chosen $w_1, \ldots, w_v$ do not nullify $a_n a_k \Delta_f$ with probability at least $1 - (2n+1)d/\mathrm{card}(S)$. □

Notice that if $\mathrm{char}(F) = 0$, then the condition $\partial f/\partial x \ne 0$ in the previous lemma is automatically satisfied. However, in the case that $\mathrm{char}(F) = p > 0$, this condition cannot be omitted. E.g. if F is a finite field with p elements, then $x^p + y$ is irreducible but for every $w \in F$, $x^p + w = (x+w)^p$ is not squarefree. Lemma 4 in section 3 proves, to some extent, that this is the only kind of counter-example possible.

Thirdly, we establish that evaluations rarely allow a GCD of higher degree to occur. For more clarity in the later proof of theorem 2 we shall defer the application of lemma 1 and not formulate this lemma in terms of probabilities.

Lemma 3: Let $f_1, \ldots, f_k \in F[x_1, \ldots, x_v]$, F a field, with $\deg(f_i) \le \delta$ for $1 \le i \le k$ and $\mathrm{GCD}(f_1, \ldots, f_k) = 1$. Furthermore, assume that $f_1(0, \ldots, 0) \ne 0$. Then there exists a polynomial $\Delta(y_2, \ldots, y_v) \in F[y_2, \ldots, y_v]$ with $\deg(\Delta) \le 2\delta^2$ such that for any elements $c_2, \ldots, c_v \in F$ with $\Delta(c_2, \ldots, c_v) \ne 0$ the $\mathrm{GCD}_{1 \le i \le k}\,(f_i(x_1, c_2x_1, \ldots, c_vx_1)) = 1$.

Proof: As can be seen easily from the fact that $x_1 \nmid f_1(x_1, y_2x_1, \ldots, y_vx_1)$, $\mathrm{GCD}_{1 \le i \le k}\,(f_i(x_1, y_2x_1, \ldots, y_vx_1)) = 1$ in $F[x_1, y_2, \ldots, y_v]$. Therefore we can find (not necessarily unique) polynomials $s_1, \ldots, s_k \in F(y_2, \ldots, y_v)[x_1]$ with $\deg_{x_1}(s_i) < \delta$ such that

$$1 = \sum_{i=1}^{k} s_i(y_2,\ldots,y_v,x_1)\, f_i(x_1,y_2x_1,\ldots,y_vx_1).$$

This identity leads to a linear system over $F(y_2, \ldots, y_v)$ in 2δ equations and $k\delta$ unknown coefficients of s_i. Hence we can find a solution in $\dfrac{1}{\Delta(y_2,\ldots,y_v)} F[y_2, \ldots, y_v]$ where Δ is a $2m$ by $2m$, $m \le \delta$, determinant of coefficients of powers of x_1 in $f_i(x_1, y_2x_1, \ldots, y_vx_1)$. Therefore $\deg(\Delta) \le 2\delta^2$ and any choice of $c_2, \ldots, c_v$ with $\Delta(c_2, \ldots, c_v) \ne 0$ forces $\mathrm{GCD}_{1 \le i \le k}\,(f_i(x_1, c_2x_1, \ldots, c_vx_1)) = 1$ since $\sum_{i=1}^{k} s_i(c_2, \ldots, c_v, x_1)\, f_i(x_1, c_2x_1, \ldots, c_vx_1) =$

1. □

In theorem 2 we will need a non-monic version of the Hensel lemma whose statement and proof follows for completeness. We adopt the following vector notation: $\underline{k} \equiv (k_1,\ldots,k_v)$, $\underline{0} \equiv (0,\ldots,0)$, $\underline{y}^{\underline{k}} \equiv y_1^{k_1}\cdots y_v^{k_v}$, $\underline{k} \pm \underline{k}' \equiv (k_1 \pm k_1', \ldots, k_v \pm k_v')$, $\underline{k} \le \underline{k}'$ if, for all i, $k_i \le k_i'$, and finally $|\underline{k}| \equiv k_1 + \cdots + k_v$ if $\underline{k} \ge \underline{0}$, and $-\infty$ otherwise.

Theorem 1 (*Hensel lemma*): Let $f(y_1,\ldots,y_v,x) \in F[y_1,\ldots,y_v,x]$, F a field, be of degree n in x, $l(y_1,\ldots,y_v) = \mathrm{ldcf}_x(f)$ such that $l_{\underline{0}} = l(0,\ldots,0) \ne 0$ and $f_{\underline{0}}(x) = f(0,\ldots,0,x)$ is squarefree. Suppose

$$\left(l_{\underline{0}}x^i + g_{\underline{0}}(x)\right)\left(l_{\underline{0}}x^j + h_{\underline{0}}(x)\right) = l_{\underline{0}} f_{\underline{0}}(x),\quad i+j=n$$

is a non-trivial factorization of $l_{\underline{0}} f_{\underline{0}}$ in $F[x]$. Then there exist, for all $\underline{k}$ with $|\underline{k}| \ge 1$, unique polynomials $g_{\underline{k}}(x)$, $h_{\underline{k}}(x) \in F[x]$ with $\deg(g_{\underline{k}}) < i$, $\deg(h_{\underline{k}}) < j$ such that

$$l(y_1,\ldots,y_v)\, f(y_1,\ldots,y_v,x) = \tag{1}$$

$$\left(l(y_1,\ldots,y_v)x^i + \sum_{\underline{k}\ge\underline{0}} g_{\underline{k}}(x)\underline{y}^{\underline{k}}\right)\left(l(y_1,\ldots,y_v)x^j + \sum_{\underline{k}\ge\underline{0}} h_{\underline{k}}(x)\underline{y}^{\underline{k}}\right).$$

Proof: We truncate the multivariate Taylor series in (1) to maximum order m and establish the existence and uniqueness of $g_{\underline{k}}$, $h_{\underline{k}}$, $0 \le |\underline{k}| \le m$ in that truncated equation by induction on m. For $m = 0$, $\underline{k} = \underline{0}$ and the statement is true by assumption. Rewrite $l = \sum_{\underline{k}\ge\underline{0}} l_{\underline{k}}\, \underline{y}^{\underline{k}}$ with $l_{\underline{k}} \in F$, and $lf - l^2x^n = \sum_{\underline{k}\ge\underline{0}} f_{\underline{k}}\, \underline{y}^{\underline{k}}$ with $f_{\underline{k}} \in F[x]$ and $\deg(f_{\underline{k}}) < n$. We now consider the coefficient of $\underline{y}^{\underline{k}}$, $|\underline{k}| = m$, in

$$\left(lx^i + \sum_{\underline{k}\ge\underline{0}} g_{\underline{k}}\, \underline{y}^{\underline{k}}\right)\left(lx^j + \sum_{\underline{k}\ge\underline{0}} h_{\underline{k}}\, \underline{y}^{\underline{k}}\right) - l^2x^n,$$

namely

$$g_{\underline{k}}(l_{\underline{0}}x^j + h_{\underline{0}}) + h_{\underline{k}}(l_{\underline{0}}x^i + g_{\underline{0}}) +$$

$$\sum_{\underline{0}\le\underline{s}\le\underline{k},\, 1\le|\underline{s}|\le|\underline{k}|-1} \left(l_{\underline{s}}(x^i h_{\underline{k}-\underline{s}} + x^j g_{\underline{k}-\underline{s}}) + g_{\underline{s}} h_{\underline{k}-\underline{s}}\right)$$

where we denote the sum in this expression by $b_{\underline{k}}$. By induction hypothesis, $b_{\underline{k}}$ is unique and $\deg(b_{\underline{k}}) < n$. It is necessary and sufficient for (1) to be true to order m that $g_{\underline{k}}$ and $h_{\underline{k}}$, $|\underline{k}| = m$, satisfy

$$g_{\underline{k}}(l_{\underline{0}}x^j + h_{\underline{0}}) + h_{\underline{k}}(l_{\underline{0}}x^i + g_{\underline{0}}) = f_{\underline{k}} - b_{\underline{k}}.$$

Since $f_{\underline{0}}$ is squarefree, $l_{\underline{0}}x^j + h_{\underline{0}}$ and $l_{\underline{0}}x^i + g_{\underline{0}}$ have no common polynomial factor which, by the extended Euclidean algorithm for polynomials guarantees the existence of $g_{\underline{k}}$ and $h_{\underline{k}}$. Under the degree constraints $\deg(g_{\underline{k}}) < i$, $\deg(h_{\underline{k}}) < j$ and the fact $\deg(f_{\underline{k}} - b_{\underline{k}}) < n$ these polynomials are also unique. □

Remark: The purpose of multiplying f with l before lifting is to be able to uniquely predetermine the leading coefficients of any possible polynomial factorization of $f = g\,h$.

3. An Effective Hilbert Irreducibility Theorem

We proceed to prove a random, but very effective version of the Hilbert irreducibility theorem for multivariate polynomials over an arbitrary field F with one restriction. In the case in which $\mathrm{char}(F) = p > 0$ we require that for each element $a \in K$ there exists a $b \in K$ such that $b^p = a$. This condition is, of course, satisfied if F is a finite field.

The fundamental theorem of this section follows now.

Theorem 2: Let $f(x_1, \ldots, x_v) \in F[x_1, \ldots, x_v]$, F a field, have total degree δ and be irreducible. Assume that $\partial f / \partial x_v \neq 0$. Let $S \subseteq F$ and let $c_2, \ldots, c_{v-1}, w_1, \ldots, w_{v-1}$ be random elements in S. Then the probability

$$P(f(x_1 + w_1, c_2 x_1 + w_2, \ldots, c_{v-1} x_1 + w_{v-1}, x_2)$$
$$\text{becomes reducible in } F[x_1, x_2]) \leq \frac{4\delta\, 2^{\delta}}{\mathrm{card}(S)}.$$

Proof: By lemma 2 the probability that $f(w_1, \ldots, w_{v-1}, x)$ remains squarefree and of the same degree as f is at least $1 - (2n+1)d/\mathrm{card}(S)$ where $n = \deg_{x_v}(f)$ and $d = \deg_{x_1, \ldots, x_{v-1}}(f)$. Assume now that this is the case.

We first show how to evaluate f such that it remains irreducible in $F(x_1)[x_2]$. Write

$$g(y_1, \ldots, y_{v-1}, x) = l(y_1, \ldots, y_{v-1})\, f(y_1 + w_1, \ldots, y_{v-1} + w_{v-1}, x)$$

where

$$l(y_1, \ldots, y_{v-1}) = \mathrm{ldcf}_{x_v}(f)(y_1 + w_1, \ldots, y_{v-1} + w_{v-1}).$$

Let $F[[y_1, \ldots, y_{v-1}]]$ denote the domain of formal power series in $y_1, \ldots, y_{v-1}$ over F. We set

$$g_{\underline{c}}(y_1, x) = g(y_1, c_2 y_1, \ldots, c_{v-1} y_1, x)$$

and

$$l_{\underline{c}}(y_1) = l(y_1, c_2 y_1, \ldots, c_{v-1} y_1).$$

Then each factor $\hat{h}(y_1, x) \in F[[y_1]][x]$ of $g_{\underline{c}}$ with $\mathrm{ldcf}_x(\hat{h}) = l_{\underline{c}}$ corresponds to a factor $h \in F[[y_1, \ldots, y_{v-1}]][x]$ of g with $\mathrm{ldcf}_x(h) = l$ such that

$$\hat{h}(y_1, x) = h_{\underline{c}}(y_1, x) = h(c_2 y_1, \ldots, c_{v-1} y_1, x).$$

Since if that were not the case we could present, by theorem 1, two different factorizations of $g_{\underline{c}}$, which, when evaluated at $y_1 = 0$ would result in one and the same factorization of $g_{\underline{c}}(0, x) \in F[x]$. But this is impossible due to the uniqueness of the Hensel lifting procedure, as proven in theorem 1.

We will show that for integers $c_2, \ldots, c_{v-1}$ not nullifying a certain polynomial $\pi(z_2, \ldots, z_{v-1}) \in F[z_2, \ldots, z_{v-1}]$ of degree at most $4d(2^{n-1}-1)$ no factor derived from g in such a way can be a polynomial dividing $g_{\underline{c}}$.

Let

$$h(y_1, \ldots, y_{v-1}, x) = \sum_{j=0}^{i} \sum_{\underline{k} \geq \underline{0}} b_{\underline{k},j}\, \underline{y}^{\underline{k}}\, x^j$$

be a factor of $g(y_1, \ldots, y_v, x)$ in $F[[y_1, \ldots, y_{v-1}]][x]$ with $0 < i < n$ and $\mathrm{ldcf}_x(h) = l$ and let

$$\bar{h}(y_1, \ldots, y_{v-1}, x) = \sum_{j=0}^{n-i} \sum_{\underline{k} \geq \underline{0}} \bar{b}_{\underline{k},j}\, \underline{y}^{\underline{k}}\, x^j$$

be its cofactor, i.e. $g = h\,\bar{h}$. There must exist at least one $b_{\underline{k},j}$ or $\bar{b}_{\underline{k},j}$ with

$$2d < |\underline{k}| \leq 4d \text{ and } (b_{\underline{k},j} \neq 0 \text{ or } \bar{b}_{\underline{k},j} \neq 0).$$

To see this, assume the contrary. Then

$$\left(\sum_{j=0}^{i} \sum_{0 \leq |\underline{k}| \leq 2d} b_{\underline{k},j}\, \underline{y}^{\underline{k}}\, x^j \right) \left(\sum_{j=0}^{n-i} \sum_{0 \leq |\underline{k}| \leq 2d} \bar{b}_{\underline{k},j}\, \underline{y}^{\underline{k}}\, x^j \right) = g(y_1, \ldots, y_{v-1}, x)$$

since no monomial $a\,\underline{y}^{\underline{k}}\, x^j$, a a non-zero element of F, with $2d < |\underline{k}| \leq 4d$ in the left product could be cancelled by higher terms in the product of the complete expansion of h and $\bar{h}$. Notice that g does not contain a monomial in $\underline{y}$ of degree larger than $2d$. But this contradicts the fact that f is irreducible. Without loss of generality we now can assume the existence of a vector $\underline{p}$ and an integer m such that

$$b_{\underline{p},m} \neq 0 \text{ with } 2d < |\underline{p}| \leq 4d \text{ and } 0 \leq m < i.$$

Set

$$t_{\underline{p},m}(y_1, \ldots, y_{v-1}) = \sum_{|\underline{j}| = |\underline{p}|} b_{\underline{j},m} \underline{y}^{\underline{j}}$$

which is the coefficient of x^m in h of order $|\underline{p}|$ in $y_1, \ldots, y_{v-1}$ and which is a non-zero polynomial in $F[y_1, \ldots, y_{v-1}]$. By choosing $c_2, \ldots, c_{v-1}$ such that

$$t_{\underline{p},m}(y_1, c_2 y_1, \ldots, c_{v-1} y_1) \neq 0$$

we guarantee that $h_{\underline{c}}(y_1, x)$ has a non-zero coefficient of order $|\underline{p}|$ in y_1. Therefore $h_{\underline{c}}$ cannot be a polynomial dividing $g_{\underline{c}}$. The polynomial $\pi(z_2, \ldots, z_{v-1})$ then can be chosen as the product of $t_{\underline{p},m}(1, z_2, \ldots, z_{v-1}) \neq 0$ over all possible factor candidates h. Since there are at most n irreducible factors of g in $F[[y_1, \ldots, y_{v-1}]][x]$ and we do not need to consider complementary candidates there are at most $2^{n-1}-1$ possibly reducible factors to refute (see also remark below). Thus $\deg(\pi) \leq 4d(2^{n-1}-1)$ and we know that each non-zero $c_2, \ldots, c_{v-1}$ of π

prevents the polynomial $g_{\underline{c}}(x_1, x_2)$ from having a factor in $F[[x_1]][x_2]$ all of whose coefficients have order in x_1 less than $\deg_{x_1}(g_{\underline{c}}(x_1, x_2))$. Therefore this bivariate polynomials is irreducible in $F(x_1)[x_2]$ and so is

$$f(x_1 + w_1, c_2 x_2 + w_2, \ldots, c_{v-1} x_{v-1} + w_{v-1}, x_2).$$

We finally must refute a possible content in $F[x_1]$. Let $l_i(y_1, \ldots, y_{v-1})$ be the coefficient of x^i in $f(y_1+w_1, \ldots, y_{v-1}+w_{v-1}, x)$, $\deg(l_i) \le d$. Note that l_n is our previous l and also $l_n(0, \ldots, 0) \ne 0$. Since f is irreducible $\mathrm{GCD}_{0 \le i \le n}(l_i) = 1$. By lemma 3 there exists a polynomial Δ with $\deg(\Delta) \le 2d^2$ such that $\Delta(c_2, \ldots, c_{v-1}) \ne 0$ implies $\mathrm{GCD}_{0 \le i \le n}(l_i(y_1, c_2 y_1, \ldots, c_{v-1} y_1)) = 1$. For such c_i our evaluated polynomial cannot have a content in x_2, i.e. a factor in $F[x_1]$.

In summary, we must avoid zeros of $\pi\Delta$. By lemma 1, random $c_2, \ldots, c_{v-1}$ from S make $(\pi\Delta)(c_2, \ldots, c_{v-1}) \ne 0$ with probability $1 - (\deg(\pi) + \deg(\Delta)) / \mathrm{card}(S)$. Taking the choice of the w into account, the probability of success is at least

$$\left(1 - \frac{(2n+1)d}{\mathrm{card}(S)}\right) \left(1 - \frac{4d(2^{n-1}-1) + 2d^2}{\mathrm{card}(S)}\right) \ge 1 - \frac{4\delta 2^\delta - 3d}{\mathrm{card}(S)} \ge 1 - \frac{4\delta 2^\delta}{\mathrm{card}(S)}$$

with $\delta = \deg(f)$. □

Remark: The bound $4\delta 2^\delta/\mathrm{card}(S)$ can be substantially improved if one knows the number r of factors of $g(0, \ldots, 0, x)$ in $F[x]$. E.g. $2\delta(2^r + 2\delta)/\mathrm{card}(S)$ is a possible upper bound for the probability of failure.

As we have already pointed out after lemma 2, the condition $\partial f/\partial x_v \ne 0$ is automatically satisfied if $\mathrm{char}(F) = 0$. For characteristic $p > 0$ we can prove that theorem 2 is still correct without this assumption about the derivative of f provided that for each element $a \in F$ there exists an element $b \in F$ such that $b^p = a$. We need the following additional lemmas.

Lemma 4: Let F be a field of characteristic $p > 0$ and let $f(x) = a_n x^n + \cdots + a_0 \in F[x]$ be irreducible. Furthermore, assume that there exists an index i, $1 \le i \le n$, such that for all $b \in F$, $b^p \ne a_i$. Then $f(x^{p^\lambda})$ is irreducible in $F[x]$ for all integers $\lambda \ge 0$.

Proof: By induction on λ. For $\lambda = 0$, $f(x)$ is irreducible in $F[x]$ by assumption. Now assume that $f(x^{p^{\lambda-1}})$ is irreducible in $F[x]$, but suppose $f(x^{p^\lambda})$ is not. Then there exist polynomials $g, h \in F[x]$, g non-constant and irreducible, $\mathrm{GCD}(g, h) = 1$ such that

$$f(x^{p^\lambda}) = g(x)^k \; h(x), \quad k \ge 1 \tag{*}$$

and either $k \ge 2$ or $h \ne 1$. Differentiating (*) we get, since $\lambda \ge 1$,

$$k \, \frac{\mathrm{d}g}{\mathrm{d}x} \, h = -g \, \frac{\mathrm{d}h}{\mathrm{d}x}.$$

Hence, $\mathrm{d}h/\mathrm{d}x = 0$, which is equivalent to $h(x) = \bar{h}(x^p)$, $\bar{h} \in F[x]$, and either $k = p\,l$ or $\mathrm{d}g/\mathrm{d}x = 0$, each of which imply that $g(x)^k = \bar{g}(x^p)^{\bar{k}}$ $\bar{g} \in F[x]$ non-constant, $\bar{k} \geq 1$. Therefore, (*) can be rewritten, with $y = x^p$, as

$$f(y^{p^{\lambda-1}}) = \bar{g}(y)^{\bar{k}}\ \bar{h}(y).$$

By induction hypothesis we conclude that $\bar{h} = 1$ and $\bar{k} = 1$. Thus $h = 1$ and $k \geq 2$ and we must have $f(x^{p^{\lambda}}) = (g(x)^l)^p$ which means that each coefficient a_i is the p-th power of a coefficient of $g(x)^l$, contradicting our second assumption. □

Lemma 5: Let $f(x_1, \ldots, x_v) \in F[x_1, \ldots, x_v]$, F a field of characteristic $p > 0$, have total degree δ and assume that there exists an index i, $1 \leq i \leq v$, such that $\partial f/\partial x_i \neq 0$. Furthermore, let $S \subseteq F$ and let $c_2, \ldots, c_v$, $w_1, \ldots, w_v$ be random elements in S. Then the probability

$$P\left(\frac{\mathrm{d}f(x_1{+}w_1, c_2x_1{+}w_2, \ldots, c_vx_1{+}w_v)}{\mathrm{d}x_1} = 0\right) \leq \frac{\delta}{\mathrm{card}(S)}.$$

Proof: Write

$$f(x_1, \ldots, x_v) = \sum_{0 \leq |\underline{k}| \leq \delta} a_{\underline{k}} x_1^{k_1} \cdots x_v^{k_v}.$$

Then, by assumption there exists a $\underline{k}$ such that $a_{\underline{k}} \neq 0$ and $p \nmid k_i$. The coefficient of $x_1^{k_i}$ in $f(x_1 + y_1, z_2x_1 + y_2, \ldots, z_vx_1 + y_v) \in F[x_1, y_1, \ldots, y_v, z_2, \ldots, z_v]$ is

$$\gamma(y_1, \ldots, y_v, z_2, \ldots, z_v) = a_{\underline{k}}\ y_1^{k_1}\ y_2^{k_2} \cdots y_{i-1}^{k_{i-1}}\ z_i^{k_i}\ y_{i+1}^{k_{i+1}} \cdots y_v^{k_v} + \cdots$$

where the given monomial only occurs once since we can unambiguously deduce from the given exponents the term in the expansion it came from. Therefore $\gamma \neq 0$ with $\deg(\gamma) \leq \delta$. Thus, by lemma 1, $\gamma(w_1, \ldots, w_v, c_2, \ldots, c_v) = 0$ with at most the given probability, but this is obviously necessary for $\mathrm{d}f(x_1{+}w_1, \ldots, c_vx_1{+}w_v)/\mathrm{d}x_1 = 0$. □

We now formulate our irreducibility theorem in the most general way we shall prove here.

Theorem 3 (*Effective Hilbert Irreducibility Theorem*): Let $f(x_1, \ldots, x_v) \in F[x_1, \ldots, x_v]$, F a field, have total degree δ and be irreducible. If $\mathrm{char}(F) = p > 0$ we require that each coefficient of f in F possesses a p-th root in F. A sufficient condition for this to be true is that F be perfect. Let $S \subseteq F$ and let $c_2, \ldots, c_{v-1}$, $w_1, \ldots, w_{v-1}$ be random elements in S. Then the probability

$$\begin{aligned} &P(f(x_1 + w_1, c_2x_1 + w_2, \ldots, c_{v-1}x_1 + w_{v-1}, x_2) \\ &\quad \text{becomes reducible in } F[x_1, x_2]) \leq \frac{4\delta\, 2^{\delta}}{\mathrm{card}(S)}. \end{aligned}$$

Proof: If $\mathrm{char}(F) = 0$ or $\partial f/\partial x_v \neq 0$ then our theorem is identical to theorem 2. Therefore assume that $\mathrm{char}(F) = p > 0$ and that

$$f(x_1,\ldots,x_v) = \bar{f}(x_1,\ldots,x_{v-1},x_v^{p^\mu}),\ \ \mu \geq 1,$$

with $\bar{f}(x_1,\ldots, x_{v-1}, z) \in F[x_1,\ldots, x_{v-1}, z]$ and $\partial\bar{f}/\partial z \neq 0$ (i.e. μ is as large as possible). Since f is irreducible so must be $\bar{f}$ and we can apply theorem 2 to $\bar{f}$. Looking at the last inequality in the proof of theorem 2, randomly chosen $w_1,\ldots, w_{v-1}, c_2,\ldots, c_{v-1}$ from S keep $\bar{f}(x_1+w_1, c_2x_1+w_2,\ldots, c_{v-1}x_1+w_{v-1}, x_2)$ irreducible in $F[x_1, x_2]$ with probability at least $1 - (4\delta 2^\delta - 3d)/\mathrm{card}(S)$ where $d = \deg_{x_1,\ldots,x_{v-1}}(\bar{f}) = \deg_{x_1,\ldots,x_{v-1}}(f)$; note that $\deg(\bar{f}) \leq \delta$.

Now there must exist a coefficient $a_i(x_1,\ldots, x_{v-1})$ of $(x_v^{p^\mu})^i$ in f such that not all $\partial a_i/\partial x_j$, $1 \leq j \leq v-1$, vanish. Otherwise, by virtue of our assumption, f would be a p-th power of a polynomial, hence reducible. Let $w_1,\ldots, w_{v-1}, c_2,\ldots, c_{v-1}$ in addition to the constraints of theorem 2 also be such that, for

$$\bar{a}_i(x_1) = a_i(x_1+w_1, c_2x_1+w_2,\ldots,c_{v-1}x_1+w_{v-1}),$$

$d\bar{a}_i/dx_1 \neq 0$. Then

$$\hat{f}(x_1, x_2) = f(x_1+w_1, c_2x_1+w_2,\ldots,c_{v-1}x_1+w_{v-1}, x_2)$$

must be irreducible in $F[x_1, x_2]$. For, interpreting the evaluated polynomial corresponding to $\bar{f}$ as an element of $F(x_1)[x_2]$ it is clear that its coefficient $\bar{a}_i$ is not a p-th power. Hence lemma 4 applies and shows that $\hat{f}$ is irreducible in $F(x_1)[x_2]$. By the proof of theorem 2, $\hat{f}$ cannot possess a content in $F[x_1]$.

It remains to estimate with which probability the additional condition on the $w_1,\ldots, c_{v-1}$ is fulfilled. By lemma 5 this is true with probability at least $1 - d/\mathrm{card}(S)$, thus the overall rate of success is at least

$$1 - \left(\frac{4\delta 2^\delta - 3d}{\mathrm{card}(S)} + \frac{d}{\mathrm{card}(S)}\right) \geq 1 - \frac{4\delta 2^\delta}{\mathrm{card}(S)}. \quad \Box$$

We remark that one can generalize theorem 3 to arbitrary fields. Using von zur Gathen's (1985a) Lemma 4.2 we get a slightly smaller success probability $1 - 5d\, 2^d/\mathrm{card}(S)$ for these exceptional fields. We note, however, that the usual fields occurring in algebraic computation are perfect, such as fields of characteristic 0, finite fields, and algebraically closed fields, and therefore do not discuss the details of that generalization.

4. Probabilistic Irreducibility Testing

We now apply theorem 3 to construct a probabilistic irreducibility test for a sparse multivariate polynomial $f(x_1,\ldots, x_v) \in F[x_1,\ldots, x_v]$, F an arbitrary field (with the restriction stated in theorem 3 in case that $\mathrm{char}(F) > 0$). Our algorithm outputs ‘‘definitely irreducible’’ or ‘‘probably composite’’ or ‘‘failure’’ where the chance that the irreducibility of f is not recognized as such is less than a given constant $\varepsilon \ll 1$. The algorithm selects random elements in $S \subseteq F$ and calls an irreducibility test for polynomials in two or three variables, depending on the characteristic of F. Apart from the calls to these unspecified subroutines our algorithm works in polynomially many steps in $\deg(f)$ and $\text{monomials}(f)$, where $\text{monomials}(f)$ denotes the number of non-zero monomials in f.

If we furthermore specify $F = \mathbf{Q}$ or $\mathbf{Z}_p$, then our algorithm is also of polynomial complexity in the number of bits needed to encode the coefficients of f and $\log 1/\varepsilon$. In this case the required polynomial-time subroutines exist. (Cf. Kaltofen (1985a) for $F = \mathbf{Q}$ and von zur Gathen and Kaltofen (1985) for $F = \mathbf{Z}_p$. The latter algorithm is only a probabilistic one and may, with controllably small probability, return ‘‘failure’’.)

For $\text{char}(F) = 0$ our algorithm is quite simple:

Algorithm 1:
[Given an irreducible polynomial $f(x_1, \ldots, x_v) \in F[x_1, \ldots, x_v]$, $\text{char}(F) = 0$, this algorithm attempts to prove the irreducibility of f with a failure chance less than $\varepsilon \ll 1$:]

(R) [Random choices:] From a set $S \subseteq F$ with $\text{card}(S) \geq 4\deg(f)\,2^{\deg(f)}/\varepsilon$ select random elements $c_2, \ldots, c_{v-1}, w_1, \ldots, w_{v-1}$.

(I) [Irreducibility test:]
$\bar{f}(x_1, x_2) \leftarrow f(x_1+w_1, c_2x_1+w_2, \ldots, c_{v-1}x_1+w_{v-1}, x_2)$.
IF $\deg_{x_1}(\bar{f}) < \deg_{x_1}(f)$ THEN RETURN (‘‘failure’’). ELSE call an algorithm testing $\bar{f}(x_1, x_2)$ for irreducibility in $F[x_1, x_2]$. IF $\bar{f}$ is irreducible THEN RETURN ‘‘f is definitely irreducible’’ ELSE RETURN ‘‘f is probably composite’’. □

Complexity analysis for $F = \mathbf{Q}$*:* We first multiply by a common denominator of all rational coefficients of f. Therefore we may assume that $f \in \mathbf{Z}[x_1, \ldots, x_v]$. Now let $\delta = \deg(f)$ and choose S the interval $\{-2\delta 2^{\delta}/\varepsilon \leq s \leq 2\delta 2^{\delta}/\varepsilon\}$. We evaluate each monomial $b_{\underline{k}}\,\underline{x}^{\underline{k}}$ of f, $|\underline{k}| \leq \delta$, and then add up to get $\bar{f}$. It is easy to see that

$$g_{\underline{k}}(x_1, x_2) = b_{\underline{k}}\ (x_1+w_1)^{k_1}\ (c_2x_1+w_2)^{k_2}\cdots(c_{v-1}x_1+w_{v-1})^{k_{v-1}}\,x_2^{k_v}$$

can be computed in $O(\delta^2)$ integer operations. In fact, the coefficient of x_1^i in $g_{\underline{k}}$ is

$$b_{\underline{k}} \sum_{\substack{i_1+\cdots+i_{v-1}=i \\ 0\leq i_1\leq k_1,\ldots,0\leq i_{v-1}\leq k_{v-1}}} \binom{k_1}{i_1} \cdots \binom{k_{v-1}}{i_{v-1}}\ w_1^{k_1-i_1}\ c_2^{i_2}\ w_2^{k_2-i_2} \cdots c_{v-1}^{i_{v-1}}\ w_{v-1}^{k_{v-1}-i_{v-1}}$$

which is $O(2^{|\underline{k}|}\ (2\delta 2^{\delta}/\varepsilon)^{|\underline{k}|})$ in magnitude. Therefore $\log|g_{\underline{k}}| = O(\delta^2 + \delta\log 1/\varepsilon + \log|f|)$ and $\log|\bar{f}| = O(\log\mu + \log|g_{\underline{k}}|)$ where $\mu = \text{monomials}(f)$. To add up all $g_{\underline{k}}$ takes $O(\mu\,\delta^2)$ integer operations. In summary, algorithm 1 runs in $O(\mu\,\delta^2)$ integer operation with integers of

$$O(\delta^2 + \delta\log\frac{1}{\varepsilon} + \log|f| + \log\mu)$$

digits. The later is also a bound for $\log |\bar{f}|$. The algorithm needs $O(v\delta + v \log 1/\varepsilon)$ random bit choices. This analysis does not account for testing $\bar{f}(x_1, x_2)$ for irreducibility. We can call Kaltofen (1985a), Algorithm 2, but the cost of this call might be quite high, $O(\delta^{14} \log^3 |\bar{f}|)$, which most likely does not reflect the true behavior of that algorithm. However, the actual cost can be expected to grow quickly with δ. This is why we chose S dependent on ε, the wanted failure probability, and call the bivariate algorithm just once.

We now treat the case in which F has only finitely many elements. Algorithm 1 obviously may run into problems since the sufficiently large subset S of F may not exist. Our approach here is to work in $F^* = F[x_1]$. We now present the algorithm.

Algorithm 2:
[Given an irreducible polynomial $f(x_1, \ldots, x_v) \in F[x_1, \ldots, x_v]$, card$(F) < \infty$, this algorithm attempts to prove the irreducibility of f with a failure chance less than $\varepsilon \ll 1$:]

(C) [Check for content in $F^* = F[x_1]$:] Rewrite f to $f^*(x_2, \ldots, x_v) \in F^*[x_2, \ldots, x_v]$ and verify that all coefficients of f^* in F^* have no GCD in $F[x_1]$. Otherwise RETURN (''f is definitely composite'').

(R) [Random choices:] From a set $S \subseteq F^*$ with card$(S) \geq 4\deg(f^*)\, 2^{\deg(f^*)}/\varepsilon$ select random elements $c_3, \ldots, c_{v-1}, w_2, \ldots, w_{v-1}$.

(I) [Irreducibility test:]

$$\bar{f}(x_2, x_3) \leftarrow f^*(x_2 + w_2, c_3 x_2 + w_3, \ldots, c_{v-1} x_2 + w_{v-1}, x_3).$$

IF $\deg_{x_3}(\bar{f}) < \deg_{x_3}(f^*)$ THEN RETURN (''failure''). Compute the GCD of all coefficients of $\bar{f}$ in F^*, $g^*[x_1]$. Set $\hat{f}(x_1, x_2, x_3) \leftarrow \bar{f}(x_2, x_3)/g^*(x_1) \in F[x_1, x_2, x_3]$. Now call an algorithm testing $\hat{f}$ for irreducibility in $F[x_1, x_2, x_3]$. IF $\hat{f}$ is irreducible THEN RETURN (''f is definitely irreducible'') ELSE RETURN (''f is probably composite''). □

The correctness of this algorithm follows from Gauss' lemma stating that if a polynomial $h(x_1, \ldots, x_v) \in D[x_1, \ldots, x_v]$, D a unique factorization domain, is irreducible, it remains irreducible in QF$(D)[x_1, \ldots, x_v]$. We again select a concrete field F to carry out timing estimates.

Complexity analysis for $F = \mathbf{Z}_p$: Let $\delta = \deg(f^*)$ and choose

$$S = \{s(x_1) \mid s(x_1) \in F[x_1] \text{ and } \deg(s) \leq \left\lfloor \frac{(\delta+2)\log 2 + \log\delta - \log\varepsilon}{\log p} \right\rfloor \}.$$

Notice that card$(S) \geq 4\delta 2^\delta/\varepsilon$. Step (C) takes $O(\mu\delta^2)$ field operations in $\mathbf{Z}_p$, μ = monomials(f). Furthermore, $\bar{f}$ can be computed in $O(\mu\delta^2 \cdot \delta^2 (\frac{\delta - \log\varepsilon}{\log p})^2)$ where the second factor arises from computing powers of c_i and w_i. Also $\deg_{x_1}(\bar{f}) = O(\delta \frac{\delta - \log\varepsilon}{\log p})$ and

$\deg_{x_2,x_3}(\bar{f}) \leq \delta$. Hence the calculation of the GCD g^* costs $O(\delta^3 (\frac{\delta - \log\varepsilon}{\log p})^2)$ operations in $\mathbf{Z}_p$. Assuming that $\delta - \log\varepsilon \geq \log p$, algorithm 2 runs in

$$O(\mu\ \delta^4\ (\delta + \log\frac{1}{\varepsilon})^2)$$

binary steps. The algorithm needs $O(v\ \ (\delta - \log\varepsilon))$ random bit choices. Again, we do not account for testing $\hat{f}(x_1, x_2, x_3)$ for irreducibility. We can call the algorithm presented in von zur Gathen and Kaltofen (1985). That algorithm is also random and has a small probability of failure. Furthermore, its complexity in δ is quite high.

In this section we only dealt with irreducibility testing of sparse polynomials. Theorem 3 can, of course, be employed to produce sparse factorizations in the spirit of Zippel (1981) and von zur Gathen (1985b) (see also Kaltofen (1985b)). In Zippel (1981) the sparse Hensel lifting is started with $f(c_1, \ldots, c_{v-1}, x_1)$, $c_1, \ldots, c_{v-1} \in F$ whereas in von zur Gathen (1985b) the evaluation is to $f(x_1, x_2, c_3 x_1 + u_3 x_2 + w_3, \ldots, c_v x_1 + u_v x_2 + w_v)$, $c_i, u_i, w_i \in F$. Unfortunately, we have no effective Hilbert Irreducibility Theorem for evaluations in F and neither we nor von zur Gathen (1985b) choose evaluations in the coefficient domain. In order to use a unified Hensel procedure which always evaluates in F we could, however, view theorem 3 in the following way. Let the coefficient field of $f(x_1, \ldots, x_v)$ be $F(x_1)$ $(F(x_1, x_2)$ for char$(F) > 0)$. Then our algorithm must select random elements in this field which are linear in x_1 (x_2 for char$(D) > 0$).

5. Conclusion

Though we were able to prove a very effective version for the Hilbert Irreducibility Theorem in the case in which the coefficients came from a transcendental extension of the integers, the classical version with integral coefficients still defies such error estimates. Again the set of evaluation points mapping the irreducible multivariate polynomial into a reducible univariate one is of measure 0 (cf. Dörge (1926)). Although recent research has produced very concrete descriptions of integer point sets preserving polynomial irreducibility (cf. Fried (1974) and Sprindzhuk (1983)), the possibility that the first integer preserving irreducibility might be exponentially in size cannot be excluded yet. However, practical experience indicates that the classical theorem also provides an excellent, though not proven, irreducibility test.

Within the last two years since this paper has been written the Effective Hilbert Irreducibility Theorem presented here has been applied in two new settings. First, it is used to determining the factorization pattern of a multivariate polynomial defined by a straight-line program (cf. von zur Gathen (1985a) and Kaltofen (1985c)). Furthermore, it is used in the algorithm by Kaltofen (1985c) for factoring multivariate polynomials given by straight-line programs into sparse factors. In retrospect, the usage of linear substitutions also eliminates the so called ‘‘leading coefficient problem’’ during the Hensel lifting process and therefore appears to be superior to classical evaluation techniques.

Acknowledgement

I like to thank Joachim von zur Gathen for the many fruitful discussions we have had on this subject. Several remarks of the referee have also been helpful.

References

Berlekamp, E.R. (1970), Factoring Polynomials over Large Finite Fields, *Math. Comp.* **24**, 713-735.

Chistov, A.L., and Grigoryev, D.Y. (1982), Polynomial-Time Factoring of Multivariate Polynomials over a Global Field, Lomi preprint E-5-82, Leningrad 1982.

Dörge, K. (1929), Zum Hilbertschen Irreduzibilitätssatz, *Math. Ann.* **95**, 84-97.

Fried, M. (1974), On Hilbert's Irreducibility Theorem, *J. Number Theory* **6**, 211-231.

von zur Gathen, J. (1985a), Irreducibility of Multivariate Polynomials, *J. Comp. System Sci.*, to appear.

von zur Gathen, J. (1985b), Factoring Sparse Multivariate Polynomials, *J. Comp. System Sci.*, to appear.

von zur Gathen, J., and Kaltofen, E. (1985), Factoring Multivariate Polynomials Over Finite Fields, *Math. Comp.*, to appear.

Heintz, J., and Sieveking, M. (1981), Absolute Primality of Polynomials is Decidable in Random Polynomial Time in the Number of Variables, *in* ''Proc. 1981 Internat. Conf. Automata, Languages and Programming,'' Springer Lec. Notes Comp. Sci. **115**, 16-28.

Kaltofen, E. (1985a), Polynomial-Time Reductions from Multivariate to Bi- and Univariate Integral Polynomial Factorization, *SIAM J. Comp.* **14**, 469-489.

Kaltofen, E. (1985b), Sparse Hensel Lifting, *in* ''Proc. EUROCAL '85,'' Springer Lec. Notes Comp. Sci., to appear.

Kaltofen, E. (1985c), Computing with Polynomials Given by Straight-Line Programs II; Sparse Factorization, *in* ''Proc. 26th Symp. Foundations Comp. Sci.,'' IEEE Computer Society, to appear.

Landau, S. (1985), Factoring Polynomials over Algebraic Number Fields is in Polynomial Time, *SIAM J. Comp.* **14**, 184-195.

Lenstra, A. K., Lenstra, H. W., and Lovász, L. (1982), Factoring Polynomials with Rational Coefficients, *Math. Ann.* **261**, 515-534.

Schwartz, J.T. (1980), Fast Probabilistic Algorithms for Verification of Polynomial Identities, *J. ACM* **27**, 701-717.

Sprindzhuk, V. G. (1981), Diophantine Equations with Unknown Prime Numbers, *Proc. Steklov Institute of*

Mathematics **158**, 180-196, 1983 English translation 197-214.

Zippel, R. E. (1981), Newton’s Iteration and the Sparse Hensel Algorithm, *in* ‘‘Proc. 1981 ACM Symp. Symbolic Alg. Comp.’’, ACM, 68-72.