SIAM J COMPUT.
Vol. 14, No. 2, May 1985

015

# POLYNOMIAL-TIME REDUCTIONS FROM MULTIVARIATE TO BI- AND UNIVARIATE INTEGRAL POLYNOMIAL FACTORIZATION*

ERICH KALTOFEN†

**Abstract.** Consider a polynomial $f$ with an arbitrary but fixed number of variables and with integral coefficients. We present an algorithm which reduces the problem of finding the irreducible factors of $f$ in polynomial-time in the total degree of $f$ and the coefficient lengths of $f$ to factoring a univariate integral polynomial. Together with A. Lenstra's, H. Lenstra's and L. Lovász' polynomial-time factorization algorithm for univariate integral polynomials [Math. Ann., 261 (1982), pp. 515–534] this algorithm implies the following theorem. Factoring an integral polynomial with a fixed number of variables into irreducibles, except for the constant factors, can be accomplished in deterministic polynomial-time in the total degree and the size of its coefficients. Our algorithm can be generalized to factoring multivariate polynomials with coefficients in algebraic number fields and finite fields in polynomial-time. We also present a different algorithm, based on an effective version of a Hilbert Irreducibility Theorem, which polynomial-time reduces testing multivariate polynomials for irreducibility to testing bivariate integral polynomials for irreduciblity.

**Key words.** polynomial factorization, polynomial-time complexity, algorithm analysis, Hensel lemma, Hilbert irreducibility theorem

## 1. Introduction.

Both the classical Kronecker algorithm [17, p. 10] (see also van der Waerden [28, pp. 136–137]) and the modern multivariate Hensel algorithm (cf. Musser [26], Wang [29], Zippel [35]) solve the problem of factoring multivariate polynomials with integral coefficients by reduction to factoring univariate integral polynomials and reconstructing the multivariate factors from the univariate ones. However, as we will see in § 3, the running time of both methods suffers from the fact that, in rare cases, a number of factor candidates obtained from the univariate factorization which is exponential in the input degree may have to be tried to determine the true multivariate factors. In this paper we will present a new algorithm which does not require exponential-time in its worst case. But before we can state our result precisely, 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 zeros are listed. Hence, the size of a polynomial with $v$ variables, given that the absolutely largest coefficient has $l$ digits and the highest degree of any variable is $n$, is of order $O(l(n+1)^v)$.

Let $v$, the number of variables, be a fixed integer. We will show that the problem of determining all irreducible factors of $v$-variate polynomials is polynomial-time (Turing-, Cook-) reducible to completely factoring univariate polynomials. Recently, A. Lenstra, H. Lenstra, and L. Lovász [22] have shown that factoring univariate rational polynomials is achievable in polynomial-time. Therefore, our result implies the following theorem. Factoring an integral polynomial with a fixed number of variables into irreducibles, except for the constant factors, can be accomplished in deterministic polynomial time in the total degree and the size of its coefficients. Our algorithm is a multivariate version of an algorithm due to H. Zassenhaus [34], which, instead of leading to an integer linear programming problem, as is the case for Zassenhaus' algorithm, leads to a system of linear equations for the coefficients of an irreducible multivariate factor.

* Received by the editors March 15, 1983, and in revised form April 9, 1984. This work was partially supported by the National Science Foundation under grant MCS-7909158 and by the Department of Energy, under grant DE-AS02-ER7602075.

† Department of Computer Science, University of Toronto, Toronto, Ontario M5S 1A4, Canada. Current address: Department of Mathematical Sciences, Rensselaer Polytechnic Institute, Troy, New York 12181.

In Kaltofen [12] we have already established a polynomial-time reduction from multivariate to bivariate polynomial factorization. However, our new algorithm is less complex. On the other hand, the results in Kaltofen [12] imply a polynomial-time (m-, Karp-) reduction for irreducibility testing, which our new algorithm does not provide. This older algorithm (cf. § 7) is based on an effective version of a Hilbert Irreducibility Theorem [11] (see also Franz [5]), an idea which since has been used successfully in von zur Gathen [7] to construct a probabilistic algorithm for factoring sparse multivariate polynomials with a growing number of variables, and in Chistov and Grigoryev [3] to provide another polynomial-time reduction from bivariate to univariate integral polynomial factorization.

If one does not fix the number of variables, our definition of input size may not be appropriate since the input size then grows exponentially with the number of variables. Although our algorithm remains polynomial in the expression $l(n+1)^v$, our size measure only applies to dense inputs and for sparse polynomials our algorithm is of exponential complexity in the number of variables.[1] Unfortunately, in the sparse case little is known about even the space complexity of the answer under these conditions. In § 8 open problem 1 corresponds to this question.

The question arises whether our algorithm is of practical importance. Unlike in the univariate case, in the multivariate Hensel algorithm the factors of the reduced univariate polynomial are almost always the true images of the multivariate factors, in which case no exponential running time occurs. This empirical observation can be explained by a distributive version of the Hilbert Irreducibility Theorem (cf. § 3) but there seems to be no known guarantee that one can always avoid bad reductions in polynomial-time. However, we like to point out that so far we know of no class of polynomials for which our polynomial-time algorithm could perform better than the standard multivariate Hensel algorithm. In this connection we state open problem 2 in § 8.

In this paper we only consider the problem of multivariate polynomial factorization with integral coefficients. However, the presented algorithms can be generalized to coefficient domains such as algebraic extensions of the rationals as well as finite fields. Besides outlining the necessary ideas in § 8 we refer to the papers by Chistov and Grigoryev [3], Landau [19], von zur Gathen and Kaltofen [8], and Lenstra [20] and [21].

We shall briefly outline the organization of this paper. Section 2 establishes our notation and some well-known facts about polynomials. Exponentially bad cases for both the Kronecker and the multivariate Hensel algorithm are then constructed in § 3. In § 4 we introduce some well-known preliminary transformations on our input polynomials and also establish that these transformations are polynomial-time reductions. The main algorithm is presented in § 5 including the necessary arguments for its correctness. Its complexity is analyzed in § 6. In particular we show that the size of all intermediately computed integers stays within polynomial bounds. An effective version of the Hilbert Irreducibility Theorem and its applications to the factorization problem are discussed in § 7. We conclude in § 8 by raising 3 open problems.

**2. Notation.** By $\mathbf{Z}$ we denote the set of the integers, by $\mathbf{Q}$ the set of the rational numbers and by $\mathbf{C}$ the set of the complex numbers. $\mathbf{Z}_p$ denotes the set of the residues modulo a prime number $p$. If $D$ is an integral domain, $D[x_1, \cdots, x_v]$ denotes the set of polynomials in $x_1, \cdots, x_v$ over $D$, $D(x_1, \cdots, x_v)$ its field of quotients; $\deg_{x_1}(f)$ denotes the highest degree of $x_1$ in $f \in D[x_1, \cdots, x_v]$, $\deg_{x_1,x_2}(f)$ the highest total

[1] Our algorithm remains even polynomial in some slightly sharper input size measures such as $l(d_1+1)\cdots(d_v+1)$ where $d_i$ is the degree of the $i$th variable.

degree of monomials in $x_1$ and $x_2$ in $f$, and $\deg(f) = \deg_{x_1,\cdots,x_v}(f)$ the total degree of $f$. Thus, $\deg(f)$ is the maximum of all exponent sums of monomials in $x_1, \cdots, x_v$ with nonzero coefficients in $f$. 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 $\mathrm{ldcf}_{x_v}(f)$. Notice that $\mathrm{ldcf}_{x_v}(f) \in D[x_1, \cdots, x_{v-1}]$. We call $f$ monic in $x_v$ if $\mathrm{ldcf}_{x_v}(f)$ is the unity of $D$. As is well known, $D[x_1, \cdots, x_v]$ is a unique factorization domain (UFD) provided that $D$ is a UFD. In this case the content of $f \in D[x_1, \cdots, x_v]$ in $x_v$, $\mathrm{cont}_{x_v}(f)$, is the greatest common divisor (GCD) of all coefficients of $f(x_v)$ as elements in $D[x_1, \cdots, x_{v-1}]$. Notice again that $\mathrm{cont}_{x_v}(f) \in D[x_1, \cdots, x_{v-1}]$. 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 $f$ is less than or equal to the total degree of $f$. The infinity norm of $f \in \mathbf{C}[x_1, \cdots, x_v]$, the maximum of the absolute values of the complex coefficients of $f$, will be denoted by $|f|$. The square root of the sum of squares of the absolute values 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 $a_i, b_j \in D[x_1, \cdots, x_{v-1}]$. By $\mathrm{Syl}_{x_v}(f, g)$ we denote the Sylvester matrix of $f$ and $g$,

$$\begin{bmatrix}
a_l & a_{l-1} & & & \cdots & & a_1 & a_0 & & \\
 & a_l & a_{l-1} & & \cdots & & a_2 & a_1 & a_0 & \\
 & & \ddots & \ddots & & & & & & \ddots \\
 & & & a_l & a_{l-1} & \cdots & a_m & & \cdots & a_0 \\
b_m & b_{m-1} & & b_1 & b_0 & & & & & \\
 & b_m & b_{m-1} & & & b_0 & & & & \\
 & & & \ddots & & & \ddots & & & \\
 & & & \ddots & & & & & & \\
 & & & & & & b_m & b_{m-1} & \cdots & b_0
\end{bmatrix}$$

where the empty entries are assumed to be 0 (there are $m$ rows with coefficients of $f$ and $l$ rows with coefficients of $g$ and the matrix has $l+m$ columns). Its determinant is the resultant of $f$ and $g$ with respect to $x_v$ and will be denoted by

$$\mathrm{res}_{x_v}(f, g) = \det(\mathrm{Syl}_{x_v}(f, g)).$$

In order to be able to manipulate with monomials in a short way we adopt the following vector notation: $\underset{\sim}{k} \equiv (k_1, \cdots, k_v)$, $\underset{\sim}{0} \equiv (0, \cdots, 0)$, $y^{\underset{\sim}{k}} \equiv y_1^{k_1} \cdots y_v^{k_v}$, $\underset{\sim}{k} \pm \underset{\sim}{l} \equiv (k_1 \pm l_1, \cdots, k_v \pm l_v)$, $\underset{\sim}{k} \leqq \underset{\sim}{l}$ if, for all $i$, $k_i \leqq l_i$ and finally $|\underset{\sim}{k}| \equiv k_1 + \cdots + k_v$, if $\underset{\sim}{k} \geqq \underset{\sim}{0}$, and $-\infty$ otherwise. By $\binom{n}{m}$ we denote the binomial coefficient $n!/(m!(n-m)!)$.

**3. Exponential cases for the Kronecker and Hensel algorithms.** We only consider bivariate polynomials though the constructions easily generalize. First, we discuss some exponential cases for the Kronecker algorithm. This algorithm transforms the bivariate polynomial $f(z, x)$ into $\bar{f}(y) = f(y^d, y)$, $d = \max(\deg_z(f), \deg_x(f)) + 1$. Since the

degree in $z$ or $x$ of any factor $g(z, x)$ of $f(z, x)$ is less than $d$, $\bar{g}(y) = g(y^d, y)$, which is a factor of $\bar{f}(y)$, can be used to retrieve $g(z, x)$ in a quick and unambiguous way. Kronecker's algorithm proceeds in transforming all univariate factors of $\bar{f}(y)$ back to bivariate factor candidates for $f$ and then tests whether any candidate is a true factor. However, it clearly requires time exponential in the degree of $f$ in the case where $f$ is irreducible, but $\bar{f}$ splits into linear factors. It is easy to construct such $f$'s, as we do below, by working backward from $\bar{f}(y)$.

*Example* 1.

$$\bar{f}(y) = (y-4)(y-3)(y-2)(y-1)(y+1)(y+2)(y+3)(y+4)$$
$$= y^8 - 30y^6 + 273y^4 - 820y^2 + 576.$$

Set $d = 3$: $f_1(z, x) = z^2x^2 - 30z^2 + 273xz - 820x^2 + 576$ which is irreducible. Kronecker's algorithm has to refute 127 factor candidates to determine irreducibility of $f_1$.

Set $d = 5$: $f_2(z, x) = x^3z - 30xz + 273x^4 - 820x^2 + 576$ which is irreducible because $\deg_z(f) = 1$. This condition can always be enforced by choosing $d$ large enough and yields exponential cases of arbitrarily high degree.

*Example* 2. Let $n = (\prod_{i=2}^{k} p_i) - 2$ with $p_i$ the $i$th prime number. Let $f_3(z, x) = x^n - z^2$, which is irreducible since $n$ is odd. We obtain $\bar{f}_3(y) = y^n(1 - y^{n+2})$ where $1 - y^{n+2}$ factors into $2^{k-1}$ cyclotomic polynomials (cf. van der Waerden [28, p. 113]). Since $n$ is of order $O(e^{k\log(k)})$ (cf. Hardy and Wright [10, § 22.2]) the number of possible factor candidates cannot be polynomial in $n$.

The abundance of univariate factors usually disappears as soon as we choose a slightly different evaluation. For example,

$$f_1(3x^3, x) = 9x^8 - 270x^6 + 819x^4 - 820x^2 + 576$$

and

$$f_2(2x^5, x) = 2x^8 - 60x^6 + 273x^4 - 820x^2 + 576$$

are both irreducible. In Kaltofen [12] we have used a similar evaluation for polynomials with three variables which resulted in a deterministic reduction to bivariate factorization. There we also conjectured that it is highly probable that substituting $2x^d$ or $3x^d$ for $z$ in $f(z, x)$ already preserves the irreducibility of $f$. However, to prove that a multiplier of polynomial length definitely works seems difficult, and we have only succeeded in showing this for the multivariate to bivariate reduction (cf. § 7, Theorem 3).

In order to give exponentially bad inputs for the multivariate Hensel algorithm we need an irreducible polynomial $f(y_1, \cdots, y_v, x)$ such that $f(0, \cdots, 0, x)$ has all linear factors. Such a polynomial is quite easy to obtain and the following example demonstrates the construction of a polynomial which has all linear factors for various evaluation points.

*Example* 3.3. Let $f(y, x)$ have $\deg_y(f) \leqq 3$ and

$$f(-1, x) = (x-2)(x-1)(x+1)(x+2) = x^4 - 5x^2 + 4,$$
$$f(0, x) = (x-1)x(x+1)(x+2) = x^4 + 2x^3 - x^2 - 2x,$$
$$f(1, x) = (x-2)(x-1)x(x+1) = x^4 - 2x^3 - x^2 + 2x,$$

and $f(2, x) = x^4 + 2$. By interpolation $f(y, x) \in \mathbf{Q}[y, x]$ is determined uniquely, namely

$$f(y, x) = x^4 + (2y^3 - 3y^2 - 3y + 2)x^3 + (\tfrac{5}{6}y^3 - 2y^2 + \tfrac{7}{6}y - 1)x^2 + (-2y^3 + 3y^2 + 3y - 2)x - \tfrac{1}{3}y^3 + 2y^2 - \tfrac{5}{3}y.$$

We can also remove the rational denominators, namely

$$\bar{f}(y, x) = 6^4 f\left(y, \frac{x}{6}\right) = x^4 + (12y^3 - 18y^2 - 18y + 12)x^3 + (30y^3 - 72y^2 + 42y - 36)x^2 + (-432y^3 + 648y^2 + 648y - 432)x - 432y^3 + 2592y^2 - 2160y.$$

Since $f(2, x)$ is irreducible, so is $\bar{f}(y, x)$, but

$$\bar{f}(-1, x) = (x - 12)(x - 6)(x + 6)(x + 12),$$
$$\bar{f}(0, x) = (x - 6)x(x + 6)(x + 12),$$
$$\bar{f}(1, x) = (x - 12)(x - 6)x(x + 6).$$

The above construction obviously generalizes for arbitrarily high degrees but the number of unlucky evaluation points (i.e. those integers $b$ for which $f(b, x)$ splits into linear factors) seems bounded by the degree in $y$. The classical Hilbert irreducibility theorem states that for any irreducible polynomial $f(y, x) \in \mathbf{Z}[y, x]$ there exists an integer $b$ such that $f(b, x)$ remains irreducible. It can be shown that the ratio of unlucky points to the size of the interval, from which the points are taken, tends to zero as the size of the interval goes to infinity (cf. Dörge [4]). The reader is referred to Kaltofen [14, Appendix B] for a short bibliography on the Hilbert Irreducibility Theorem. Unfortunately, we do not understand the distribution of unlucky evaluation points of small size. Open problem 2 in § 8 refers to this question.

**4. Initial transformations.** In this section we present an algorithm which transforms the problem of factoring the polynomial $\bar{f}(z_1, \cdots, z_v, x)$ to factoring a polynomial $f(y_1, \cdots, y_v, x)$ such that $f$ is monic in $x$, $f(0, \cdots, 0, x)$ is squarefree, i.e. each of its irreducible polynomial factors occurs with multiplicity 1, and both $\deg(f)$ and $\log(|f|)$ are polynomially bounded in $\deg(\bar{f})$ and $\log(|\bar{f}|)$. For simplicity we only consider finding a single irreducible factor of $\bar{f}$. In Lemma 2 we will state a uniform coefficient bound for all possible factors of $\bar{f}$ which is of polynomial size in $\deg(\bar{f})$ and $\log(|\bar{f}|)$. Therefore, in order to obtain the complete factorization of $\bar{f}$ into irreducible factors in polynomial-time we can apply our algorithm recursively to the co-factor of the irreducible factor.

We wish to emphasize that this version of our algorithm can be improved significantly, e.g. by resolving the recursion mentioned above. However, here we are most interested in the theoretical result, namely that the algorithm works in polynomial-time. For this reason we also allow ourselves to present rather crude upper bounds in our complexity analysis. We also do not consider the influence which the underlying data structure used to represent multivariate polynomials could have on our algorithm performance. Furthermore, we will formulate the asymptotic complexity as a function in the total degree rather than the maximum degree of individual variables. Since the number of variables is fixed, both notions for the degree are codominant.

The following algorithm computes a squarefree factor of the primitive part of the input polynomial. It then applies two classical transformations to this squarefree factor

to make the polynomial monic and squarefree also when evaluated at 0 for the minor variables.

ALGORITHM 1

[Given $\bar{f}(z_1, \cdots, z_v, x) \in \mathbf{Z}[z_1, \cdots, z_v, x]$, this algorithm constructs an irreducible factor $\bar{g}\ (z_1, \cdots, z_v, x) \in \mathbf{Z}[z_1, \cdots, z_v, x]$ of $\bar{f}$ by preconditioning $\bar{f}$ and calling Algorithm 2.]

**(I)** [Test for univariate case:]
IF cont $(\bar{f})$ or $\mathrm{pp}(\bar{f})$ is univariate THEN factor it by a univariate factorization algorithm and return one irreducible factor, ELSE perform steps (S) through (E2).

**(S)** Determine a primitive squarefree factor $\bar{s}(z_1, \cdots, z_v, x)$ of $\bar{f}$ by a squarefree decomposition algorithm such as Yun's algorithm [32] or Wang and Trager's algorithm [30].

**(M)** [Transform $\bar{s}$ into a polynomial $s$ monic in $x$:] $n \leftarrow \deg_x(\bar{s})$;

$$c(z_1, \cdots, z_v) \leftarrow \mathrm{ldcf}_x(\bar{s});$$

$$s(z_1, \cdots, z_v, x) \leftarrow c(z_1, \cdots, z_v)^{n-1} \bar{s}\left(z_1, \cdots, z_v, \frac{x}{c(z_1, \cdots, z_v)}\right).$$

[Notice that $s$ is monic in $x$, an irreducible factor of which can be back-transformed to an irreducible factor of $\bar{s}$ (see step (E2)).]

**(T)** [Find good integral evaluation points $w_1, \cdots, w_v$ such that $s(w_1, \cdots, w_v, x)$ is squarefree.]
FOR ALL integers $w_i$ with $|w_i| \leqq \lceil (2n-1)/2 \deg_{z_i}(s) \rceil$, $1 \leqq i \leqq v$, DO
Test whether $s(w_1, \cdots, w_v, x)$ is squarefree. If so, exit loop.

$$f(y_1, \cdots, y_v, x) \leftarrow s(y_1 + w_1, \cdots, y_v + w_v, x).$$

**(R)** Call Algorithm 2 given below to find an irreducible factor $g(y_1, \cdots, y_v, x)$ of $f(y_1, \cdots, y_v, x)$.

**(E)** [Recover a possibly nonmonic factor $\bar{g}(z_1, \cdots, z_v, x)$ of $\bar{f}(z_1, \cdots, z_v, x)$.]

**(E1)** $g(z_1, \cdots, z_v, x) \leftarrow g(z_1 - w_1, \cdots, z_v - w_v, x)$.

**(E2)** $\bar{g}(z_1, \cdots, z_v, x) \leftarrow \mathrm{pp}_x(g(z_1, \cdots, z_v, c(z_1, \cdots, z_v)x))$. □

We shall first prove the correctness of the above algorithm. Obviously, if $g(y_1, \cdots, y_v, x)$ divides $f$ then $g(z_1, \cdots, z_v, x)$ divides $s(z_1, \cdots, z_v, x)$. The proof for the correctness of the transformations in the steps (M) and (E2) is quite easy and can be found in Knuth [16, p. 438, Exercise 18]. We first must show that step (T) will yield good evaluation points.

LEMMA 1. *Let $s(z_1, \cdots, z_v, x) \in \mathbf{Z}[z_1, \cdots, z_v, x]$ be monic of degree $n$ in $x$ and squarefree. Then there exist integers $w_i$ with $|w_i| \leqq \lceil (2n-1)/2 \deg_{z_i}(s) \rceil$, $1 \leqq i \leqq v$, such that $s(w_1, \cdots, w_v, x)$ is squarefree in $\mathbf{Z}[x]$.*

*Proof.* Let $d_i = \deg_{z_i}(s)$ for $1 \leqq i \leqq v$. Since $s$ is squarefree, its discriminant

$$\Delta(z_1, \cdots, z_v) = \mathrm{res}_x\left(s, \frac{\partial s}{\partial x}\right) \neq 0$$

(cf. van der Waerden [28, p. 86]). Since $\Delta$ is the given resultant, it follows that $\deg_{z_i}(\Delta) \leqq (2n-1)d_i$ for $1 \leqq i \leqq v$. If we write $\Delta(z_1, \cdots, z_v)$ as a polynomial in the variables $z_2, \cdots, z_v$ with coefficients in $\mathbf{Z}[z_1]$, not all these coefficients can be zero. Let $u(z_1)$ be one particular nonvanishing coefficient. Since $\deg(u) \leqq (2n-1)d_1$ there exists

an integer $w_1$ with $|w_1| \leqq \lceil (2n-1)/2d_1 \rceil$ and $u(w_1) \neq 0$. Therefore $\Delta(w_1, z_2, \cdots, z_v) \neq 0$ and the lemma now follows by induction on the number of variables. □

We now briefly discuss that the above algorithm is of polynomial complexity in $\deg(\bar{f})$ and $\log(|\bar{f}|)$ provided that this is also true for Algorithm 2. To obtain a squarefree factor $\bar{s}$ of $\bar{f}$, we can use any of squarefree decomposition algorithms referred to in step (S), all of which employ polynomial GCD computations. Furthermore, any of the available GCD algorithms such as the primitive remainder, subresultant or the modular algorithm (cf. Brown [1]), or the EZGCD algorithm by Moses and Yun [25], takes for a fixed number of variables polynomially many steps in the maximum degree of the input polynomial and the size of its coefficients. That this time bound extends to the squarefree factorization process is shown, e.g., in Yun [33]. Of course, $\deg(\bar{s}) \leqq \deg(\bar{f})$ in step (S), and a bound for $|\bar{s}|$ can be determined by the following lemma.

LEMMA 2. *Let* $g_1, \cdots, g_m \in \mathbf{C}[x_1, \cdots, x_v]$, *let* $f = g_1 \cdots g_m$ *and let* $n_j = \deg_{x_j}(f)$, $n = \sum_{j=1}^{v} n_j$. *Then*

$$\prod_{i=1}^{m} |g_i| \leqq 2^n |f| \prod_{j=1}^{v} \left(\frac{n_j+1}{2}\right)^{1/2} \leqq c^n |f|$$

*with* $c < \sqrt{6} \approx 2.44949$ (cf. Gel'fand [9, pp. 135–139]).

Therefore $|\bar{s}| \leqq c^{(v+1)\deg(\bar{f})} |\bar{f}|$. That the steps (M) and (T) take polynomial-time is quite easily established. As a matter of fact, some of the GCD algorithms used for the squarefree decomposition of $\bar{f}$ in step (S) already provide the points $w_1, \cdots, w_v$ of step (T) as a by-product. Step (M) produces a substantially, yet polynomially, larger output compared to its input $\bar{s}$. (For example

$$\deg(s) \leqq n \deg(\bar{s}) \quad \text{and} \quad |s| \leqq (\deg(\bar{s})+1)^{vn} |\bar{s}|^n;$$

cf. Lemma 7.) Step (T) again may produce a larger result, but $|f|$ is clearly polynomial in the size of $s$. (For example

$$|f| \leqq v^{\deg(s)} \deg(s)^v \deg(s)^{2\deg(s)} |s|;$$

see also Lemma 1 and Lemma 4.)

We wish to remark that step (M) could be entirely avoided by modifying Algorithm 2. However, these modifications would complicate the complexity analysis and for the reasons discussed above we shall retain the monicity condition on $f$ during Algorithm 2. The matter becomes more manageable if the coefficients are in a finite field. Some details to this case can be found in von zur Gathen and Kaltofen [8].

Step (E1) is the counterpart of the transformation of step (T). Step (E2) is similar to step (M), but also involves a content computation. Both steps can obviously be performed in time polynomial in $\deg(g)$ and $\log(|g|)$.

**5. The main algorithm.** In this section, we shall discuss an algorithm which computes an irreducible factor of a polynomial $f(y_1, \cdots, y_v, x)$, monic in $x$ with $f(0, \cdots, 0, x)$ squarefree, in polynomial-time in $\deg(f)$ and $\log(|f|)$. We will also prove the proposed algorithm correct. The analysis of its complexity is deferred to the next section. The algorithm first computes a multivariate Taylor series approximation of a root of $f$ for $x$. It then finds the minimal polynomial for this root by solving a linear system in the coefficients of this polynomial.

ALGORITHM 2.

[Input: $f(y_1, \cdots, y_v, x) \in \mathbf{Z}[y_1, \cdots, y_v, x]$ monic in $x$ such that $f(0, \cdots, 0, x)$ is squarefree. $\mathbf{Z}$ can be an arbitrary UFD and $\mathbf{Q}$ its field of quotients. Output: An irreducible factor $g(y_1, \cdots, y_v, x) \in \mathbf{Z}[y_1, \cdots, y_v, x]$ of $f$.]

**(F)** [Factor $f(0, \cdots, 0, x)$:] $n \leftarrow \deg_x(f)$.
Compute an irreducible factor $t(x)$ of $f(0, \cdots, 0, x)$; $m \leftarrow \deg(t)$.
[Let $\beta$ be a root of $t$. In the following, we will perform computations in $\mathbf{Q}(\beta)$, whose elements are represented as polynomials in $\mathbf{Q}[\beta]$ modulo $t$.]

**(N)** [Newton iteration. For purposes of later analysis and reference, we emulate the Newton iteration by a Hensel lifting algorithm. Let $J$ be the ideal in $\mathbf{Q}(\beta)[y_1, \cdots, y_v]$ generated by $\{y_1, \cdots, y_v\}$. The goal is to construct

$$\alpha_j(y_1, \cdots, y_v) = \sum_{i=0}^{j} \sum_{|\underset{\sim}{k}|=i} a_{\underset{\sim}{k}}(\beta) \underset{\sim}{y}^{\underset{\sim}{k}}, \quad \text{where } a_{\underset{\sim}{k}}(\beta) \in \mathbf{Q}(\beta),$$

for $j = 1, 2, \cdots$ such that

$$f(y_1, \cdots, y_v, \alpha_j(y_1, \cdots, y_v)) \equiv 0 \bmod J^{j+1},$$

i.e. no monomials in $y_1, \cdots, y_v$ with total degree less than $j+1$ occur on the left-hand side of the given equation.]
Rewrite $f(y_1, \cdots, y_v, x) = \sum_{\underset{\sim}{k} \geqq \underset{\sim}{0}} f_{\underset{\sim}{k}}(x) \underset{\sim}{y}^{\underset{\sim}{k}}$, where $f_{\underset{\sim}{k}}(x) \in \mathbf{Z}[x]$. [Notice that $f_{\underset{\sim}{0}}(x) = f(0, \cdots, 0, x)$ and, since $f$ is monic and $\deg_x(f) = n$, $\deg(f_{\underset{\sim}{k}}) < n$ for $|\underset{\sim}{k}| \geqq 1$.]
[Set order for approximation:] $d \leftarrow \deg_{y_1, \cdots, y_v}(f)$; $K \leftarrow d(2n-1)$.
[Initialize for Hensel lifting:]

$$a_{\underset{\sim}{0}} \leftarrow \beta; \quad g_{\underset{\sim}{0}}(x) \leftarrow x - \beta; \quad h_{\underset{\sim}{0}}(x) \leftarrow f_{\underset{\sim}{0}}(x) / g_{\underset{\sim}{0}}(x) \in \mathbf{Q}(\beta)[x].$$

FOR ALL $\underset{\sim}{k}$ with $1 \leqq |\underset{\sim}{k}| \leqq K$ DO steps (N1) and (N2). [The $\underset{\sim}{k}$ must be generated in an order such that $|\underset{\sim}{k}|$ is nondecreasing. We will compute polynomials $g_{\underset{\sim}{k}}(x)$ and $h_{\underset{\sim}{k}}(x) \in \mathbf{Q}(\beta)[x]$, $\underset{\sim}{k} \geqq \underset{\sim}{0}$, satisfying

$$\left( \sum_{\underset{\sim}{k} \geqq \underset{\sim}{0}} g_{\underset{\sim}{k}}(x) \underset{\sim}{y}^{\underset{\sim}{k}} \right) \left( \sum_{\underset{\sim}{k} \geqq \underset{\sim}{0}} h_{\underset{\sim}{k}}(x) \underset{\sim}{y}^{\underset{\sim}{k}} \right) = \sum_{\underset{\sim}{k} \geqq \underset{\sim}{0}} f_{\underset{\sim}{k}}(x) \underset{\sim}{y}^{\underset{\sim}{k}}. \quad ] \tag{1}$$

**(N1)** $b_{\underset{\sim}{k}}(x) \leftarrow f_{\underset{\sim}{k}}(x) - \sum_{\underset{\sim}{0} \leqq \underset{\sim}{s} \leqq \underset{\sim}{k}, 1 \leqq |\underset{\sim}{s}| \leqq |\underset{\sim}{k}| - 1} g_{\underset{\sim}{s}}(x) h_{\underset{\sim}{k}-\underset{\sim}{s}}(x).$

**(N2)** [Step (N1) and (1) lead to

$$g_{\underset{\sim}{0}}(x) h_{\underset{\sim}{k}}(x) + h_{\underset{\sim}{0}}(x) g_{\underset{\sim}{k}}(x) = b_{\underset{\sim}{k}}(x) \tag{2}$$

with $g_{\underset{\sim}{k}}(x)$, $h_{\underset{\sim}{k}}(x) \in \mathbf{Q}(\beta)[x]$, $\deg(g_{\underset{\sim}{k}}) \leqq \deg(g_{\underset{\sim}{0}}) - 1 = 0$, $\deg(h_{\underset{\sim}{k}}) \leqq \deg(h_{\underset{\sim}{0}}) - 1 = n-2$. In the Hensel lifting algorithm, (2) is accomplished by the extended Euclidean algorithm (cf. Knuth [16, p. 417, Exercise 3], but since $\deg(g_{\underset{\sim}{k}}) = 0$ we can use direct formulas:]

$$a_{\underset{\sim}{k}} \leftarrow g_{\underset{\sim}{k}}(x) \leftarrow \frac{b_{\underset{\sim}{k}}(\beta)}{f'_{\underset{\sim}{0}}(\beta)}; \quad h_{\underset{\sim}{k}}(x) \leftarrow \frac{b_{\underset{\sim}{k}}(x) - h_{\underset{\sim}{0}}(x) g_{\underset{\sim}{k}}(x)}{g_{\underset{\sim}{0}}(x)}.$$

[Assign approximate root:] $\alpha_j \leftarrow \sum_{0 \leqq |\underset{\sim}{k}| \leqq j} a_{\underset{\sim}{k}} \underset{\sim}{y}^{\underset{\sim}{k}}$ for $0 \leqq j \leqq K$.

**(L)** [Find minimal polynomial for $\alpha_K$:]
[Compute powers of $\alpha_K$:]
FOR $i \leftarrow 0, \cdots, n-1$ DO $\alpha_K^{(i)} \leftarrow \alpha_K^i \bmod J^{K+1}$.
FOR $I \leftarrow m, \cdots, n-1$ DO
$L \leftarrow d(I+n-1)$.
With $a_L^{(i)} \equiv \alpha_K^{(i)} \bmod J^{L+1}$ try to solve the equation

$$\alpha_L^{(I)} + \sum_{i=0}^{I-1} u_i(y_1, \cdots, y_v) \alpha_L^{(i)} \equiv 0 \bmod J^{L+1} \tag{3}$$

for polynomials $u_i(y_1, \cdots, y_v) \in \mathbf{Q}[y_1, \cdots, y_v]$ such that $\deg_{y_1,\cdots,y_v}(u_i) \leqq d$. Let $u_i(y_1, \cdots, y_v) = \sum_{0 \leqq |\underset{\sim}{s}| \leqq d} u_{i,\underset{\sim}{s}} \underset{\sim}{y}^{\underset{\sim}{s}}$ and let

$$\alpha_L^{(i)} = \sum_{0 \leqq |\underset{\sim}{k}| \leqq L} \left( \sum_{j=0}^{m-1} a_{\underset{\sim}{k},j}^{(i)} \beta^j \right) \underset{\sim}{y}^{\underset{\sim}{k}}.$$

Then (3) leads to the linear system

$$a_{\underset{\sim}{k},j}^{(I)} + \sum_{i=0}^{I-1} \sum_{0 \leqq |\underset{\sim}{s}| \leqq d} \alpha_{\underset{\sim}{k}-\underset{\sim}{s},j}^{(i)} u_{i,\underset{\sim}{s}} = 0 \tag{4}$$

for $0 \leqq |\underset{\sim}{k}| \leqq L$, $j = 0, \cdots, m-1$ in the variables $u_{i,\underset{\sim}{s}}$, $i = 0, \cdots, I-1$, $0 \leqq |\underset{\sim}{s}| \leqq d$. [There are $I\binom{v+d}{d}$ unknowns in $m\binom{v+L}{L}$ linear equations. (Cf. Lemma 4.)] IF (4) has a solution (which, as we will prove below, is then integral and unique) THEN

$$g(y_1, \cdots, y_v, x) \leftarrow x^I + \sum_{i=0}^{I-1} u_i(y_1, \cdots, y_v) x^i$$

and EXIT. [We will also show that then $g$ is an irreducible factor of $f$.] [At this point, the above FOR loop has not produced a solution to (3). In this case, $f$ is irreducible.] $g \leftarrow f$. □

Notice that $L$, the order of the approximation needed, grows with $I$, the possible degree of the minimal polynomial. Hence we could improve our algorithm by increasing the order of the approximation within the loop on $I$ in step $L$ instead of computing the best approximation eventually needed a priori in step (N). Also, a complete factorization of $f_{\underset{\sim}{0}}$ may exclude certain degrees for $g$. For example, if $f_{\underset{\sim}{0}}$ factors into irreducibles of even degree, then $g$ cannot be of odd degree. (Cf. Knuth [16, p. 434 and § 4.6.2, Exercise 26].)

We shall now prove the correctness of the above algorithm. We first show that step (N) computes a root $\alpha_K(y_1, \cdots, y_v)$ of $f(y_1, \cdots, y_v, x)$ modulo $J^{K+1}$. The polynomials $g_{\underset{\sim}{k}}(x)$ and $h_{\underset{\sim}{k}}(x) \in \mathbf{Q}(\beta)[x]$, $\underset{\sim}{k} \geqq \underset{\sim}{0}$, must satisfy (1) and thus (2). We now note that $g_{\underset{\sim}{0}}(\beta) = 0$ and $h_{\underset{\sim}{0}}(\beta) = f_{\underset{\sim}{0}}'(\beta)$. The second equation follows from the fact that if $\beta, \beta_2, \cdots, \beta_n$ are the roots of $f_{\underset{\sim}{0}}(x)$ then $h_{\underset{\sim}{0}}(x) = \prod_{i=2}^n (x - \beta_i)$ and hence $h_{\underset{\sim}{0}}(\beta) = \prod_{i=2}^n (\beta - \beta_i) = f_{\underset{\sim}{0}}'(\beta)$. Therefore the unique solution of (2) with $\deg(g_{\underset{\sim}{k}}) = 0$ is $a_{\underset{\sim}{k}} = b_{\underset{\sim}{k}}(\beta)/f_{\underset{\sim}{0}}'(\beta)$. If we now solve (3) for $h_{\underset{\sim}{k}}(x)$, we get

$$h_{\underset{\sim}{k}}(x) = \frac{b_{\underset{\sim}{k}}(x) - h_{\underset{\sim}{0}}(x) g_{\underset{\sim}{k}}(x)}{g_{\underset{\sim}{0}}(x)}$$

which is a polynomial in $x$ since $b_{\underset{\sim}{k}}(\beta) - h_{\underset{\sim}{0}}(\beta) a_{\underset{\sim}{k}} = 0$, and is of degree at most $n-2$. As we will see in § 6, the solution for (3) with $\deg(g_{\underset{\sim}{k}}) < \deg(g_{\underset{\sim}{0}})$ and $\deg(h_{\underset{\sim}{k}}) < \deg(h_{\underset{\sim}{0}})$ is uniquely determined by a linear system in $n$ unknowns, whose coefficient matrix is the Sylvester matrix of $g_{\underset{\sim}{0}}(x)$ and $h_{\underset{\sim}{0}}(x)$, the determinant of which in our case happens to be equal to $f_{\underset{\sim}{0}}'(\beta)$.

We now conclude that

$$f(y_1, \cdots, y_v, \alpha_K(y_1, \cdots, y_v)) \equiv 0 \mod J^{K+1}$$

because

$$\left( x - \sum_{0 \leqq |\underset{\sim}{k}| \leqq K} a_{\underset{\sim}{k}} \underset{\sim}{y}^{\underset{\sim}{k}} \right) \left( \sum_{0 \leqq |\underset{\sim}{k}| \leqq K} h_{\underset{\sim}{k}}(x) \underset{\sim}{y}^{\underset{\sim}{k}} \right) \equiv f(y_1, \cdots, y_v, x) \mod J^{K+1}.$$

The polynomial $g(y_1, \cdots, y_v, x)$ is constructed in step (L) such that

$$g(y_1, \cdots, y_v, \alpha_L(y_1, \cdots, y_v)) \equiv 0 \mod J^{L+1}.$$

We will now prove that $g$ must divide $f$. Our argument will show that if $g$ does not divide $f$, then (3) has a solution for $I < \deg(g)$. One main condition for this to be true is that our approximation is at least of order $L$. First, we must prove a simple lemma.

LEMMA 3. *Let* $g(y_1, \cdots, y_v, x)$ *divide* $f(y_1, \cdots, y_v, x)$ *in* $\mathbf{Z}[y_1, \cdots, y_v, x]$ *and assume that* $g(0, \cdots, 0, \beta) = 0$ *in* $\mathbf{Q}(\beta)$. *Then*

$$g(y_1, \cdots, y_v, \alpha_j(y_1, \cdots, y_v)) \equiv 0 \mod J^{j+1}$$

*for all* $j \geqq 1$ *with* $\alpha_j(y_1, \cdots, y_v)$ *as computed in step* (N).

*Proof.* The reason is simply that since $x - \alpha_j(y_1, \cdots, y_v)$ divides $f(y_1, \cdots, y_v, x) \bmod J^{j+1}$ and $\beta$ is a root of single multiplicity, $x - \alpha_j(y_1, \cdots, y_v)$ must also divide $g(y_1, \cdots, y_v, x) \bmod J^{j+1}$. This argument can be made formal but we shall provide a more indirect proof. Let $p$ be the first index such that

$$g(y_1, \cdots, y_v, \alpha_p(y_1, \cdots, y_v)) \not\equiv 0 \mod J^{p+1}.$$

Because $p$ is the first index

$$g(y_1, \cdots, y_v, \alpha_p(y_1, \cdots, y_v)) \equiv \sum_{|\underset{\sim}{k}|=p} \gamma_{\underset{\sim}{k}} \underset{\sim}{y}^{\underset{\sim}{k}} \mod J^{p+1}$$

with at least one $\gamma_{\underset{\sim}{k}} \neq 0$. Let $h$ be the cofactor of $g$, i.e. $f = gh$. Since $\beta$ is a single root, $r = h(0, \cdots, 0, \beta) \neq 0$. Therefore

$$g(y_1, \cdots, y_v, \alpha_p(y_1, \cdots, y_v))h(y_1, \cdots, y_v, \alpha_p(y_1, \cdots, y_v)) \equiv \sum_{|\underset{\sim}{k}|=p} \gamma_{\underset{\sim}{k}} r \underset{\sim}{y}^{\underset{\sim}{k}} \not\equiv 0 \mod J^{p+1}$$

in contradiction to $\alpha_p(y_1, \cdots, y_v)$ being the $p$th approximation of a root of $f$. □

THEOREM 1. *The first solution of* (3) *in step* (L), *as I increases, determines a proper factor* $g$ *of* $f$ *in* $\mathbf{Z}[y_1, \cdots, y_v, x]$. *This factor is also irreducible.*

*Proof.* We show that $g$ must divide $f$ provided its coefficients satisfy (4). The irreducibility of $g$ then follows immediately from the fact that the minimal polynomial for the root of $f(y_1, \cdots, y_v, x)$ corresponding to $\alpha_L$ also provides a solution to (3) and hence (4). Let

$$D(y_1, \cdots, y_v, x) = \mathrm{GCD}(f(y_1, \cdots, y_v, x), g(y_1, \cdots, y_v, x))$$

and let $I = \deg_x(g)$, $j = \deg_x(D)$. We shall prove that the condition $j < I$ is impossible. Assume that this condition is satisfied, i.e. $0 \leqq j < I$. Let $f = x^n + t_{n-1}x^{n-1} + \cdots + t_0$ and $g = x^I + u_{I-1} + \cdots + u_0$ with $t_l, u_m \in \mathbf{Z}[y_1, \cdots, y_v]$. Using the extended Euclidean algorithm (cf. Knuth [16, p. 417, Exercise 3]) we establish the existence of polynomials $U_j, V_j \in \mathbf{Q}(y_1, \cdots, y_v)[x]$, $\deg_x(U_j) < I - j$ and $\deg_x(V_j) < n - j$, such that

$$U_j f + V_j g = D. \tag{A}$$

It is easy to show that under the given degree constraints these polynomials are uniquely determined. Therefore we must have a nonsingular coefficient matrix for the linear system derived from (A) for the coefficients of $x^j, \cdots, x^{I+n-j-1}$ with the unknowns being the coefficients of $U_j$, $V_j$ of $x$. By $s_j$ we denote the determinant of this coefficient matrix namely

$$s_j = \det \begin{bmatrix} 1 & t_{n-1} & \cdots & & & & & t_{2j-I+1} \\ & & & 1 & t_{n-1} & \cdots & & t_j \\ 1 & u_{I-1} & \cdots & u_{j+1} & & \cdots & & u_{2j-n+1} \\ & & & & 1 & u_{I-1} & \cdots & u_j \end{bmatrix} \neq 0. \tag{B}$$

(In fact, $s_j$ is the leading coefficient of the $j$th sub-resultant of $f$ and $g$ as polynomials in $x$; cf. Brown and Traub [2].) Cramer's rule implies that $s_jU_j,\ s_jV_j \in \mathbf{Z}[y_1, \cdots, y_v, x]$. Moreover,

$$f(y_1, \cdots, y_v, \alpha_L) \equiv g(y_1, \cdots, y_v, \alpha_L) \equiv 0 \mod J^{L+1}$$

and hence

$$s_j(y_1, \cdots, y_v) D(y_1, \cdots, y_v, \alpha_L) \equiv 0 \bmod J^{L+1}.$$

However, from Lemma 3 and the fact that $g$ is the polynomial of smallest degree solving (3) we conclude that $D(0, \cdots, 0, \beta) \neq 0$, which implies with the previous congruence that

$$\text{(C)} \qquad s_j(y_1, \cdots, y_v) \equiv 0 \mod J^{L+1}.$$

On the other hand, using (B) we can bound the degree of $s_j$ by

$$\deg_{y_1, \cdots, y_v}(s_j) \leqq (I + n - 2j - 1)d \leqq (I + n - 1)d = L$$

which together with (C) implies that $s_j = 0$, in contradiction to (B). □

This concludes the correctness proof for Algorithm 2. In the case that $v = 1$ the bound $K$ of step (N) and $L$ of step (L) can be improved to $\lceil d(2n-1)/m \rceil$ (cf. Kaltofen [13, Thm. 4.1]). However, this improvement seems not to carry over for $v \geqq 2$, since $\mathbf{Q}[y_1, \cdots, y_v]$ is not a Euclidean domain.

**6. Complexity analysis of the reduction algorithm.** The goal of this section is to prove that Algorithm 2 takes, for a fixed number of variables $v$, polynomially many steps in $\deg(\bar{f}) \log(|\bar{f}|)$, provided that we can factor $f_{\underline{0}}$ in time polynomial in $\deg(f_{\underline{0}}) \log(|f_{\underline{0}}|)$.

*Step* (F). As A. Lenstra, H. Lenstra and L. Lovász have shown, $t(x)$ can be computed in at most $O(\deg(f_{\underline{0}})^{12} + \deg(f_{\underline{0}})^9 (\log |f_{\underline{0}}|_2)^3)$ steps [22]. This complexity bound can be slightly improved using the results of Kaltofen [15].

*Step* (N). We first count the number of additions, subtractions and multiplications over $\mathbf{Q}(\beta)$ (which we shall call *ASM ops*) needed for this step. Then we bound the absolute value of all elements of $\mathbf{Q}(\beta)$ which appear as intermediate results. Finally, we bound the size of all computed rational numerators and denominators, and then we count the number of rational operations. The most difficult task will be to compute size bounds.

We can ignore the time it takes to retrieve the polynomials $f_{\underline{k}}(x)$ as well as the execution time for the initializations of step (N). In order to count the number of times steps (N1) and (N2) are performed, we need the following lemma.

LEMMA 4. *There exist*

$$\binom{v+j-1}{v-1} \leqq (j+1)^{v-1}$$

*distinct $v$-dimensional integral vectors $\underline{k}$ with $|\underline{k}| = j$. The number of vectors with $|\underline{k}| \leqq j$ is*

$$\binom{v+j}{v} \leqq (j+1)^v.$$

Therefore, steps (N1) and (N2) are executed at most $(K+1)^v$ times. Step (N1) requires at most $O(K^v n)$ *ASM ops* in $\mathbf{Q}(\beta)$. Clearly this bound also dominates the complexity of step (N2). Hence $\alpha_K$ can be calculated in $O(K^{2v} n)$ *ASM ops.*

We now proceed to compute an upper bound $B_1$ for all absolute values of the coefficients of $\alpha_K$ in $\mathbf{Q}(\beta)$.

LEMMA 5. *Let $f(x) \in \mathbf{Z}[x]$ be monic, squarefree, of degree $n$ and let $g(x), h(x) \in \mathbf{C}[x]$ be monic such that $f(x) = g(x)h(x)$.*

a) *Then both $|g|, |h| \leqq 2^n |f|_2 \leqq \sqrt{n+1}\, 2^n |f|$ and if $\beta$ is any root of $f$, $|\beta| < 2|f|$.*

b) *If $M$ is any $(n-1)$ by $(n-1)$ submatrix of the Sylvester matrix of $g$ and $h$, then*

$$|\det(M)| < T(f) = (n2^n|f|)^{n-1}.$$

c) *The resultant of $g$ and $h$ is bounded by $1/S(f) < |\operatorname{res}(g, h)| < 2T(f)$ with*

$$S(f) = (4|f|)^{(n-1)(n-2)/2}.$$

*Proof.* a) The bound for $|g|$ and $|h|$ is the Landau-Mignotte bound translated to maximum norms [24]. Assume $f(x) = a_n x^n + \cdots + a_0$ and let $\beta \in \mathbf{C}$ with $|\beta| \geqq 2|f|$. Then

$$|a_{n-1}\beta^{n-1} + \cdots + a_0| \leqq |f| \frac{|\beta|^n - 1}{|\beta| - 1} < |\beta|^n \leqq a_n |\beta|^n$$

because $|f| \geqq 1$. therefore $f(\beta) \neq 0$. Notice that for this part the monicity of $f$ is not required.

b) By part a), we know that each entry in the Sylvester matrix of $g$ and $h$ is bounded by $\sqrt{n+1}\, 2^n |f|$. Hadamard's determinant inequality (cf. Knuth [16, § 4.6.1, Exercise 15]) then gives the bound.

c) Let $g(x) = (x-\beta_1)\cdots(x-\beta_k)$ and $h(x) = (x-\beta_{k+1})\cdots(x-\beta_n)$. Then

$$\operatorname{res}(g, h) = \prod_{i=1,\cdots,k;\, j=k+1,\cdots,n} (\beta_i - \beta_j)$$

and the discriminant of $f$, $\Delta = \prod_{i \neq j} (\beta_i - \beta_j)$, is an integer not equal 0 (cf. van der Waerden [28, pp. 87-89]). From a) we conclude that $|\beta_i - \beta_j| < 4|f|$ for $1 \leqq i < j \leqq n$. Therefore

$$\begin{aligned} 1 \leqq \sqrt{|\Delta|} &= \left( \prod_{1 \leqq i < j \leqq k} |\beta_i - \beta_j| \right) |\operatorname{res}(g, h)| \left( \prod_{k+1 \leqq i < j \leqq n} |\beta_i - \beta_j| \right) \\ &< |\operatorname{res}(g, h)| (4|f|)^{(n-1)(n-2)/2} \end{aligned}$$

because $k(k-1) + (n-k)(n-k-1) \leqq (n-1)(n-2)$ for $1 \leqq k \leqq n-1$. The upper bound follows from b) and the fact that $g$ and $h$ are monic. □

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

LEMMA 6. *Let $d_{\underset{\sim}{k}} = 1$ for all $v$-dimensional vectors $\underset{\sim}{k}$ with $|\underset{\sim}{k}| = 1$ and let*

$$d_{\underset{\sim}{k}} = \sum_{\underset{\sim}{0} \leqq \underset{\sim}{s} \leqq \underset{\sim}{k},\, 1 \leqq |\underset{\sim}{s}| \leqq |\underset{\sim}{k}| - 1} d_{\underset{\sim}{s}} d_{\underset{\sim}{k} - \underset{\sim}{s}} \quad \text{for } |\underset{\sim}{k}| \geqq 2.$$

*Then*

$$d_{\underset{\sim}{k}} = \frac{1}{|\underset{\sim}{k}|} \binom{2|\underset{\sim}{k}| - 2}{|\underset{\sim}{k}| - 1} \frac{|\underset{\sim}{k}|!}{k_1! \cdots k_v!} < (4v)^{|\underset{\sim}{k}|}.$$

*Proof.* Let $G(y_1, \cdots, y_v) = \sum_{|\underset{\sim}{k}| \geqq 1} d_{\underset{\sim}{k}} \underset{\sim}{y}^{\underset{\sim}{k}}$ be the generating function for $d_{\underset{\sim}{k}}$. Then

$$G(y_1, \cdots, y_v)^2 = G(y_1, \cdots, y_v) - (y_1 + \cdots + y_v)$$

and thus

$$G(y_1, \cdots, y_v) = \frac{1}{2}\left(1 - \sqrt{1 - 4(y_1 + \cdots + y_v)}\right) = \sum_{i=1}^{\infty} \frac{1}{i} \binom{2i-2}{i-1} (y_i + \cdots + y_v)^i$$

which yields our formula. Since $|\underset{\sim}{k}|!/(k_1! \cdots k_v!)$ is a multinominal coefficient, it is less than $v^{|\underset{\sim}{k}|}$. Similarly the given binomial coefficient is less than $2^{2|\underset{\sim}{k}|}$. □

We are now in the position to formulate and prove the main theorem on the coefficient growth for the Hensel lifting algorithm. This theorem also resolves the growth problem left open by Kung and Traub [18] who considered the Newton iteration for the case that $v=1$. We actually use a slightly more general approach which we will also use in § 7.

THEOREM 2. *Let $f(y_1, \cdots, y_v, x) \in \mathbf{Z}[y_1, \cdots, y_v, x]$ be monic of degree $n$ in $x$, such that $f_{\underset{\sim}{0}}(x) = f(0, \cdots, 0, x)$ is squarefree. Let $\beta$ be an algebraic integer generating a subfield of the splitting field for $f_{\underset{\sim}{0}}$. By $\mathbf{Z}[\beta]$ we denote the ring generated by $\mathbf{Z}$ and $\{\beta\}$ whose elements are polynomials in $\beta$ with integral coefficients of degree $[\mathbf{Q}(\beta):\mathbf{Q}]-1$. Let $g_{\underset{\sim}{0}}(x)h_{\underset{\sim}{0}}(x) = f_{\underset{\sim}{0}}(x)$ be a nontrivial factorization of $f_{\underset{\sim}{0}}$ in $(\mathbf{Z}[\beta])[x]$ with $g_{\underset{\sim}{0}}$ and $h_{\underset{\sim}{0}}$ both monic in $x$. Then there exist unique polynomials $g_{\underset{\sim}{k}}(x)$, $h_{\underset{\sim}{k}}(x) \in \mathbf{Q}(\beta)[x]$ with $|\underset{\sim}{k}| \geqq 1$ and* $\deg(g_{\underset{\sim}{k}}) < \deg(g_{\underset{\sim}{0}})$, $\deg(h_{\underset{\sim}{k}}) < \deg(h_{\underset{\sim}{0}})$ *such that*

$$f(y_1, \cdots, y_v, x) = \left(\sum_{\underset{\sim}{k} \geqq \underset{\sim}{0}} g_{\underset{\sim}{k}}(x)\underset{\sim}{y}^{\underset{\sim}{k}}\right)\left(\sum_{\underset{\sim}{k} \geqq \underset{\sim}{0}} h_{\underset{\sim}{k}}(x)\underset{\sim}{y}^{\underset{\sim}{k}}\right).$$

*Furthermore, let*

$$\frac{1}{\operatorname{res}(g_{\underset{\sim}{0}}, h_{\underset{\sim}{0}})} = \frac{1}{R} r(\beta) \quad \text{with } R \in \mathbf{Z},\ r(\beta) \in \mathbf{Z}[\beta],$$

*and let $S(f_{\underset{\sim}{0}})$ and $T(f_{\underset{\sim}{0}})$ be as defined in Lemma 5. Finally, let $N(f) = \max(n^2, n|f|)$, and let $d_{\underset{\sim}{k}}$ be as defined in Lemma 6. Then for all $\underset{\sim}{k}$ with $|\underset{\sim}{k}| \geqq 1$*

$$R^{2|\underset{\sim}{k}|-1} g_{\underset{\sim}{k}}(x),\ R^{2|\underset{\sim}{k}|-1} h_{\underset{\sim}{k}}(x) \in (\mathbf{Z}[\beta])[x]$$

*and, independently of which root $\beta$ of $f_{\underset{\sim}{0}}$ we choose,*

$$|g_{\underset{\sim}{k}}|, |h_{\underset{\sim}{k}}| \leqq d_{\underset{\sim}{k}}(N(f)S(f_{\underset{\sim}{0}})T(f_{\underset{\sim}{0}}))^{2|\underset{\sim}{k}|-1}.$$

*Proof.* The existence and uniqueness of $g_{\underset{\sim}{k}}$ and $h_{\underset{\sim}{k}}$ follows from the fact that (2) has a unique solution with the given degree constraints, $b_{\underset{\sim}{k}}$ being computed as in step (N1). Now let $C_{\underset{\sim}{k}} = \max(|g_{\underset{\sim}{k}}|, |h_{\underset{\sim}{k}}|, |f|)$ and let $D_{\underset{\sim}{k}} = |b_{\underset{\sim}{k}}|$. Since $\deg(g_{\underset{\sim}{s}}) < \deg(g_{\underset{\sim}{0}})$ and $\deg(h_{\underset{\sim}{k}-\underset{\sim}{s}}) < \deg(h_{\underset{\sim}{0}})$, we conclude that

$$|g_{\underset{\sim}{s}} h_{\underset{\sim}{k}-\underset{\sim}{s}}| \leqq (n-1)|g_{\underset{\sim}{s}}||h_{\underset{\sim}{k}-\underset{\sim}{s}}| \leqq (n-1)C_{\underset{\sim}{s}}C_{\underset{\sim}{k}-\underset{\sim}{s}}.$$

By definition $C_{\underset{\sim}{s}} \geqq |f|$ and thus we obtain from (N1)

$$D_{\underset{\sim}{k}} \leqq n \sum_{\underset{\sim}{0} \leqq \underset{\sim}{s} \leqq \underset{\sim}{k},\ 1 \leqq |\underset{\sim}{s}| \leqq |\underset{\sim}{k}|-1} C_{\underset{\sim}{s}} C_{\underset{\sim}{k}-\underset{\sim}{s}}. \tag{A}$$

Let $\vec{p}$ denote the coefficient vector $(p_m, \cdots, p_0)$ of the polynomial $p(x) = p_m x^m + \cdots + p_0$. Now if we solve (2) by undetermined coefficients for $g_{\underset{\sim}{k}}$ and $h_{\underset{\sim}{k}}$ we encounter the Sylvester matrix of $g_{\underset{\sim}{0}}$ and $h_{\underset{\sim}{0}}$, $\operatorname{Syl}(g_{\underset{\sim}{0}}, h_{\underset{\sim}{0}})$, as the coefficient matrix, namely

$$(\vec{h}_{\underset{\sim}{k}}, \vec{g}_{\underset{\sim}{k}}) \operatorname{Syl}(g_{\underset{\sim}{0}}, h_{\underset{\sim}{0}}) = \vec{b}_{\underset{\sim}{k}}, \tag{B}$$

where $(\vec{h}_{\underset{\sim}{k}}, \vec{g}_{\underset{\sim}{k}})$ denotes the vector obtained by concatenation of the vectors $\vec{h}_{\underset{\sim}{0}}$ and $\vec{g}_{\underset{\sim}{k}}$. Using Cramer's rule for (B) and the fact that

$$\frac{1}{|\det(\operatorname{Syl}(g_{\underset{\sim}{0}}, h_{\underset{\sim}{0}}))|} = \frac{1}{|\operatorname{res}(g_{\underset{\sim}{0}}, h_{\underset{\sim}{0}})|} < S(f_{\underset{\sim}{0}})$$

(by Lemma 5c), we get the estimate

$$C_{\underline{k}} \leqq \max(|f|, nD_{\underline{k}} S(f_{\underline{0}}) T(f_{\underline{0}})) \tag{C}$$

(also using Lemma 5b). We now prove our claims by induction on $|\underline{k}|$.

*Case* $|\underline{k}| = 1$. Since $b_{\underline{k}} = f_{\underline{k}} \in \mathbf{Z}[x]$, Cramer's rule applied to (B) yields $Rg_{\underline{k}}$, $Rh_{\underline{k}} \in (\mathbf{Z}[\beta])[x]$. (Notice that $\beta$ is an algebraic integer.) Also $D_{\underline{k}} \leqq |f|$ and hence by (C)

$$C_{\underline{k}} \leqq \max(|f|, n|f| S(f_{\underline{0}}) T(f_{\underline{0}})) \leqq d_{\underline{k}} N(f) S(f_{\underline{0}}) T(f_{\underline{0}}).$$

*Case* $|\underline{k}| > 1$. By hypothesis and from (N1) we obtain $R^{2|\underline{k}|-2} b_{\underline{k}} \in (\mathbf{Z}[\beta])[x]$. Cramer's rule applied to (B) then yields $R^{2|\underline{k}|-1} g_{\underline{k}}$, $R^{2|\underline{k}|-1} h_{\underline{k}} \in (\mathbf{Z}[\beta])[x]$. From (A) and the hypothesis we also get

$$\begin{aligned} D_{\underline{k}} &\leqq n \sum_{\underline{0} \leqq \underline{s} \leqq \underline{k}, 1 \leqq |\underline{s}| \leqq |\underline{k}|-1} C_{\underline{s}} C_{\underline{k}-\underline{s}} \\ &\leqq n (N(f) S(f_{\underline{0}}) T(f_{\underline{0}}))^{2|\underline{k}|-2} \left( \sum_{\underline{0} \leqq \underline{s} \leqq \underline{k}, 1 \leqq |\underline{s}| \leqq |\underline{k}|-1} d_{\underline{s}} d_{\underline{k}-\underline{s}} \right) \\ &= n (N(f) S(f_{\underline{0}}) T(f_{\underline{0}}))^{2|\underline{k}|-2} d_{\underline{k}}. \end{aligned}$$

By (C) we finally obtain

$$\begin{aligned} C_{\underline{k}} &\leqq \max(|f|, nD_{\underline{k}} S(f_{\underline{0}}) T(f_{\underline{0}})) \\ &\leqq d_{\underline{k}} \frac{n^2}{N(f)} (N(f) S(f_{\underline{0}}) T(f_{\underline{0}}))^{2|\underline{k}|-1} \\ &\leqq d_{\underline{k}} (N(f) S(f_{\underline{0}}) T(f_{\underline{0}}))^{2|\underline{k}|-1}. \end{aligned}$$

□

Since the polynomials $g_{\underline{k}}$ and $h_{\underline{k}}$ are unique, we can conclude from Theorem 2 that

$$|a_{\underline{k}}| \leqq d_{\underline{k}} (N(f) S(f_{\underline{0}}) T(f_{\underline{0}}))^{2|\underline{k}|-1} \quad \text{for } 1 \leqq |\underline{k}| \leqq K.$$

From Lemmas 5 and 6 we obtain

$$\begin{aligned} |\alpha_K| \leqq B_1(f) &= (4v)^K (n^2 |f| (4|f|)^{n^2/2} 2^{n^2} (n|f|)^n)^{2K-1} \\ &< (4v)^K (2n|f|)^{2Kn^2}, \end{aligned} \tag{5}$$

assuming that $n \geqq 4$. Obviously, $\log(B_1(f))$ is polynomial in $\deg(f)$ and $\log(|f|)$.

We now demonstrate for the polynomials $g_{\underline{0}} = x - \beta$ and $h_{\underline{0}}$ as computed in step (N), that

$$\frac{R}{\operatorname{res}(g_{\underline{0}}, h_{\underline{0}})} \in \mathbf{Z}[\beta], \quad \text{with } R = \operatorname{res}(t(x), f'_{\underline{0}}(x)),$$

where $t$ is the minimal polynomial of $\beta$. Let $\beta_2, \cdots, \beta_n$ be the roots of $h_{\underline{0}}$. Then

$$\operatorname{res}(g_{\underline{0}}, h_{\underline{0}}) = \prod_{i=2}^{n} (\beta - \beta_i) = f'_{\underline{0}}(\beta).$$

There exist polynomials $A(x)$ and $B(x) \in \mathbf{Z}[x]$ such that $At + Bf'_{\underline{0}} = R$. Thus $R/f'_{\underline{0}}(\beta) = B(\beta) \in \mathbf{Z}[\beta]$, which we wanted to show. Now let $m = \deg(t)$. By Lemma 5a) $|t| \leqq \sqrt{n+1}\, 2^n |f_{\underline{0}}|$, and using Hadamard's determinant inequality for the resultant $\operatorname{res}(t, f'_{\underline{0}})$ we obtain

$$\begin{aligned} |R| &\leqq (\sqrt{(m+1)(n+1)}\, 2^n |f_{\underline{0}}|)^{n-1} (\sqrt{n}\, n |f_{\underline{0}}|)^m \\ &< ((n+1) 2^n |f_{\underline{0}}|)^{m+n} < (2n|f|)^{n^3/2}, \end{aligned} \tag{6}$$

for $n \geqq 4$. Again, we note that $\log(|R|)$ is bounded by a polynomial in $\deg(f)$ and $\log(|f|)$. From Theorem 2 we can also conclude that

$$R^{2|\underset{\sim}{k}|-1} a_{\underset{\sim}{k}} \in \mathbf{Z}[\beta] \quad \text{for } 1 \leqq |\underset{\sim}{k}| \leqq K. \tag{7}$$

We now extend our estimates to the powers of $\alpha_K \bmod J^{K+1}$ as well as count the *ASM ops* needed to compute the powers of $\alpha_K$.

LEMMA 7. *Let* $\alpha_K^{(i)} = \sum_{0 \leqq |\underset{\sim}{k}| \leqq K} a_{\underset{\sim}{k}}^{(i)} \underset{\sim}{y}^{\underset{\sim}{k}}$ *for* $2 \leqq i \leqq n-1$, *then*

$$|a_{\underset{\sim}{k}}^{(i)}| \leqq (K+1)^{v(i-1)} B_1(f)^i \text{ and } R^{2|\underset{\sim}{k}|-1} a_{\underset{\sim}{k}}^{(i)} \in \mathbf{Z}[\beta],$$

*with R as defined above. All* $\alpha_K^{(i)}$, $2 \leqq i \leqq n-1$, *can be computed in* $O(K^{2v}n)$ *ASM ops.*

*Proof.* It is easy to show that

$$a_{\underset{\sim}{k}}^{(i+1)} = \sum_{0 \leqq \underset{\sim}{s} \leqq \underset{\sim}{k}} a_{\underset{\sim}{s}}^{(i)} a_{\underset{\sim}{k}-\underset{\sim}{s}}, \qquad 0 \leqq |\underset{\sim}{k}| \leqq K, \quad i \geqq 1,$$

where there are, by Lemma 4, at most $(|\underset{\sim}{k}|+1)^v \leqq (K+1)^v$ terms under the right-hand sum. The lemma now follows by induction on $i$. □

Therefore we get from (5) for all $0 \leqq i \leqq n-1$ and for $n \geqq 4$

$$|\alpha_K^{(i)}| \leqq B_2(f) = ((K+1)^v B_1(f))^{n-1} < 2^{3vnK} (2n|f|)^{2K(n^3-n^2)}. \tag{8}$$

Lemma 7 also establishes that the common denominator of any rational coefficient computed throughout step (N) is $R^{2K-1}$. We are now in the position of estimating the size of any numerator of the rational coefficients of $\alpha_K^{(i)}$, $1 \leqq i \leqq n-1$. To do this, we shall state a useful lemma.

LEMMA 8. *Let* $\beta$ *be any root of* $t(x) \in \mathbf{Z}[x]$, *monic, squarefree of degree m. Let A be a real upper bound for the absolute value of any conjugate* $\beta_j$, $1 \leqq j \leqq m$, *of* $\beta$. *Assume that for all* $1 \leqq j \leqq m$

$$\left| \sum_{i=0}^{m-1} c_i \beta_j^i \right| \leqq C \quad \text{with } c_i \in \mathbf{Z}.$$

*Furthermore, let D be the absolute value of the discriminant of t. Then*

$$|c_i| \leqq \frac{Cm! A^{m(m-1)/2}}{\sqrt{D}}, \qquad 0 \leqq i < m$$

(*cf. Weinberger and Rothschild* [31, *Lemma* 8.3]).

In our case, we can choose $A = 2|f_{\underset{\sim}{0}}|$, by Lemma 5a), $C = B_2(f) R^{2K-1}$, and $D \geqq 1$. Therefore, if we bring all rationals computed in step (N) to the common denominator $R^{2K-1}$, we have shown that the absolute values of the numerators are bounded by

$$B_3(f, m) = R^{2K-1} B_2(f) m! (2|f_{\underset{\sim}{0}}|)^{m(m-1)/2} < 2^{3vnK} (2n|f|)^{3Kn^3}, \tag{9}$$

using (6), (8) and $n \geqq 4$. Though this bound is quite large, it is of length polynomial in $\deg(f)$ and $\log(|f|)$. This bound also implies, that all *ASM ops* are computable in time polynomial in $\deg(f)$ and $\log(|f|)$. Addition and subtraction in $\mathbf{Q}(\beta)$ means adding or subtracting the numerators of polynomials in $\mathbf{Q}[\beta]$ of degree $m-1$, after eventually multiplying them with a power of $R$ to produce a common denominator. Multiplication in $\mathbf{Q}(\beta)$ is multiplication of $m-1$ degree polynomials in $\mathbf{Q}[\beta]$ followed by a remainder computation w.r.t. $t(\beta)$. Again a common denominator can be extracted a priori. Any *ASM op* takes at most $O(m^2)$ integral operations.

*Step* (L). By Lemma 4, it follows that (4) consists of

$$p = m \binom{v+K}{K} \leqq m(K+1)^v$$

equations in

$$q = I\binom{v+d}{d} \leqq (n-1)(d+1)^v$$

unknowns. Applying Gaussian elimination to (4) takes $O(pq^2)$ rational operations. It is easy to show that this is the dominant operation count, which, expressed in input terms, is

$$O(mn^{v+3}d^{3v}). \tag{10}$$

From the previous analysis, we know that all $a_{k,j}^{(i)}$ can be brought to the common denominator $R^{2K-1}$ and their numerators, $\text{num}(a_{k,j}^{(i)})$, then satisfy $|\text{num}(a_{k,j}^{(i)})| \leqq B_3(f, m)$. As can be shown with little effort, all intermediate rationals computed during the Gaussian elimination process are fractions of subdeterminants of the coefficient matrix for (4) extended by the vector of constants (cf. Gantmacher [6, Chap. 2]). It is not necessary to calculate the GCD of the numerator and denominator of a newly obtained rational since, as can also be shown, the denominator of the row used for the elimination in subsequent rows divides the numerators and denominators in these rows after the elimination step. Thus Hadamard's determinant inequality produces a bound for the size of any intermediately computed integer which is polynomial in $\deg(f)\log(|f|)$. E.g., one such bound is

$$B_4(f, m) = (\sqrt{q}B_3(f, m))^q$$

whose logarithm is by (8) of order

$$\log(B_4(f, m)) = O(d^{v+1}vn^5 \log(n|f|)). \tag{11}$$

Hence, step (L) also takes at most polynomial-time in $\deg(f)$ and $\log(|f|)$. Notice that (10) and (11) give a very crude bound for the complexity of the steps (N) and (L). Since we know that any solution of (4) must be integral of quite a small size, due to Lemma 2, a Chinese remaindering algorithm could be used to solve (4) (cf. McClellan [23]) and we believe that this approach will be much more efficient, in practice.

**7. Multivariate irreduciblity testing.** As we have seen in § 5, in order to establish the irreducibility of the polynomial $f$ by Algorithm 2 we need to factor $f_0$. Reducibility of $f_0$ does, of course, not imply reducibility of $f$. The following theorem partially fills this gap by constructing from a polynomial $f(y_1, \cdots, y_v, x)$, monic in $x$ with $f(0, \cdots, 0, x)$ squarefree, a polynomial $g(y_1, x)$ in time polynomial in $\deg(f)$ and $\log(|f|)$, such that $g$ is irreducible if and only if $f$ is irreducible. Unfortunately, our approach does not allow us to eliminate $y_1$. We could include this as an open problem, but in view of the polynomial-time algorithm for bivariate factorization a solution appears not to be so significant.

LEMMA 9. *Let $t(y_1, \cdots, y_v) \in \mathbf{Z}[y_1, \cdots, y_v]$ be a nonzero polynomial. Then $t(y_1, cy_1, y_3, \cdots, y_v) \neq 0$ for an integer $c$ with $|c| \geqq 2|t|$.*

*Proof.* Let $ay_1^{e_1} \cdots y_v^{e_v}$ be a monomial in $t$ with $a \neq 0$. Then $t(y_1, cy_1, \cdots, y_v)$ contains the monomial $b(c)y^{e_1+e_2}y_3^{e_3} \cdots y_v^{e_v}$ where $b(c)$ is an integral polynomial in $c$ with degree at most $e_1 + e_2$. Since $b(c) = \cdots + ac^{e_2} + \cdots$ it cannot, as a polynomial, be identical to 0. From Lemma 5a and the fact that $|b| \leqq |t|$ we conclude that $b(c) \neq 0$ for any integer of the stated size. □

THEOREM 3. *Let $f(y_1, \cdots, y_v, x) \in \mathbf{Z}[y_1, \cdots, y_v, x]$ be monic of degree $n$ in $x$ such that $f_0 = f(0, \cdots, 0, x)$ is squarefree. Let $T(f_0)$ be as in Lemma 5b, and let $N(f)$ be as in Theorem 2. Furthermore, assume that $f(y_1, \cdots, y_v, x)$ is irreducible. Finally let*

$d = \deg_{y_1,\cdots,y_v}(f)$. *Then for any integer* $c$ *with*

$$|c| \geqq B_5(f) = 2(4v)^{2d}(2N(f)T(f_{\underset{\sim}{0}})^2)^{4d-1}$$

$f(y_1, cy_1, y_3, \cdots, y_v, x)$ *is irreducible in* $\mathbf{Z}[y_1, y_3, \cdots, y_v, x]$.

*Proof.* Let $\mathbf{Q}[[y_1, \cdots, y_v]]$ denote the domain of formal power series in $y_1, \cdots, y_v$ over $\mathbf{Q}$, and let

$$g_c(y_1, y_3, \cdots, x) = f(y_1, cy_1, y_3, \cdots, x).$$

Then each factor of $g_c(y_1, y_3, \cdots, x) \in \mathbf{Q}[[y_1, y_3, \cdots, y_v]][x]$ corresponds to a factor of $f(y_1, y_2, \cdots, x) \in \mathbf{Q}[[y_1, y_2, \cdots, y_v]][x]$ with $y_2$ replaced by $cy_1$. For, if a factor of $g_c$ were not obtainable from a factor of $f$, we could present two different factorizations of $g_c$ which, when evaluated at $y_1 = y_3 = \cdots = y_v = 0$, would result in one and the same factorization of $g_c(0, \cdots, 0, x) \in \mathbf{Q}[x]$. But this is impossible due to the uniqueness of the Hensel lifting procedure as proven in Theorem 2.[2] 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 $g_c$. Our plan is the following: We first show that any candidate factor $h(y_1, y_2, \cdots, x)$ of $f(y_1, y_2, \cdots, x) \in \mathbf{Q}[[y_1, \cdots, y_v]][x]$ contains at least one monomial $b_{\underset{\sim}{p},m}\underset{\sim}{y}^{\underset{\sim}{p}}x^m$ with $b_{\underset{\sim}{p},m} \neq 0$ and $d < |\underset{\sim}{p}| \leqq 2d$. From it we get a polynomial coefficient of $x^m$ in $h$ whose total degree in $y_1, \cdots, y_v$ equals $|\underset{\sim}{p}|$. By choosing $c$ sufficiently large (cf. Lemma 9) we will be able to preserve this coefficient throughout $h_c = h(y_1, cy_1, \cdots, x)$. Hence such an $h_c$ contains a monomial in $y_1, y_3, \cdots, y_v$ of total degree $|\underset{\sim}{p}| > d$. Therefore $h_c$ cannot be a polynomial dividing $g_c$ for otherwise its total degree in $y_1, y_3, \cdots, y_v$ could not be larger than $d$. Let

$$h(y_1, \cdots, y_v, x) = \sum_{i=0}^{l} \sum_{\underset{\sim}{k} \geqq \underset{\sim}{0}} b_{\underset{\sim}{k},i}\underset{\sim}{y}^{\underset{\sim}{k}}x^i$$

be a factor of $f(y_1, y_2, \cdots, x)$ in $\mathbf{Q}[[y_1, \cdots, y_v]][x]$ and let

$$\bar{h}(y_1, \cdots, y_v, x) = \sum_{i=0}^{n-l} \sum_{\underset{\sim}{k} \geqq \underset{\sim}{0}} \bar{b}_{\underset{\sim}{k},i}\underset{\sim}{y}^{\underset{\sim}{k}}x^i$$

be its cofactor, i.e. $f = h\bar{h}$. We first can assume that

$$h(0, \cdots, 0, x) = \sum_{i=0}^{l} b_{\underset{\sim}{0},i}x^i \in \mathbf{Z}[x].$$

Otherwise $h(y_1, cy_1, y_3, \cdots, x)$ could not be an integral polynomial for any choice of $c$.

Now there must exist at least on $b_{\underset{\sim}{k},i}$ or $\bar{b}_{\underset{\sim}{k},i}$ with

$$d < |\underset{\sim}{k}| \leqq 2d \quad \text{and} \quad (b_{\underset{\sim}{k},i} \neq 0 \text{ or } \bar{b}_{\underset{\sim}{k},i} \neq 0).$$

To see this, assume the contrary. Then

$$\left(\sum_{i=0}^{l} \sum_{0 \leqq |\underset{\sim}{k}| \leqq d} b_{\underset{\sim}{k},i}\underset{\sim}{y}^{\underset{\sim}{k}}x^i\right)\left(\sum_{i=0}^{n-l} \sum_{0 \leqq |\underset{\sim}{k}| \leqq d} \bar{b}_{\underset{\sim}{k},i}\underset{\sim}{y}^{\underset{\sim}{k}}x^i\right) = f(y_1, \cdots, y_v, x)$$

since no monomial $a\underset{\sim}{y}^{\underset{\sim}{k}}x^i$, $a$ a nonzero rational, with $d < |\underset{\sim}{k}| \leqq 2d$ in the left product could be canceled by higher terms in the product of the complete expansion of $h$ and $\bar{h}$. Notice that $f$ does not contain a monomial in $\underset{\sim}{y}$ of degree larger than $d$. But this contradicts the fact that $f$ is irreducible. Without loss of generality we now can assume

[2] I owe this argument to Prof. Hendrik W. Lenstra, Jr.

the existence of a vector $\underset{\sim}{p}$ and an integer $m$ such that

$$b_{\underset{\sim}{p},m} \neq 0 \quad \text{with } d < |\underset{\sim}{p}| \leqq 2d \text{ and } 0 \leqq m \leqq l.$$

Let us consider the coefficient of $x^m$ in $h$ whose total degree in $y_1, \cdots, y_v$ is $|\underset{\sim}{p}|$. Set

$$t_{\underset{\sim}{p},m}(y_1, \cdots, y_v) = \sum_{|\underset{\sim}{j}|=|\underset{\sim}{p}|} b_{\underset{\sim}{j},m} \underset{\sim}{y}^{\underset{\sim}{j}}$$

which is a polynomial in $\mathbf{Q}[y_1, \cdots, y_v]$ not identical to 0.

We now apply Theorem 2 with $\beta = 1$, $g_{\mathbf{Q}}(x) = h(0, \cdots, 0, x) \in \mathbf{Z}[x]$ and $h_{\mathbf{Q}}(x) = \bar{h}(0, \cdots, 0, x) \in \mathbf{Z}[x]$. First notice that, since $f_{\mathbf{Q}}$ is squarefree, $0 \neq R = \operatorname{res}(g_{\mathbf{Q}}, h_{\mathbf{Q}}) \in \mathbf{Z}$ and hence $1/|R| \leqq 1$ meaning that we can set $S(f_{\mathbf{Q}}) = 1$. Secondly,

$$|b_{\underset{\sim}{j},m}| \leq |g_{\underset{\sim}{j}}| \leqq (4v)^{|\underset{\sim}{j}|}(N(f)T(f_{\mathbf{Q}}))^{2|\underset{\sim}{j}|-1} \leqq (4v)^{2d}(N(f)T(f_{\mathbf{Q}}))^{4d-1}$$

because of Lemma 6 and $|\underset{\sim}{j}| = |\underset{\sim}{p}| \leqq 2d$. Finally,

$$R^{2|\underset{\sim}{j}|-1} b_{\underset{\sim}{j},m} \in \mathbf{Z} \quad \text{and} \quad R^{2|\underset{\sim}{j}|-1} \leqq R^{4d-1} < (2T(f_{\mathbf{Q}}))^{4d-1},$$

the last inequality by Lemma 5c. In summary,

$$0 \neq R^{4d-1} t_{\underset{\sim}{p},m}(y_1, \cdots, y_v) \in \mathbf{Z}[y_1, \cdots, y_v]$$

and

$$|R^{4d-1} t_{\underset{\sim}{p},m}| < (4v)^{2d}(2N(f)T(f_{\mathbf{Q}})^2)^{4d-1} = \tfrac{1}{2}B_5(f).$$

From Lemma 9 we now conclude that for any integer $c \geqq B_5(f)$

$$t_{\underset{\sim}{p},m}(y_1, cy_1, y_3, \cdots, y_v) \neq 0.$$

Therefore $h(y_1, cy_1, y_3, \cdots, x)$ contains a nonzero monomial in $y_1, y_3, \cdots, y_v$ of total degree larger than $d$ and cannot be a polynomial factor of $f(y_1, cy_1, y_3, \cdots, x)$, as argued above. Our given bound then obviously works for any factor candidate $h$. □

Our irreducibility test can now be constructed easily by induction. We compute the integers $c_1, \cdots, c_{v-1}$ such that for the sequence of polynomials $f_1 = f$,

$$f_2(y_1, y_3, \cdots, x) = f_1(y_1, c_1 y_1, y_3, \cdots, x),$$

$$f_3(y_1, y_4, \cdots, x) = f_2(y_1, c_2 y_1, y_2, \cdots, x), \cdots,$$

$$f_v(y_1, x) = f_{v-1}(y_1, c_{v-1} y_1, x), \qquad g = f_v,$$

we have $c_i \geqq B_5(f_i)$ for all $1 \leqq i \leqq v-1$. Since $v$ is assumed to be fixed and since $B_5(f_i)$ is of size polynomial in $\deg(f_i)$ and $\log(|f_i|)$, $g$ can be constructed in time polynomial in $\deg(f)$ and $\log(|f|)$. By Theorem 3, $g$ is irreducible if $f$ is irreducible. On the other hand, if $f = h_1 h_2$ then

$$g(y_1, x) = h_1(y_1, c_1 y_1, \cdots, c_{v-1} y_1, x) h_2(y_1, c_1 y_1, \cdots, c_{v-1} y_1, x).$$

One can prove Theorem 3 for the more general substitution $y_2 = cy_1^s$, $s$ being an arbitrary positive integer. Since the bound $B_5(f)$ grows monotonically in $|f|$ we can, in the case that $f$ is reducible, find a bound for $c$ using Lemma 2 such that the given subsitution maps all irreducible factors of $f$ into irreducible polynomials in one less variable. Together with a Kronecker like algorithm this then leads to a different polynomial-time reduction from multivariate to bivariate polynomial factorization. In the case of $v = 2$ the complete proof is given in Kaltofen [12], which, following the lines of the proof for Theorem 3, is readily extended to any fixed $v$. Instead of using Kronecker's algorithm one can also apply the multivariate Hensel lifting algorithm by

Musser [26] with the coefficients in $\mathbf{Q}(y_1)$. Since our evaluation guarantees that no extraneous factors can occur, all computed coefficients must actually lie in $\mathbf{Z}[y_1]$. A version of Theorem 3 can also be formulated if the coefficients are from a finite field (cf. Chistov and Grigoryev [3, Thm. 4]).

The type of substitution $y_2 = cy_1^s$ is derived from a version of the Hilbert irreducibility theorem by Franz [5] and Theorem 3 can be regarded as its effective counterpart. For the classical Hilbert irreducibility theorem, no such an effective formulation seems to be known. (See open problem 2 in § 8.)

**8. Conclusion.** We have shown how to overcome the extraneous factor problem during the multivariate Hensel algorithm by approximating a root and then determining its minimal polynomial, which leads to solving a system of linear equations. Our main algorithm was formulated for coefficients from a unique factorization domain and hence can also be applied to polynomials over Galois fields or algebraic extensions of the rationals. It can be shown that in both cases the algorithm works in polynomial-time.

In the case of algebraic coefficients we need a polynomial-time algorithm for univariate factorization. That this is possible is a consequence of the polynomial-time algorithm for factoring univariate polynomials over the integers (cf. Landau [19]). One usually describes an algebraic extension of the rationals by the minimal polynomial of an algebraic integer generating the field and then reduces the problem to factoring polynomials with coefficients which are algebraic integers. The ring of algebraic integers is in general not a unique factorization domain. Therefore we cannot guarantee that a solution of (4) consists of algebraic integers but one can prove that the numbers are algebraic integers within an integral quotient (cf. Weinberger and Rothschild [31, Lemma 7.1]).

In the case that the coefficients are elements from a finite field one may not be able to carry out all transformations of § 4. It may happen that good translation points $w_i$ do not exist within the coefficient field. Then the coefficient domain has to be extended to a larger field and thus the factors returned by Algorithm 2 may have coefficients which are not in the original coefficient field. A simple trick by taking the norm (cf. Trager [27]) can then be used to determine the irreducible factors in the smaller field. This approach together with the Berlekamp algorithm (cf. Knuth [16, § 4.6.2]) gives an algorithm which works in time polynomial in the total degree of the input polynomial and the cardinality of the coefficient field, as shown in von zur Gathen and Kaltofen [8].

We conclude this paper with a list of open problems.

*Problem* 1. Do there exist a polynomial $p(d, v)$ and an infinite sequence of polynomials $f(x_1, \cdots, x_v) \in \mathbf{Z}[x_1, \cdots, x_v]$ with the following property: Any $f$ in the sequence contains less than $p(d(f), v)$ monomials with nonzero coefficients where

$$d(f) = \max_{i=1,\cdots,v} \{\deg_{x_i}(f)\};$$

moreover, there does not exist a polynomial $q(d, v)$ such that any factor of $f$ contains less than $q(d(f), v)$ monomials with nonzero coefficients? In simple words, are there sparse polynomials with dense factors? See von zur Gathen [7] for a partial positive answer.

*Problem* 2. Given any polynomial $p(n)$, does there exist an infinite sequence of irreducible polynomials $f(y, x) \in \mathbf{Z}[y, x]$, $n = \deg(f)$, such that for all integers $i < p(n)$ all polynomials $f(i, x)$ are reducible? This problem asks whether there is a strongly effective version of the Hilbert irreducibility theorem.

*Problem* 3. Given a polynomial $f(x_1, \cdots, x_v) \in \mathbf{Z}_p[x_1, \cdots, x_v]$, $p$ prime, can one determine irreducibility of $f$ in deterministic time polynomial in $\log(p) \deg(f)$?

**Acknowledgments.** The problem of polynomial-time reductions for multivariate polynomial factorization was brought to my attention by Prof. George Collins. I also wish to thank Prof. Bobby Caviness and Prof. B. David Saunders for all their support. The final presentation has also benefitted from the careful remarks of one referee. This paper could not have been typeset without the help of my wife Hoang.

The examples in § 3 were computed on the MACSYMA system.

*Note added in proof.* A. K. Lenstra has presented another polynomial-time algorithm for factoring multivariate integral polynomials at the 10th International Colloquium on Automata, Languages and Programming. Cf. Lecture Notes in Computer Science 154, Springer, Berlin 1983, pp. 458-465.

## REFERENCES

[1] W. S. BROWN, *On Euclid's algorithm and the computation of polynomial greatest common divisors*, J. ACM, 18 (1971), pp. 478-504.

[2] W. S. BROWN AND J. F. TRAUB, *On Euclid's algorithm and the theory of subresultants*, J. ACM, 18 (1971), pp. 505-514..

[3] A. L. CHISTOV AND D. Y. GRIGORYEV, *Polynomial-time factoring of the multivariable polynomials over a global field*, Lomi preprint E-5-82, Leningrad 1982.

[4] K. DÖRGE, *Zum Hilbertschen Irreduzibilitätssatz*, Math. Annal., 95 (1926), pp. 84-97.

[5] W. FRANZ, *Untersuchungen zum Hilbertschen Irreduzibilitätssatz*, Math. Z., 33 (1931), pp. 275-293.

[6] F. R. GANTMACHER, *Matrix Theory, Vol.* 1, Chelsea, New York, 1959.

[7] J. VON ZUR GATHEN, *Factoring sparse multivariate polynomials*, Proc. 1983 IEEE Symposium on Foundations of Computer Science, pp. 172-197.

[8] J. VON ZUR GATHEN AND E. KALTOFEN, *A polynomial-time algorithm for factoring multivariate polynomials over finite fields*, Proc. 1983 International Conference on Automata, Languages and Programming. Lecture Notes in Computer Science 154, Springer, Berlin, 1983, pp. 250-263.

[9] A. O. GEL'FAND, *Transcendental and Algebraic Numbers*, Dover, New York, 1960.

[10] G. H. HARDY AND E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 5th ed. Oxford Univ. Press, Cambridge, 1979.

[11] D. HILBERT, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math., 110 (1892), pp. 104-29.

[12] E. KALTOFEN, *A polynomial reduction from multivariate to bivariate integral polynomial factorization*, Proc. 1982 ACM Symposium Theory of Computers, pp. 261-266.

[13] ———, *A polynomial-time reduction from bivariate to univariate integral polynomial factorization*, Proc. 23rd, IEEE Symposium on Foundations of Computer Science, 1982, pp. 57-64.

[14] ———, *On the complexity of factoring polynomials with integer coefficients*, Ph.D. thesis, Rensselaer Polytechnic Institute, Troy, NY, December 1982.

[15] ———, *On the complexity of finding short vectors in an integer lattice*, Proc. 1983 European Computational Algebra Conference, Lecture Notes in Computer Science, 162, Springer, Berlin, 1983, pp. 236-244.

[16] D. E. KNUTH, *The Art of Computer Programming, Vol* 2, *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, MA, 1981.

[17] L. KRONECKER, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*. J. Reine Angew. Math., 92 (1882), pp. 1-122.

[18] H. T. KUNG AND J. F. TRAUB, *All algebraic functions can be computed fast*, J. ACM, 25 (1978), pp. 245-260.

[19] S. LANDAU, *Factoring polynomials over algebraic number fields is in polynomial time*, this Journal, 14 (1985), pp. 184-195.

[20] A. K. LENSTRA, *Factoring polynomials over algebraic number fields*, Proc. 1983 European Computational Algebra Conference, Lecture Notes in Computer Science 162, Springer, Berlin, 1983, pp. 245-254.

[21] ———, *Factoring multivariate polynomials over a finite field*, Proc. 1983 ACM Symposium on Theory of Computers, pp. 189-192.

[22] A. K. LENSTRA, H. W. LENSTRA AND L. LOVÁSZ, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515-534.

[23] M. T. McCLELLAN, *The exact solution of systems of linear equations with polynomial coefficients*, J. ACM 20 (1973), pp. 563-588.

[24] M. MIGNOTTE, *An inequality about factors of polynomials*, Math. Comp., 28 (1974), pp. 1153-1157.

[25] J. MOSES AND D. Y. Y. YUN, *The* EZGCD *algorithm*, Proc. 1973 ACM National Conference, pp. 159-166.

[26] D. R. MUSSER, *Multivariate polynomial factorization*, J. ACM, 22 (1976), pp. 291-308.

[27] B. M. TRAGER, *Algebraic factoring and rational function integration*, in Proc. ACM Symposium on Symbolic and Algebraic Computations 1976, R. Jenks, ed., pp. 219-226.

[28] B. L. VAN DER WAERDEN, *Modern Algebra, Vol.* 1, Engl. transl. by F. Blum, Ungar Publ., New York, 1953.

[29] P. S. WANG, *An improved multivariate polynomial factoring algorithm*, Math. Comp., 32 (1978), pp. 1215-1231.

[30] P. S. WANG AND B. M. TRAGER, *New algorithms for polynomial square-free decomposition over the integers*, this Journal, 8 (1979), pp. 300-305.

[31] P. WEINBERGER AND L. P. ROTHSCHILD, *Factoring polynomials over algebraic number fields*, ACM Trans. Math. Software, 2 (1976), pp. 335-350.

[32] D. Y. Y. YUN, *On squarefree decomposition algorithms*, in R. Jenks, ed., Proc. ACM Symposium on Symbolic and Algebraic Computations 1976 ACM, pp. 26-35.

[33] ———, *On the equivalence of polynomial* GCD *and squarefree factorization problems*, Proc. MACSYMA User's Conference 77 NASA, Washington, DC, 1977, pp. 65-70.

[34] H. ZASSENHAUS, *Polynomial time factoring of integral polynomials*, ACM SIGSAM Bulletin, 15 (May 1981), pp. 6-7.

[35] R. E. ZIPPEL, *Probabilistic algorithms for sparse polynomials*, Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, 1979.