

A POLYNOMIAL REDUCTION FROM MULTIVARIATE TO
BIVARIATE INTEGRAL POLYNOMIAL FACTORIZATION.*

Erich Kaltofen
University of Delaware

Abstract

Given an arbitrary but fixed integer $r \geq 3$. We show that testing r -variate polynomials with integer coefficients for irreducibility is m -reducible in polynomial time of the total degree and the largest coefficient length to testing bivariate polynomials for irreducibility. Factoring r -variate polynomials into irreducibles is polynomial time Turing-reducible to completely factoring bivariate polynomials.

1. Introduction

Algorithms for factoring multivariate polynomials with integer coefficients have been studied extensively in the literature. One hundred years ago L. Kronecker introduced a reduction from multivariate to univariate factorization [KRON1882, p.11] which has since become a popular device in polynomial arithmetic. In 1969 H. Zassenhaus discovered the applicability of the Hensel lemma of p -adic analysis to the factorization problem whose multivariate counterpart has been used successfully in the past decade (cf. [MUSD75], [WANG78], [ZIPR81]). This method also reduces the problem to first factoring a univariate polynomial derived from the input polynomial by evaluating all but one variable at certain integers. However, the running time of both methods suffers from the fact that in rare cases an exponential number of factor candidates obtained from the univariate factorization may have to be tested to determine the true factors. It appears natural to ask

*This work has been partially supported by the National Science Foundation under Grant #MCS-7909158. This paper is taken in part from a thesis to be submitted in partial fulfillment for the degree of Ph.D. in the Department of Math. Sciences at Rensselaer Polytechnic Institute.

whether there exists any reduction which works in polynomial time of the size of the input.

Before we can state our result we need to clarify what we mean by input-size. We will assume that our input polynomials are densely encoded that is all coefficients including zeroes are listed. Hence the size of a polynomial with r variables, given that the absolutely largest coefficients has ℓ digits and the highest degree of any variable is n , is of order $O(\ell n^r)$.

Let r , the number of variables, be a fixed integer. Then testing r -variate integer polynomials for irreducibility is polynomially m -reducible to testing bivariate integer polynomials for irreducibility. Moreover determining all irreducible factors of r -variate integer polynomials is polynomially Turing-reducible to completely factoring bivariate integer polynomials.

We wish to mention that in [ADOD81] a similar reducibility was conjectured from univariate polynomials to integers. The reduction from bivariate to univariate polynomials must also remain an open problem. Furthermore, we remark that there is no known algorithm which factors univariate polynomials in polynomial time [KAMS81]. Our proof is based on Kronecker's reduction and the idea of using Puiseux series expansions for a certain version of the Hilbert irreducibility theorem [FRAW31]. We also have to estimate the coefficient growth of the used power series expansions.

We shall briefly outline the organization of this paper. For the sake of clarity we will present the proofs for the trivariate to bivariate reduction only. However, in section 5 we will briefly sketch how our methods generalize to the r -variate case. Section 2 establishes our notation and some well-known facts needed in our proofs. In section 3 we introduce a preliminary transformation on our input polynomials. The proofs of our main theorems are contained in section 4. Section 6 concludes this paper.

2. Notation and Mathematical Background

By Z we denote the integers, by Q the rationals and by $1/r Z$ those rationals whose denominator divides the integer r ; C denotes the complex numbers. If D is an integral domain, $D[u,v,x]$ denotes the ring of polynomials in

u , v , and x over D ; $\deg_u(f)$ denotes the highest degree of u in $f \in D[u,v,x]$, $\deg_{u,v}(f)$ the highest total degree of monomials in u and v in f , and $\deg(f) = \deg_{u,v,x}(f)$ the total degree of f . The coefficient of the highest power of x in f is referred to as the leading coefficient of f in x , $\ell c_x(f)$. We call f monic in x if $\ell c_x(f)$ is the unity of D . As is well-known, $D[u,v,x]$ is a unique factorization domain (UFD) provided that D is a UFD. In this case the content of $f \in D[u,v,x]$ in x , $\text{cont}_x(f)$, is the greatest common divisor (GCD) of all coefficients of $f(x)$ as elements in $D[u,v]$. The primitive part of f in x $\text{pp}_x(f) = 1/\text{cont}_x(f) f$ and we call f primitive in x if $f = \text{pp}_x(f)$. We also note that the total degree of any monomial in a factor of f is less than or equal to the total degree of that monomial in f . The infinity norm of $f \in Q[u,v,x]$, the maximum of the absolute values of the rational coefficients of f , will be denoted by $|f|$.

Let $f(x) = a_\ell x^\ell + a_{\ell-1} x^{\ell-1} + \dots + a_0$, $g(x) = b_m x^m + \dots + b_0$ with $a_i, b_j \in D[u,v]$. By $\text{Syl}_x(f,g)$ we denote the Sylvester matrix of f and g

$$\text{Syl}_x(f,g) = \begin{bmatrix} a_\ell & a_{\ell-1} & \dots & a_0 & & 0 \\ & a_\ell & a_{\ell-1} & \dots & a_0 & \\ 0 & & & & a_\ell & a_{\ell-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & & 0 \\ & b_m & b_{m-1} & \dots & b_0 & \\ 0 & & & & b_m & b_{m-1} & \dots & b_0 \end{bmatrix} \begin{matrix} \left. \begin{matrix} \text{---} \\ \text{---} \\ \text{---} \end{matrix} \right\} m \text{ rows} \\ \left. \begin{matrix} \text{---} \\ \text{---} \\ \text{---} \end{matrix} \right\} \ell \text{ rows} \end{matrix}$$

Its determinant is the resultant of f and g with respect to x and will be denoted by $\text{res}_x(f,g) = \det(\text{Syl}_x(f,g))$.

Lemma 1: Let f and g be given as above. Then $\deg_t(\text{res}_x(f,g)) \leq \ell \deg_t(g) + m \deg_t(f)$ for $t = u$ or v . $\square$

The next lemma establishes coefficient bounds for the factors of multivariate polynomials.

Lemma 2: Let $g_1, \dots, g_m \in C[u,v,x]$, let $f = g_1 \dots g_m$ and let $n = \deg_u(f) + \deg_v(f) + \deg_x(f)$. Then,

$$\prod_{i=1}^m |g_i| \leq e^n |f| \text{ with } e \approx 2.71828.$$

Proof: See [GELA60, pp.135-139]. $\square$

We now can bound the resultant of a factor and the cofactor of a polynomial in one variable.

Lemma 3: Let $f(x) = g(x) h(x)$ be a non-trivial factorization of $f \in C[x]$ of degree n . Then if M is any $(n-1)$ by $(n-1)$ submatrix of $\text{Syl}(g,h)$, its determinant satisfies

$$\det(M) \leq (\sqrt{n-1} \cdot 3^n |f|)^{n-1}.$$

Proof: By lemma 2 we know that each entry in M is bounded by $3^n |f|$. Hadamard's determinant

inequality then gives the bound. $\square$

In theorem 2 of section 4 we will need the algebraic closure of polynomial domains and we shall introduce the theory now. Let K be a field of characteristic 0, $\bar{K}$ its algebraic closure. By $K(t)^*$ we denote the fractional power series domain in t over $\bar{K}$, any element of which is of the form

$$\sum_{i=-k}^{\infty} a_i t^{i/q}$$

with $k, q \in \mathbb{Z}$, $q \geq 1$ and $a_i \in \bar{K}$ for $i \geq -k$. It is a classical result in complex analysis that every algebraic function admits a fractional power series expansion which converges in a neighborhood of zero. We state this theorem in its algebraic version as a lemma.

Lemma 4 (Puisseux's Theorem): $\bar{K}[t]$, the algebraic closure of $K[t]$, can be embedded into $K(t)^*$.

Proof: See [VdWA39, pp.50-54]. $\square$

We write $K(u,v)^*$ for $(K(u,v))^*$ and notice that $K(u,v)^*$ contains the algebraic closure of $K[u,v]$.

3. Initial Transformations

In this section we will review some well-known methods which will make the input polynomials monic and squarefree. We first notice that all arithmetic operations on $\mathbb{Z}[u,v,x]$ including substitutions and GCD computations take time polynomial in the input size (cf. [KNUD81, pp.399-416]). Let $f \in \mathbb{Z}[u,v,x]$ be our input polynomial which we want to factor or prove irreducible.

First we separate the content and primitive part of f by calculating the GCD of all coefficients of $f(x)$. We then squarefree decompose the primitive part of f , $\bar{f} = \text{pp}_x(f)$, by repeated multivariate GCD computations of the type $\text{GCD}(\bar{f}, \partial \bar{f} / \partial x)$ [YUND76]. We now proceed with factoring all squarefree factors of f . Let g be such a factor.

A standard technique makes g monic in x . Let $n = \deg_x(g)$, $c(u,v) = \ell c_x(g)$ and let

$$h(u,v,x) = c(u,v)^{n-1} g(u,v,x/c(u,v)).$$

Then h is monic in x and a complete factorization of $h = h_1 \dots h_m$ gives a complete factorization of g

$$g(u,v,x) = \prod_{i=1}^m \text{pp}_x(h_i(u,v,c(u,v) \cdot x))$$

[KNUD81, p.438, exercise 18].

Finally we translate the variables $u = \bar{u} + a$ and $v = \bar{v} + b$ with $a, b \in \mathbb{Z}$ such that

$$\bar{h}(\bar{u}, \bar{v}, x) = h(\bar{u} + a, \bar{v} + b, x)$$

is squarefree at $\bar{u} = 0$ and $\bar{v} = 0$. To show that we can find such integers a and b in polynomial time we prove the following lemma.

Lemma 5: Let $h(u,v,x) \in \mathbb{Z}[u,v,x]$ be squarefree (in x) and let $d = \max(\deg_u(h), \deg_v(h))$. Then there exist integers a and b with $0 \leq a, b \leq 2d^2 - d$ such that $h(a,b,x) \in \mathbb{Z}[x]$ is also squarefree.

Proof: Since h is squarefree its discriminant $D(u,v) = \text{res}_x(h, \partial h / \partial x) \neq 0$ [VdWA53, p.86]. By lemma 1 the highest degree of any variable is $2d^2-d$. If we write $D(u,v)$ as a polynomial in $(Z[u])[v]$ not all coefficients in $Z[u]$ can be zero. Since their degrees in u are bounded by $2d^2-d$, not all of the $2d^2-d+1$ numbers $0, 1, \dots, 2d^2-d$ can be roots of one particular non-vanishing coefficient. Therefore there exists an integer a with $0 \leq a \leq 2d^2-d$ and $D(a,v) \neq 0$. The same argument shows the existence of a proper b . $\square$

The above lemma shows that we at most have to test $(2 \deg(h))^2$ pairs of points a and b . Testing whether $h(a,b,x)$ is squarefree is again a GCD computation as mentioned above.

4. Main Theorem

In the next lemma and theorem the following predicate repeatedly appears under a summation sign and we shall therefore introduce a separate symbol for it, namely

$$\pi(i,j,s,t) \equiv 0 \leq s \leq i \text{ and } 0 \leq t \leq j \text{ and } 1 \leq s+t \leq i+j-1.$$

The following lemma estimates the size of a general version of Catalan numbers.

Lemma 6: Let $d_{01} = d_{10} = 1$ and let $d_{ij} = \sum_{\pi(i,j,s,t)} d_{st} d_{i-s,j-t}$ for $i \geq 0, j \geq 0, i+j \geq 2$. Then

$$d_{ij} = \frac{1}{i+j} \binom{2(i+j)-2}{i+j-1} \frac{(i+j)!}{i!j!} < 8^{(i+j)}$$

with $\binom{\alpha}{\beta}$ denoting the usual binomial coefficient.

Proof: Let $G(u,v) = \sum_{i+j \geq 1} d_{ij} u^i v^j$ be a generating function for d_{ij} . Then $G(u,v)^2 = G(u,v) - (u+v)$ and thus $G(u,v) = 1/2(1 - \sqrt{1-4(u+v)}) = \sum_{k=1}^{\infty} 1/k \binom{2k-2}{k-1} (u+v)^k$ which yields one formula. The estimate $\binom{\alpha}{\beta} < 2^\alpha$ then implies our inequality. $\square$

Our first theorem estimates the coefficient growth of a power series expansion for our transformed input polynomial.

Theorem 1: Let $f(u,v,x) \in Z[u,v,x]$ be monic of degree n in x such that $f_{00}(x) = f(0,0,x)$ is squarefree. Let $g_{00}(x) h_{00}(x) = f_{00}(x)$ be a non-trivial factorization of $f_{00}(x)$ in $Z[x]$ i.e.

$$g_{00}(x) \in Z[x] \text{ and } 1 \leq \deg(g_{00}) < n.$$

Then there exist unique polynomials $g_{ij}(x), h_{ij}(x)$ with $i \geq 0, j \geq 0, i+j \geq 1$ and $\deg(g_{ij}) < \deg(g_{00})$, $\deg(h_{ij}) < \deg(h_{00})$ such that

$$f(u,v,x) = \left(\sum_{i,j=0}^{\infty} g_{ij}(x) u^i v^j \right) \left(\sum_{i,j=0}^{\infty} h_{ij}(x) u^i v^j \right).$$

Furthermore, let $R = \text{res}(g_{00}, h_{00})$ and let T be an upper bound for any $(n-1)$ by $(n-1)$ subdeterminant of $\text{Syl}(g_{00}, h_{00})$ (see lemma 3). Let $N = \max(n^2, n|f|)$ and let d_{ij} be as defined in lemma 6.

Then for all $i \geq 0, j \geq 0, i+j \geq 1$

$$g_{ij}(x) \text{ and } h_{ij}(x) \in (1/R^{2(i+j)-1} Z)[x]$$

and both

$$|g_{ij}|, |h_{ij}| \leq d_{ij} (NT)^{2(i+j)-1}.$$

Proof: The existence of g_{ij} and h_{ij} follows from lemma 4 or from the Hensel lemma which we will also use to obtain our estimates. Let $f_{ij}(x)$ denote the coefficient of the monomial $u^i v^j$ in f as an element of $(Z[x])[u,v]$. Since f is monic in x , $\deg(f_{ij}) < n$ for all $i+j \geq 1$. Hence for all $i \geq 0, j \geq 0, i+j \geq 1$ the polynomials g_{ij}, h_{ij} are uniquely determined by the given degree bounds,

$$(1) \quad g_{00}(x) h_{ij}(x) + h_{00}(x) g_{ij}(x) = b_{ij}(x)$$

with $b_{01}(x) = f_{01}(x), b_{10}(x) = f_{10}(x)$ and for $i+j \geq 2$.

$$(2) \quad b_{ij}(x) = f_{ij}(x) - \sum_{\pi(i,j,s,t)} g_{st}(x) h_{i-s,j-t}(x).$$

Now let $C_{ij} = \max(|g_{ij}|, |h_{ij}|, |f|)$ and let $B_{ij} = |b_{ij}|$. Since $\deg(g_{st}) < \deg(g_{00})$ and $\deg(h_{i-s,j-t}) < \deg(h_{00})$ we can conclude that $|g_{st} h_{i-s,j-t}| \leq (n-1) |g_{st}| |h_{i-s,j-t}| \leq (n-1) C_{st} C_{i-s,j-t}$. Observing that any C_{st} is at least of size $|f|$ we obtain from (2)

$$(3) \quad B_{ij} \leq n \sum_{\pi(i,j,s,t)} C_{st} C_{i-s,j-t} \text{ for } i+j \geq 2.$$

If we solve (1) by undetermined coefficients for g_{ij} and h_{ij} we encounter $\text{Syl}(g_{00}, h_{00})$ as the coefficient matrix, namely

$$(4) \quad (\vec{g}_{ij}, \vec{h}_{ij}) \text{ Syl}(g_{00}, h_{00}) = \vec{b}_{ij} \text{ for } i+j \geq 1.$$

By $\vec{p}$ we mean the coefficient vector $(p_m, p_{m-1}, \dots, p_0)$ of the polynomial $p(x) =$

$p_m x^m + \dots + p_0$. Using Cramer's rule for (4) and the fact that $\det(\text{Syl}(g_{00}, h_{00})) = R$ is an integer not equal to zero (f_{00} is squarefree) we get the estimate

$$(5) \quad C_{ij} \leq \max(|f|, n B_{ij} T).$$

Our claims now follow by induction on $i+j$.

Case $i+j = 1$: Since $b_{01}, b_{10} \in Z[x]$, Cramer's rule applied to (4) yields $g_{01}, g_{10}, h_{01}, h_{10} \in (1/R Z)[x]$. Also $B_{01}, B_{10} \leq |f|$ and hence by (5) $C_{01}, C_{10} \leq n |f| T \leq NT = d_{01} NT = d_{10} NT$.

Case $i+j \geq 2$: Applying the hypothesis to (2) we obtain $b_{ij} \in (1/R^{2(i+j)-2} Z)[x]$. Again by Cramer's rule we conclude from (4) that $g_{ij}, h_{ij} \in (1/R^{2(i+j)-1} Z)[x]$. By the hypothesis we get from (3) that

$$\begin{aligned}
B_{ij} &\leq n \sum_{\pi(i,j,s,t)} C_{st} C_{i-s,j-t} \\
&\leq (n(NT))^{2(i+j)-2} \sum_{\pi(i,j,s,t)} d_{st} d_{i-s,j-t} \\
&= (n(NT))^{2(i+j)-2} d_{ij}.
\end{aligned}$$

By (5) we finally obtain

$$\begin{aligned}
C_{ij} &\leq \max(|f|, nB_{ij}, T) \leq d_{ij} n^{2/N(NT)^{2(i+j)-1}} \\
&\leq d_{ij} (NT)^{2(i+j)-1}. \quad \square
\end{aligned}$$

Our second theorem is the essence of our paper and states that if the above polynomial $f(u,v,x)$ is irreducible then for any integer exponent s the polynomial $f(u, cu^s, x)$ remains irreducible for almost all integers c . The difficulty is to show that c can be chosen polynomially large.

Theorem 2: Let $f(u,v,x) \in Z[u,v,x]$ be monic of degree n in x such that $f(0,0,x)$ is squarefree. Let $\bar{R}$ be the maximum of all $R = \text{res}(g_{00}, h_{00})$

derived from any non-trivial factorization $f(0,0,x) = g_{00}(x)h_{00}(x)$ in $Z[x]$ and let $\bar{T}$ be an upper bound of any $(n-1)$ by $(n-1)$ subdeterminant of all $\text{Syl}(g_{00}, h_{00})$. Furthermore assume that $f(u,v,x)$ is irreducible. Let $d = \deg_{u,v}(f)$.

Then for any given positive integer s and for any integer c with $|c| \geq 4sd \bar{R}^{4sd-1} 8^{2s^2d} (NT)^{4s^2d-1}$ $f(u, cu^s, x)$ is irreducible in $Z[u,x]$.

Proof: By lemma 4 and the subsequent remark the polynomial $g_{c,s}(u,x) = f(u, cu^s, x)$ has n roots in $Q(u)^*$ and $f(u,v,x)$ has n roots in $Q(u,v)^*$. Each of the roots of $g_{c,s}$ corresponds to a root of f with $v = cu^s$. Hence each factor of $g_{c,s}(u,x) \in Q(u)^*[x]$ corresponds to a factor of $f(u,v,x) \in Q(u,v)^*[x]$ with $v = cu^s$. We will show that for an integer c of the stated size no factor derived from f in such a way can be an integral polynomial dividing $g_{c,s}$. Our plan is the following:

We first show that any candidate factor $h(u,v,x)$ of $f(u,v,x) \in Q(u,v)^*[x]$ contains at least one monomial $b_{pqm} u^p v^q x^m$ with $b_{pqm} \neq 0$ and $sd < p+q \leq 2sd$. From it we get a monomial $t(c)u^{p+sq}x^m$ in $h(u, cu^s, x)$ where $t(c)$ is a non-zero polynomial in c . Since $\deg_u(g_{c,s}) \leq sd$ no polynomial factor of $g_{c,s}$ has a higher degree in u . By choosing c larger than the absolute value of any root of $t(c)$ we force $\deg_u(h(u, cu^s, x)) \geq p+sq > sd$ and hence $h(u, cu^s, x)$ cannot be a polynomial dividing $g_{c,s}(u,x)$. Theorem 1 will assist us to estimate the size of any root of $t(c)$.

Let $h(u,v,x) = \sum_{k=0}^l \sum_{i,j=0}^{\infty} b_{ijk} u^i v^j x^k$ be the product of l linear factors of $f(x)$ with coefficients in $Q(u,v)^*$ and let $\bar{h}(u,v,x) = \sum_{k=0}^{n-l} \sum_{i,j=0}^{\infty} \bar{b}_{ijk} u^i v^j x^k$ be its cofactor, i.e.

$f = h\bar{h}$. We first can assume that $h(0,0,x) \in Z[x]$. Otherwise $h(u, cu^s, x)$ could not be an integer polynomial at all. Now there must exist at least one b_{ijk} or $\bar{b}_{ijk}$ with $sd < i+j \leq 2sd$ and $b_{ijk} \neq 0$ or $\bar{b}_{ijk} \neq 0$. To see this assume the contrary.

Then

$$\begin{aligned}
&(\sum_{k=0}^l \sum_{i+j \leq sd} b_{ijk} u^i v^j x^k) \\
&(\sum_{k=0}^{n-l} \sum_{i+j \leq sd} \bar{b}_{ijk} u^i v^j x^k) = f(u,v,x)
\end{aligned}$$

since no monomial $\lambda u^i v^j x^k$ with $sd < i+j \leq 2sd$ in the left product could be canceled by higher terms in the product of the complete expansions h and $\bar{h}$. However, f was assumed to be irreducible.

Without loss of generality we now can assume the existence of p, q and m such that $b_{pqm} \neq 0$ with $sd < p+q \leq 2sd$. We collect all non-zero b_{ijm} with $i+sj = p+sq$ and select among them b_{yzm} with z maximal. Then the following inequalities are easily verified

$$\begin{aligned}
(1) \quad z &\leq y+z \leq 2sd \quad \text{and} \\
sd &< i+sj \leq 2s^2d \quad \text{for } i+sj = p+sq.
\end{aligned}$$

We now consider the coefficient $t(c)$ of $u^{p+sq}x^m$ in $h(u, cu^s, x)$, namely

$$t(c) = b_{yzm} c^z + \dots + b_{pqm} c^q + \dots + b_{p+sq,0,m}$$

It is well known that the absolute value of any root α of a polynomial $F(x) \in C[x]$ is bounded by

$$|\alpha| \leq 2 \deg(F) |F| / |lc(F)|.$$

By Theorem 1 with $g_{00}(x) = \sum_{k=0}^l b_{00k} x^k$ and

$h_{00}(x) = \sum_{k=0}^{n-l} \bar{b}_{00k} x^k$ it follows that $b_{yzm} \in 1/R^{2(y+z)-1} Z$. Since $b_{yzm} \neq 0$ we conclude from

(1) that $|1/b_{yzm}| \leq R^{4sd-1}$. Also from theorem 1 and lemma 6 we get $|b_{ijm}| \leq 8^{i+j} (NT)^{2(i+j)-1}$ and again by (1) it follows that $|b_{ijm}| \leq 8^{2s^2d} (NT)^{4s^2d-1}$ for $i+sj = p+sq$. Finally using (1) once more we obtain

$$\begin{aligned}
(2) \quad 2 \deg(t) |t| / |lc(t)| &\leq \\
4sd 8^{2s^2d} (NT)^{4s^2d-1} R^{4sd-1}
\end{aligned}$$

Thus for any integer c absolutely larger than the RHS of (2) we know that $t(c) \neq 0$ and therefore $h(u, cu^s, x)$ contains a non-zero monomial

$t(c)u^{p+sq}x^m$ and cannot be a polynomial factor of $g_{c,s}(u,x)$ as argued above. Our given bound then obviously works for any factor candidate h . $\square$

We shall provide a corollary to make theorem 2 more palatable.

Corollary: Let $f(u,v,x) \in Z[u,v,x]$ be monic in x , irreducible and such that $f(0,0,x)$ is squarefree. Let s be a given positive integer. Then there exists an integer bound $B(|f|, \deg(f), s)$ of length polynomial in $\log(|f|)$, $\deg(f)$ and s such that

for every integer c with $|c| \geq B(|f|, \deg(f), s)$ $f(u, cu^s, x)$ is irreducible in $Z[u, x]$. Moreover $B(|f|, \deg(f), s)$ can be chosen to grow monotonously with $|f|$, $\deg(f)$ and s .

Proof: Since all possible g_{00} and h_{00} (as defined in Theorem 2) are monic we can bound $R = \text{res}(g_{00}, h_{00}) \leq 2\bar{T}$. Since all monomial degrees are not larger than $D = \deg(f)$ we obtain the following bounds.

- (1) $\bar{T} \leq (\sqrt{D} 3^D |f|)^D$ by lemma 3,
- (2) $N \leq D^2 |f|$ by its definition in Theorem 1, and
- (3) $B(|f|, D, s) \leq 4sD (2\bar{T})^{4sD} 8^{2s^2 D} (N\bar{T})^{4s^2 D}$

by Theorem 2. The statement including monotonicity now immediately follows from (1)-(3). $\square$

We now state and prove our main result for the trivariate case.

Theorem 3: Let $f(u, v, x) \in Z[u, v, x]$. Then there is an algorithm which constructs a polynomial $g(y, x)$ in time polynomial in $\deg(f) \log(|f|)$ such that g is irreducible over the integers if and only if f is irreducible over the integers. Furthermore assume that we possess an "oracle" algorithm which splits any bivariate polynomial $h(y, x) \in Z[y, x]$ into irreducible integral factors in time polynomial in $\deg(f) \log(|f|)$. Then there is an algorithm using this oracle which completely factors f into irreducibles over the integers in time polynomial in $\deg(f) \log(|f|)$.

Proof: First we treat the irreducibility test. If after the initial transformations described in section 4 f turns out to be non-primitive or non-squarefree then f is composite and we can set $g(y, x)$ to any composite bivariate polynomial. Otherwise we can assume that f is monic in x and $f(0, 0, x)$ is squarefree. All there is not left to do is to compute an integer $c > B(|f|, \deg(f), 1)$ with B from the previous corollary and to set $g(y, x) = f(y, cy, x)$. If $f = f_1 f_2$ then $g(y, x) = f_1(y, cy, x) f_2(y, cy, x)$, while if f is irreducible then by our corollary so must be g .

The full factorization part requires Kronecker's trick. Again we first compute $\text{cont}_x(f)$ and the squarefree decomposition of $\text{pp}_x(f) = f_1^2 f_2^2 \dots f_t^t$. Since $\text{cont}_x(f)$ involves at most 2 variables our oracle can be called directly in order to factor it. We proceed to factor all f_i and note that $t < \deg_x(f)$ making only polynomially many applications of the following procedure necessary. Let g be derived from an f_i as at the end of section 4 such that g is monic and $g(0, 0, x)$ is squarefree. Let

$$D > \max(\deg_u(g), \deg_v(g))$$

and let G be the factor coefficient bound for g given in lemma 2. We now compute an integer $c > B(G, \deg(g), D)$ with B from our corollary and call the oracle with

$$h(y, x) = g(y, cy^D, x).$$

By S_D^{-1} we denote a modified inverse of the Kronecker reduction performed on the variables u and v only, taking also into account the multiplier c : S_D^{-1} is additive and if λy^{i+Dj} is a monomial with $\lambda \in Z[x]$, $i, j < D$ then $S_D^{-1}(\lambda y^{i+Dj}) = \lambda u^i v^j / c^j$. We now claim that if h_1 is a factor of h then $S_D^{-1}(h_1)$ divides g . Since the transformation S_D^{-1} can be executed in polynomial time a full factorization of h will yield one for g and applying our method for all f_i finishes our proof.

We finally show our claim. Assume $S_D^{-1}(h_1)$ does not divide g . There exists an irreducible factor g_1 of g such that h_1 divides $g_1(y, cy^D, x)$. But $|g_1| < G$ and $\deg(g_1) < \deg(g)$ hence $g_1(y, cy^D, x)$ remains irreducible by our corollary, in contradiction to its divisibility by h_1 . $\square$

5. The r-Variate Case

A complete proof for the general case will appear in [KALE82] but the ideas are very similar to the trivariate case. Lemma 6 and Theorem 1 generalize without difficulty. Theorem 2 and its corollary can be generalized as follows. If $f(u_1, \dots, u_r, x) \in Z[u_1, \dots, u_r, x]$ is monic in x , irreducible and such that $f(0, \dots, 0, x)$ is squarefree then there exists a bound $B(|f|, \deg(f), s)$ of length polynomial in $\log(|f|)$, $\deg(f)$ and s such that $f(u_1, cu_1^s, u_3, \dots, u_r, x)$ remains irreducible in $Z[u_1, u_3, \dots, x]$ for integers c with $|c| \geq B(|f|, \deg(f), s)$. The proof follows the main line of the proofs for Theorem 2 and its corollary with but one complication. The generalization of the main theorem then is shown by a simple induction on r . Notice that our reduction can be viewed as to factoring (after the initial transformations) a bivariate polynomial

$$f(x_1, c_1 x_1^D, c_2 x_1^{D^2}, \dots, c_{r-2} x_1^{D^{r-2}}, x_r)$$

with suitably large integers $c_1, \dots, c_{r-2}$ and D larger than any single degree of f . This reduction appears to be a hybrid of Kronecker's device and the evaluation process.

6. Conclusion

An effective version of Hilbert's irreducibility theorem together with Kronecker's idea lead to our result. Similar approaches seem not to work for the reduction from bivariate to univariate factorization. The difficulties which arise are twofold. First there seems to be no effective way to compute an evaluation point $t_0 \in Z$ for an irreducible polynomial $f(t, x) \in Z[t, x]$ such that $f(t_0, x)$ remains irreducible in $Z[x]$. We conjecture that such a point of length polynomial in $\deg(f) \log(|f|)$ must exist yielding at least a succinct certificate for f . On the other hand substituting cx^s for t into a root

$\alpha(t) \in \mathbb{Q}(t)^*$ of $f(t, x)$ maps the corresponding linear factor $x - \alpha(t)$ into a series domain in x whose factorization properties are unclear. As to the author's knowledge these difficulties are yet to be overcome.

Acknowledgement: The problem of polynomial time reductions was suggested to the author by Prof. George Collins. The author also wishes to thank Prof. Bobby Caviness for his encouragement to pursue this approach.

REFERENCES

- [ADOD81] Adleman, L. E., and Odlyzko, A. M., "Irreducibility testing and factorization of polynomials," in Proc. 22nd Symp. on Foundations of Comp. Sci., IEEE, Los Angeles 1981, 409-418.
- [FRAW31] Franz, W., "Untersuchungen zum Hilbertschen Irreduzibilitätssatz," Math. Zeitschrift 33 (1931), 275-293.
- [GELA60] Gelfond, A. O., Transcendental and Algebraic Numbers, Dover Publ., N.Y. 1960.
- [KAMS81] Kaltofen, E., Musser, D. R., Saunders, B. D., "A generalized class of polynomials that are hard to factor," in [WANG81].
- [KALE82] Kaltofen, E., On the Complexity of Factoring Polynomials with Integer Coefficients, Ph.D. Thesis, Rensselaer Polytechnic Institute, in preparation.
- [KNUD81] Knuth, D. E., The Art of Programming, vol. 2, 2nd ed., Addison-Wesley, Reading, MA 1981.
- [KRON1882] Kronecker, L., "Grundzüge einer arithmetischen Theorie der algebraischen Größen," J. f. reine und angew. Math. 92 (1882), 1-122.
- [MUSD75] Musser, D. R., "Multivariate polynomial factorization," J.ACM 22 (1975), 291-308.
- [VdWA39] van der Waerden, B. L., Einführung in die algebraische Geometrie, Springer Verlag, Berlin 1939.
- [VdWA53] van der Waerden, B. L., Modern Algebra, vol. 1, trans. by F. Blum, Ungar Publ., N.Y. 1953.
- [WANG78] Wang, P. S., "An improved multivariate polynomial factoring algorithm," Math. Comp. 32 (1978), 1215-1231.
- [WANG81] Wang, P. S. (ed.), Proc. of the 1981 ACM Symp. on Symbolic and Algebraic Comp., ACM Baltimore, MD 1981.
- [YUND76] Yun, D. Y. Y., "On squarefree decomposition algorithms," in R. Jenks (ed.), Proc. 1976 ACM Symp. on Symbolic and Algebraic Comp., ACM, Baltimore, MD 1976, 26-35.
- [ZIPR81] Zippel, R. E., "Newton's iteration and the sparse Hensel algorithm," in [WANG81], 68-72.

ERRATA

p. 262, Lemma 5:

$$d = \max(\deg_u(h), \deg_v(h), \deg_x(h))$$

p. 263, (4):

$$(\vec{h}_{ij}, \vec{g}_{ij}) \text{ Syl}(g_{00}, h_{00}) = \vec{b}_{ij}$$

p. 264, Second column:

A more accurate bound for α is

$$|\alpha| \leq 2 \lceil F / \log(F) \rceil$$

and hence one can remove the factor 2nd from the bound of Theorem 2.

p. 265, Theorem 3, line 9:

$$\deg(h) \log(|h|)$$

p. 266, References:

Adleman, L., M.

p. 265, first column, line 3
monotonically

p. 264, second column, line 8
 $\vec{b}_{ijk}$