Polynomial-Time Reductions from Multivariate to Bi- and Univariate Integral Polynomial Factorization*

Erich Kaltofen

University of Toronto
Department of Computer Science
Toronto, Ontario M5S 1A4, Canada

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 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 irreducibility.

Keywords. Polynomial Factorization, Polynomial-Time Complexity, Algorithm Analysis, Hensel Lemma, Hilbert Irreducibility Theorem.

---

* This work has been partially supported by the National Science Foundation under Grant #MCS-7909158 and by the Department of Energy under Grant DE-AS02-ER7602075.
Current address of the author: Rensselaer Polytechnic Institute, Department of Mathematical Sciences, Troy, New York 12181.
This paper appears in the SIAM Journal on Computing, **14**/2, pp. 469--489 (1985).

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 section 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 integral 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.

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. section 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 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.† Unfortunately, in the sparse case little is known about even the

† Our algorithm remains even polynomial in some slightly sharper input size measures such as $l(d_1+1)\cdots$

space complexity of the answer under these conditions. In section 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. section 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 section 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 section 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 section 3. In section 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 section 5 including the necessary arguments for its correctness. Its complexity is analyzed in section 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 section 7. We conclude in section 8 by raising 3 open problems.

2. Notation

By **Z** we denote the set of the integers, by **Q** the set of the rational numbers and by **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, $D[x_1,\ldots,x_v]$ denotes the set of polynomials in $x_1, \ldots, x_v$ over D, $D(x_1,\ldots,x_v)$ its field of quotients; $\deg_{x_1}(f)$ denotes the highest degree of x_1 in $f \in D[x_1,\ldots,x_v]$, $\deg_{x_1,x_2}(f)$ the highest total degree of monomials in x_1 and x_2 in f, and $\deg(f) = \deg_{x_1,\ldots,x_v}(f)$ the total degree of f. Thus, $\deg(f)$ is the maximum of all exponent sums of monomials in $x_1, \ldots, x_v$ with non-zero 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 $\mathrm{ldcf}_{x_v}(f) \in D[x_1, \ldots, x_{v-1}]$. We call f monic in x_v if $\mathrm{ldcf}_{x_v}(f)$ is the unity of

---

(d_v+1) where d_i is the degree of the i-th variable.

D. As is well-known, $D[x_1,\ldots,x_v]$ is a unique factorization domain (UFD) provided that D is a UFD. In this case the content of $f \in D[x_1,\ldots,x_v]$ in x_v, $\mathrm{cont}_{x_v}(f)$, is the greatest common divisor (GCD) of all coefficients of $f(x_v)$ as elements in $D[x_1,\ldots,x_{v-1}]$. Notice again that $\mathrm{cont}_{x_v}(f) \in D[x_1,\ldots,x_{v-1}]$. The primitive part of f in x_v is defined as

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

and we call f primitive in x_v if $f = \mathrm{pp}_{x_v}(f)$. We also note that the total degree of a factor of f is less than or equal to the total degree of f. The infinity norm of $f \in \mathbf{C}[x_1,\ldots,x_v]$, the maximum of the absolute values of the complex coefficients of f, will be denoted by $|f|$. The squareroot 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 $a_i, b_j \in D[x_1,\ldots,x_{v-1}]$. By $\mathrm{Syl}_{x_v}(f,g)$ we denote the Sylvester matrix of f and g,

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

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: $\underline{k} \equiv (k_1,\ldots,k_v)$, $\underline{0} \equiv (0,\ldots,0)$, $\underline{y}^{\underline{k}} \equiv {y_1}^{k_1}\cdots{y_v}^{k_v}$, $\underline{k} \pm \underline{l} \equiv (k_1 \pm l_1,\ldots, k_v \pm l_v)$, $\underline{k} \le \underline{l}$ if, for all i, $k_i \le l_i$ and finally $|\underline{k}| \equiv k_1+\cdots+k_v$, if $\underline{k} \ge \underline{0}$, and $-\infty$ otherwise.

By $\binom{n}{m}$ we denote the binomial coefficient $\dfrac{n!}{m!\,(n-m)!}$.

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:

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

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, Sec. 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. section 7, theorem 3).

In order to give exponentially bad inputs for the multivariate Hensel algorithm we need an irreducible polynomial $f(y_1,\ldots,y_v,x)$ such that $f(0,\ldots,0,x)$ 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 $\deg_y(f) \leq 3$ 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

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

We can also remove the rational denominators, namely

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

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 section 8 refers to this question.

4. Initial Transformations

In this section we present an algorithm which transforms the problem of factoring the polynomial $\bar{f}(z_1,\ldots,z_v,x)$ to factoring a polynomial $f(y_1,\ldots,y_v,x)$ such that f is monic in x, $f(0,\ldots,0,x)$ 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 $\bar{f}(z_1,\ldots,z_v,x) \in \mathbf{Z}[z_1,\ldots,z_v,x]$, this algorithm constructs an irreducible factor $\bar{g}(z_1,\ldots,z_v,x) \in \mathbf{Z}[z_1,\ldots,z_v,x]$ of $\bar{f}$ by preconditioning $\bar{f}$ and calling algorithm 2.]

(I) [Test for univariate case:]
IF $\mathrm{cont}(\bar{f})$ 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 $\bar{s}(z_1,\ldots,z_v,x)$ 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:] $n \leftarrow \deg_x(\bar{s})$; $c(z_1,\ldots,z_v) \leftarrow \mathrm{ldcf}_x(\bar{s})$;
$s(z_1,\ldots,z_v,x) \leftarrow c(z_1,\ldots,z_v)^{n-1}\, \bar{s}\left(z_1,\ldots,z_v,\dfrac{x}{c(z_1,\ldots,z_v)}\right)$.
[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 $w_1,\ldots,w_v$ such that $s(w_1,\ldots,w_v,x)$ is squarefree.]
FORALL integers w_i with $|w_i| \le \left\lceil \dfrac{2n-1}{2} \deg_{z_i}(s) \right\rceil$, $1 \le i \le v$, DO
Test whether $s(w_1,\ldots,w_v,x)$ is squarefree. If so, exit loop.

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

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

(E) [Recover a possibly non-monic factor $\bar{g}(z_1,\ldots,z_v,x)$ of $\bar{f}(z_1,\ldots,z_v,x)$.]

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

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

We shall first prove the correctness of the above algorithm. Obviously, if $g(y_1,\ldots, y_v, x)$ divides f then $g(z_1,\ldots, z_v, x)$ divides $s(z_1,\ldots, z_v, x)$. 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 $s(z_1,\ldots,z_v,x) \in \mathbf{Z}[z_1,\ldots,z_v,x]$ be monic of degree n in x and squarefree. Then there exist integers w_i with $|w_i| \le \left\lceil \frac{2n-1}{2} \deg_{z_i}(s) \right\rceil$, $1 \le i \le v$, such that $s(w_1,\ldots,w_v,x)$ is squarefree in $\mathbf{Z}[x]$.

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

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

(cf. van der Waerden [28, p.86]). Since Δ is the given resultant, it follows that $\deg_{z_i}(\Delta) \le (2n-1)d_i$ for $1 \le i \le v$. If we write $\Delta(z_1,\ldots,z_v)$ as a polynomial in the variables $z_2,\ldots, z_v$ with coefficients in $\mathbf{Z}[z_1]$, not all these coefficients can be zero. Let $u(z_1)$ be one particular non-vanishing coefficient. Since $\deg(u) \le (2n-1)d_1$ there exists an integer w_1 with $|w_1| \le \left\lceil \frac{2n-1}{2} d_1 \right\rceil$ and $u(w_1) \neq 0$. Therefore $\Delta(w_1,z_2,\ldots,z_v) \neq 0$ 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 [2]), 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, $\deg(\bar{s}) \le \deg(\bar{f})$ in step (S), and a bound for $|\bar{s}|$ can be determined by the following lemma.

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

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

with $c < \sqrt{6} \approx 2.44949$. (Cf. Gel'fond [9, pp.135-139].) □

Therefore $|\bar{s}| \leq c^{(v+1)\deg(\bar{f})} |\bar{f}|$. 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 $w_1,\ldots,w_v$ of step (T) as a by-product. Step (M) produces a substantially, yet polynomially, larger output s compared to its input $\bar{s}$. (E.g.

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

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

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

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

(F) [Factor $f(0,\ldots,0,x)$:] $n \leftarrow \deg_x(f)$.
Compute an irreducible factor $t(x)$ of $f(0,\ldots,0,x)$; $m \leftarrow \deg(t)$.

[Let BT be a root of t. In the following, we will perform computations in $\mathbf{Q}(BT)$, whose elements are represented as polynomials in $\mathbf{Q}[BT]$ 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 $\mathbf{Q}(BT)[y_1,\ldots,y_v]$ generated by $\{y_1,\ldots,y_v\}$. The goal is to construct

$$AL_j(y_1,\ldots,y_v) = \sum_{i=0}^{j} \sum_{|\underline{k}|=i} a_{\underline{k}}(BT)\, \underline{y}^{\underline{k}}, \qquad \text{where } a_{\underline{k}}(BT) \in \mathbf{Q}(BT),$$

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

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

i.e. no monomials in $y_1,\ldots,y_v$ with total degree less than j occur on the left-hand side of the given equation.]

Rewrite $f(y_1,\ldots,y_v,x) = SM_{\underline{k}\geq\underline{0}}\, f_{\underline{k}}(x)\, \underline{y}^{\underline{k}}$, where $f_{\underline{k}}(x) \in \mathbf{Z}[x]$. [Notice that $f_{\underline{0}}(x) = f(0,\ldots,0,x)$ and, since f is monic and $\deg_x(f) = n$, $\deg(f_{\underline{k}}) < n$ for $|\underline{k}| \geq 1$.]

[Set order for approximation:] $d \leftarrow \deg_{y_1,\ldots,y_v}(f)$; $K \leftarrow d(2n-1)$.

[Initialize for Hensel lifting:]
$a_{\underline{0}} \leftarrow BT$; $g_{\underline{0}}(x) \leftarrow x - BT$; $h_{\underline{0}}(x) \leftarrow f_{\underline{0}}(x)/g_{\underline{0}}(x) \in \mathbf{Q}(BT)[x]$.

FORALL $\underline{k}$ with $1 \leq |\underline{k}| \leq K$ DO steps (N1) and (N2). [The $\underline{k}$ must be generated in an order such that $|\underline{k}|$ is non-decreasing. We will compute polynomials $g_{\underline{k}}(x)$ and $h_{\underline{k}}(x) \in \mathbf{Q}(BT)[x]$, $\underline{k} \geq \underline{0}$, satisfying

$$\left(SM_{\underline{k}\geq\underline{0}}\, g_{\underline{k}}(x)\, \underline{y}^{\underline{k}} \right) \left(SM_{\underline{k}\geq\underline{0}}\, h_{\underline{k}}(x)\, \underline{y}^{\underline{k}} \right) = \sum_{\underline{k}\geq\underline{0}} f_{\underline{k}}(x)\underline{y}^{\underline{k}}. \qquad (1)]$$

(N1) $b_{\underline{k}}(x) \leftarrow f_{\underline{k}}(x) - \sum_{\underline{0}\leq\underline{s}\leq\underline{k}, 1\leq|\underline{s}|\leq|\underline{k}|-1} g_{\underline{s}}(x) h_{\underline{k}-\underline{s}}(x)$.

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

$$g_{\underline{0}}(x)h_{\underline{k}}(x) + h_{\underline{0}}(x)g_{\underline{k}}(x) = b_{\underline{k}}(x) \qquad (2)$$

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

$$a_{\underline{k}} \leftarrow g_{\underline{k}}(x) \leftarrow \frac{b_{\underline{k}}(BT)}{f_{\underline{0}}'(BT)}; \; h_{\underline{k}}(x) \leftarrow \frac{b_{\underline{k}}(x) - h_{\underline{0}}(x)g_{\underline{k}}(x)}{g_{\underline{0}}(x)}.$$

[Assign approximate root:] $AL_j \leftarrow SM_{0\le|\underline{k}|\le j}\ a_{\underline{k}}\ \underline{y}^{\underline{k}}$ for $0 \le j \le K$.

(L) [Find minimal polynomial for AL_K:]

[Compute powers of AL_K:]
FOR $i \leftarrow 0,\ldots,n-1$ DO $AL_K{}^{(i)} \leftarrow AL_K{}^{i} \bmod J^{K+1}$.

FOR $I \leftarrow m,\ldots,n-1$ DO
$L \leftarrow d(I+n-1)$;
With $AL_L{}^{(i)} \equiv AL_K{}^{(i)} \bmod J^{L+1}$ try to solve the equation

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

for polynomials $u_i(y_1,\ldots,y_v) \in \mathbf{Q}[y_1,\ldots,y_v]$ such that $\deg_{y_1,\ldots,y_v}(u_i) \le d$. Let $u_i(y_1,\ldots,y_v) = SM_{0\le|\underline{s}|\le d}\ u_{i,\underline{s}}\ \underline{y}^{\underline{s}}$ and let

$$AL_L{}^{(i)} = \sum_{0\le|\underline{k}|\le L} \left(\sum_{j=0}^{m-1} a_{\underline{k},j}^{(i)}\ BT^j \right)\ \underline{y}^{\underline{k}}.$$

Then (3) leads to the linear system

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

for $0 \le |\underline{k}| \le L$, $j = 0,\ldots,m-1$ in the variables $u_{i,\underline{s}}$, $i = 0,\ldots,I-1$, $0 \le |\underline{s}| \le d$. [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

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

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 $f_{\underline{0}}$ may exclude certain degrees for g. E.g., if $f_{\underline{0}}$ factors into irreducibles of even degree, then g cannot be of odd degree. (Cf. Knuth [16, p.434 and Exercise 26].)

We shall now prove the correctness of the above algorithm. We first show that step (N) computes a root $AL_K(y_1,\ldots,y_v)$ of $f(y_1,\ldots,y_v,x)$ modulo J^{K+1}. The polynomials $g_{\underline{k}}(x)$ and $h_{\underline{k}}(x) \in \mathbf{Q}(BT)[x]$, $\underline{k} \ge \underline{0}$, must satisfy (1) and thus (2). We now note that $g_{\underline{0}}(BT) = 0$ and

$h_{\underline{0}}(BT) = f_{\underline{0}}'(BT)$. The second equation follows from the fact that if BT, $BT_2,\ldots,$ BT_n are the roots of $f_{\underline{0}}(x)$ then $h_{\underline{0}}(x) = \prod_{i=2}^{n}(x-BT_i)$ and hence $h_{\underline{0}}(BT) = \prod_{i=2}^{n}(BT-BT_i) = f_{\underline{0}}'(BT)$. Therefore the unique solution of (2) with $\deg(g_{\underline{k}}) = 0$ is $a_{\underline{k}} = b_{\underline{k}}(BT)/f_{\underline{0}}'(BT)$. If we now solve (3) for $h_{\underline{k}}(x)$ we get

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

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

We now conclude that

$$f(y_1,\ldots,y_v,AL_K(y_1,\ldots,y_v)) \equiv 0 \bmod J^{K+1}$$

because

$$\left(x - \sum_{0\le|\underline{k}|\le K} a_{\underline{k}}\,\underline{y}^{\underline{k}}\right)\left(\sum_{0\le|\underline{k}|\le K} h_{\underline{k}}(x)\,\underline{y}^{\underline{k}}\right) \equiv f(y_1,\ldots,y_v,x) \bmod J^{K+1}.$$

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

$$g(y_1,\ldots,y_v,AL_L(y_1,\ldots,y_v)) \equiv 0 \bmod J^{L+1}$$

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 $g(y_1,\ldots,y_v,x)$ divide $f(y_1,\ldots,y_v,x)$ in $\mathbf{Z}[y_1,\ldots,y_v,x]$ and assume that $g(0,\ldots,0,BT) = 0$ in $\mathbf{Q}(BT)$. Then

$$g(y_1,\ldots,y_v,AL_j(y_1,\ldots,y_v)) \equiv 0 \bmod J^{j+1}$$

for all $j \ge 1$ with $AL_j(y_1,\ldots,y_v)$ as computed in step (N).

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

$$g(y_1,\ldots,y_v,AL_p(y_1,\ldots,y_v)) \not\equiv 0 \bmod J^{p+1}.$$

Because p is the first index

$$g(y_1,\ldots,y_v,AL_p(y_1,\ldots,y_v)) \equiv \sum_{|\underline{k}|=p} \gamma_{\underline{k}}\,\underline{y}^{\underline{k}} \bmod J^{p+1}$$

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

$$g(y_1,\ldots,y_v,AL_p(y_1,\ldots,y_v))\ h(y_1,\ldots,y_v,AL_p(y_1,\ldots,y_v))$$
$$\equiv \sum_{|\underline{k}|=p} \gamma_{\underline{k}} r\ \underline{y}^{\underline{k}} \not\equiv 0 \bmod J^{p+1}$$

in contradiction to $AL_p(y_1,\ldots,y_v)$ 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 $\mathbf{Z}[y_1,\ldots,y_v,x]$. 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 $f(y_1,\ldots,y_v,x)$ corresponding to AL_L also provides a solution to (3) and hence (4). Let

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

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. $0 \leq j < I$. Let $f = x^n + t_{n-1}x^{n-1} + \cdots + t_0$ and $g = x^I + u_{I-1}x^{I-1} + \cdots + u_0$ with $t_l,\ u_m \in \mathbf{Z}[y_1,\ldots,y_v]$. Using the extended Euclidean algorithm (cf. Knuth [16, p.417, Exercise 3]) we establish the existence of polynomials $U_j,\ V_j \in \mathbf{Q}(y_1,\ldots,y_v)[x]$, $\deg_x(U_j) < I-j$ 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 non-singular coefficient matrix for the linear system derived from (A) for the coefficients of $x^j, \ldots, x^{I+n-j-1}$ 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

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

(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 $s_j U_j,\ s_j V_j \in \mathbf{Z}[y_1,\ldots,y_v,x]$. Moreover,

$$f(y_1,\ldots,y_v,AL_L) \equiv g(y_1,\ldots,y_v,AL_L) \equiv 0 \bmod J^{L+1}$$

and hence

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

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

$$s_j(y_1,\ldots,y_v) \equiv 0 \bmod J^{L+1}. \tag{C}$$

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

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

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, Theorem 4.1]). However, this improvement seems not to carry over for $v \geq 2$, the reason being that $\mathbf{Q}[y_1,\ldots,y_v]$ 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 $\mathbf{Q}(BT)$ (which we shall call *ASM ops*) needed for this step. Then we bound the absolute value of all elements of $\mathbf{Q}(BT)$ 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 $\binom{v+j-1}{v-1} \leq (j+1)^{v-1}$ distinct v-dimensional integral vectors $\underline{k}$ with $|\underline{k}| = j$. The number of vectors with $|\underline{k}| \leq j$ is $\binom{v+j}{v} \leq (j+1)^v$. □

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 $\mathbf{Q}(BT)$. Clearly this bound also dominates the complexity of step (N2). Hence AL_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 AL_K in $\mathbf{Q}(BT)$.

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 $|g|$, $|h| \le 2^n |f|_2 \le \sqrt{n+1}\,2^n |f|$ and if BT is any root of f, $|BT| < 2|f|$.

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

$$|\det(M)| < T(f) = \left(n\ 2^n\ |f|\right)^{n-1}.$$

c) The resultant of g and h is bounded by $1/S(f) < |\mathrm{res}(g,h)| < 2T(f)$ 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 $BT \in \mathbf{C}$ with $|BT| \ge 2|f|$. Then

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

because $|f| \ge 1$. Therefore $f(BT) \neq 0$. 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, Sec.4.6.1, Exercise 15]) then gives the bound.

c) Let $g(x) = (x - BT_1)\cdots(x - BT_k)$ and $h(x) = (x - BT_{k+1})\cdots(x - BT_n)$. Then

$$\mathrm{res}(g, h) = \prod_{i=1,\ldots,k;\, j=k+1,\ldots,n} (BT_i - BT_j)$$

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

$$1 \le \sqrt{|\Delta|} = \left(\prod_{1 \le i < j \le k} |BT_i - BT_j|\right) |\mathrm{res}(g,h)| \left(\prod_{k+1 \le i < j \le n} |BT_i - BT_j|\right)$$

$$< |\mathrm{res}(g,h)|\ (4|f|)^{(n-1)(n-2)/2}$$

because $k(k-1) + (n-k)(n-k-1) \le (n-1)(n-2)$ for $1 \le k \le n-1$. 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 $d_{\underline{k}} = 1$ for all ν-dimensional vectors $\underline{k}$ with $|\underline{k}| = 1$ and let

$$d_{\underline{k}} = \sum_{\underline{0} \le \underline{s} \le \underline{k},\, 1 \le |\underline{s}| \le |\underline{k}| - 1} d_{\underline{s}}\ d_{\underline{k} - \underline{s}} \quad \text{for } |\underline{k}| \ge 2.$$

Then

$$d_{\underline{k}} = \frac{1}{|\underline{k}|}\left(\begin{array}{c} 2|\underline{k}|-2 \\ |\underline{k}|-1 \end{array}\right)\frac{|\underline{k}|!}{k_1!\cdots k_v!} < (4v)^{|\underline{k}|}.$$

Proof: Let $G(y_1,\ldots,y_v) = SM_{|\underline{k}|\geq 1} d_{\underline{k}}\, \underline{y}^{\underline{k}}$ be the generating function for $d_{\underline{k}}$. Then

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

and thus

$$G(y_1,\ldots,y_v) = \frac{1}{2}\left(1-\sqrt{1-4(y_1+\cdots+y_v)}\right) = \sum_{i=1}^{\infty}\frac{1}{i}\left(\begin{array}{c} 2i-2 \\ i-1 \end{array}\right)(y_1+\cdots+y_v)^i$$

which yields our formula. Since $\dfrac{|\underline{k}|!}{k_1!\cdots k_v!}$ is a multinomial coefficient, it is less than $v^{|\underline{k}|}$. Similarly the given binomial coefficient is less than $2^{2|\underline{k}|}$. □

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 section 7.

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

$$f(y_1,\ldots,y_v,x) = \left(\sum_{\underline{k}\geq\underline{0}} g_{\underline{k}}(x)\, \underline{y}^{\underline{k}}\right)\left(\sum_{\underline{k}\geq\underline{0}} h_{\underline{k}}(x)\, \underline{y}^{\underline{k}}\right).$$

Furthermore, let

$$\frac{1}{\mathrm{res}(g_{\underline{0}},h_{\underline{0}})} = \frac{1}{R}\, r(BT) \text{ with } R \in \mathbf{Z},\ r(BT) \in \mathbf{Z}[BT],$$

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

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

and, independently of which root BT of $f_{\underline{0}}$ we choose,

$$|g_{\underline{k}}|,\ |h_{\underline{k}}| \leq d_{\underline{k}}\left(N(f)\, S(f_{\underline{0}})\, T(f_{\underline{0}})\right)^{2|\underline{k}|-1}.$$

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

$$|g_{\underline{s}}\ h_{\underline{k}-\underline{s}}| \le (n-1)\,|g_{\underline{s}}|\ |h_{\underline{k}-\underline{s}}| \le (n-1)\ C_{\underline{s}}\ C_{\underline{k}-\underline{s}}.$$

By definition $C_{\underline{s}} \ge |f|$ and thus we obtain from (N1)

$$D_{\underline{k}} \le n \sum_{\underline{0} \le \underline{s} \le \underline{k}, 1 \le |\underline{s}| \le |\underline{k}|-1} C_{\underline{s}}\ C_{\underline{k}-\underline{s}}. \tag{A}$$

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

$$(\vec{h_{\underline{k}}}, \vec{g_{\underline{k}}})\ \mathrm{Syl}(g_{\underline{0}},h_{\underline{0}}) = \vec{b_{\underline{k}}}, \tag{B}$$

where $(\vec{h_{\underline{k}}}, \vec{g_{\underline{k}}})$ denotes the vector obtained by concatenation of the vectors $\vec{h_{\underline{k}}}$ and $\vec{g_{\underline{k}}}$. Using Cramer's rule for (B) and the fact that

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

(by lemma 5c), we get the estimate

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

(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 $R\ g_{\underline{k}}, R\ h_{\underline{k}} \in (\mathbf{Z}[BT])[x]$. (Notice that BT is an algebraic integer.) Also $D_{\underline{k}} \le |f|$ and hence by (C)

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

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

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

By (C) we finally obtain

$$C_{\underline{k}} \le \max(|f|, n\ D_{\underline{k}}\ S(f_{\underline{0}})\ T(f_{\underline{0}}))$$

$$\leq d_{\underline{k}} \frac{n^2}{N(f)} (N(f)\, S(f_{\underline{0}})\, T(f_{\underline{0}}))^{2|\underline{k}|-1}$$

$$\leq d_{\underline{k}} (N(f)\, S(f_{\underline{0}})\, T(f_{\underline{0}}))^{2|\underline{k}|-1}. \quad \square$$

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

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

From the lemmas 5 and 6 we obtain

$$|AL_K| \leq B_1(f) = (4v)^K \left(n^2 |f| \, (4|f|)^{n^2/2} \, 2^{n^2} (n|f|)^n \right)^{2K-1}$$

$$< (4v)^K \, (2n|f|)^{2Kn^2}, \tag{4}$$

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

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

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

where t is the minimal polynomial of BT. Let $BT_2, \ldots, BT_n$ be the roots of $h_{\underline{0}}$. Then

$$\operatorname{res}(g_{\underline{0}}, h_{\underline{0}}) = \prod_{i=2}^{n} (BT - BT_i) = f_{\underline{0}}'(BT).$$

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

$$|R| \leq \left(\sqrt{(m+1)(n+1)}\, 2^n |f_{\underline{0}}| \right)^{n-1} \left(\sqrt{n}\, n |f_{\underline{0}}| \right)^m$$

$$< \left((n+1)\, 2^n \, |f_{\underline{0}}| \right)^{m+n} < (2n|f|)^{n^3/2}, \tag{5}$$

for $n \geq 4$. 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

$$R^{2|\underline{k}|-1} a_{\underline{k}} \in \mathbf{Z}[BT] \text{ for } 1 \leq |\underline{k}| \leq K. \tag{6}$$

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

Lemma 7: Let $AL_K^{(i)} = SM_{\underline{0} \le |\underline{k}| \le K}\ a_{\underline{k}}^{(i)}\ \underline{y}^{\underline{k}}$ for $2 \le i \le n-1$, then

$$|a_{\underline{k}}^{(i)}| \le (K+1)^{\nu(i-1)} B_1(f)^i \text{ and } R^{2|\underline{k}|-1} a_{\underline{k}}^{(i)} \in \mathbf{Z}[BT],$$

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

Proof: It is easy to show that

$$a_{\underline{k}}^{(i+1)} = \sum_{0 \le \underline{s} \le \underline{k}} a_{\underline{s}}^{(i)}\ a_{\underline{k}-\underline{s}},\ 0 \le |\underline{k}| \le K,\ i \ge 1,$$

where there are, by lemma 4, at most $(|\underline{k}|+1)^\nu \le (K+1)^\nu$ terms under the right hand sum. The lemma now follows by induction on i. □

Therefore we get from (4) for all $0 \le i \le n-1$ and for $n \ge 4$

$$|AL_K^{(i)}| \le B_2(f) = ((K+1)^\nu B_1(f))^{n-1} < 2^{3\nu nK}\ (2n|f|)^{2K(n^3-n^2)}. \tag{7}$$

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 $AL_K^{(i)}$, $1 \le i \le n-1$. To do this, we shall state a useful lemma.

Lemma 8: Let BT 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 of BT. Assume that

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

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

$$|c_i| \le \frac{C\ m!\ A^{m(m-1)/2}}{\sqrt{D}},\ 0 \le i < m.$$

(Cf. Weinberger and Rothschild [31, Lemma 8.3].) □

In our case, we can choose $A = 2|f_{\underline{0}}|$, by lemma 5a), $C = B_2(f)\ R^{2K-1}$, and $D \ge 1$. 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

$$B_3(f,m) = R^{2K-1}\ B_2(f)\ m!\ (2|f_{\underline{0}}|)^{m(m-1)/2} < 2^{3\nu nK}\ (2n|f|)^{3Kn^3}, \tag{8}$$

using (5), (7) and $n \ge 4$. 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 $\mathbf{Q}(BT)$ means adding or subtracting the numerators of polynomials in $\mathbf{Q}[BT]$ of degree $m-1$, after eventually multiplying them with a power of R to produce a common denominator. Multiplication in $\mathbf{Q}(BT)$ is multiplication of $m-1$ degree polynomials in $\mathbf{Q}[BT]$ followed by a remainder computation w.r.t. $t(BT)$. 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 $p = m\binom{\nu+K}{K} \leq m(K+1)^{\nu}$ equations in $q = I\binom{\nu+d}{d} \leq (n-1)(d+1)^{\nu}$ 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

$$O(m\ n^{\nu+3}\ d^{3\nu}). \tag{9}$$

From the previous analysis, we know that all $a_{\underline{k},j}^{(i)}$ can be brought to the common denominator R^{2K-1} and their numerators, $\mathrm{num}(a_{\underline{k},j}^{(i)})$, then satisfy $|\mathrm{num}(a_{\underline{k},j}^{(i)})| \leq B_3(f,m)$. 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

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

whose logarithm is by (8) of order

$$\log(B_4(f,m)) = O(d^{\nu+1}\ \nu n^5 \log(n|f|)). \tag{10}$$

Hence, step (L) also takes at most polynomial-time in $\deg(f)$ and $\log(|f|)$. Notice that (9) and (10) 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 Irreducibility Testing

As we have seen in section 5, in order to establish the irreducibility of the polynomial f by algorithm 2 we need to factor $f_{\underline{0}}$. Reducibility of $f_{\underline{0}}$ does, of course, not imply reducibility of f. The following theorem partially fills this gap by constructing from a polynomial $f(y_1,\ldots,y_\nu,x)$, monic in x with $f(0,\ldots,0,x)$ 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 $t(y_1,\ldots,y_\nu) \in \mathbf{Z}[y_1,\ldots,y_\nu]$ be a non-zero polynomial. Then $t(y_1,cy_1,y_3,\ldots,y_\nu) \neq 0$ for any integer c with $|c| \geq 2|t|$.

Proof: Let $ay_1^{e_1}\cdots y_v^{e_v}$ be a monomial in t with $a \neq 0$. Then $t(y_1,cy_1,\ldots,y_v)$ contains the monomial $b(c)y_1^{e_1+e_2}y_3^{e_3}\cdots y_v^{e_v}$ 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 $|b| \leq |t|$ we conclude that $b(c) \neq 0$ for any integer of the stated size. □

Theorem 3: Let $f(y_1,\ldots,y_v,x) \in \mathbf{Z}[y_1,\ldots,y_v,x]$ be monic of degree n in x such that $f_{\underline{0}} = f(0,\ldots,0,x)$ is squarefree. Let $T(f_{\underline{0}})$ be as in lemma 5b, and let $N(f)$ be as in theorem 2. Furthermore, assume that $f(y_1,\ldots,y_v,x)$ is irreducible. Finally let $d = \deg_{y_1,\ldots,y_v}(f)$. Then for any integer c with

$$|c| \geq B_5(f) = 2\,(4v)^{2d}(2\,N(f)\,T(f_{\underline{0}})^2)^{4d-1}$$

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

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

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

Then each factor of $g_c(y_1,\, y_3,\ldots,x) \in \mathbf{Q}[[y_1,\, y_3,\ldots,y_v]][x]$ corresponds to a factor of $f(y_1,\, y_2,\ldots,x) \in \mathbf{Q}[[y_1,\, y_2,\ldots,y_v]][x]$ 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 $g_c(0,\ldots,0,x) \in \mathbf{Q}[x]$. But this is impossible due to the uniqueness of the Hensel lifting procedure as proven in theorem 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 $h(y_1,y_2,\ldots,x)$ of $f(y_1,y_2,\ldots,x) \in \mathbf{Q}[[y_1,\ldots,\, y_v]][x]$ contains at least one monomial $b_{\underline{p},m}\,\underline{y}^{\underline{p}}\,x^m$ with $b_{\underline{p},m} \neq 0$ and $d < |\underline{p}| \leq 2d$. From it we get a polynomial coefficient of x^m in h whose total degree in $y_1,\ldots,y_v$ equals $|\underline{p}|$. By choosing c sufficiently large (cf. lemma 9) we will be able to preserve this coefficient throughout $h_c = h(y_1,cy_1,\ldots,x)$. Hence such an h_c contains a monomial in $y_1, y_3,\ldots,y_v$ of total degree $|\underline{p}| > d$. Therefore h_c cannot be a polynomial dividing g_c for otherwise its total degree in $y_1, y_3,\ldots,y_v$ could not be larger than d.

Let

$$h(y_1,\ldots,y_v,x) = \sum_{i=0}^{l} \sum_{\underline{k}\geq\underline{0}} b_{\underline{k},i}\;\underline{y}^{\underline{k}}\;x^i$$

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

$$\bar{h}(y_1,\ldots,y_v,x) = \sum_{i=0}^{n-l} \sum_{\underline{k}\geq\underline{0}} \bar{b}_{\underline{k},i}\;\underline{y}^{\underline{k}}\;x^i$$

† I owe this argument to Prof. Hendrik W. Lenstra, Jr.

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

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

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

Now there must exist at least one $b_{\underline{k},i}$ or $\bar{b}_{\underline{k},i}$ with

$$d < |\underline{k}| \le 2d \text{ and } \left(b_{\underline{k},i} \neq 0 \text{ or } \bar{b}_{\underline{k},i} \neq 0 \right).$$

To see this, assume the contrary. Then

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

since no monomial $a\, \underline{y}^{\underline{k}}\, x^i$, a a nonzero rational, with $d < |\underline{k}| \le 2d$ 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 $\underline{y}$ of degree larger than d. But this contradicts the fact that f is irreducible. Without loss of generality we now can assume the existence of a vector $\underline{p}$ and an integer m such that

$$b_{\underline{p},m} \neq 0 \text{ with } d < |\underline{p}| \le 2d \text{ and } 0 \le m \le l.$$

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

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

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

We now apply theorem 2 with $BT = 1$, $g_{\underline{0}}(x) = h(0,\ldots,0,x) \in \mathbf{Z}[x]$ and $h_{\underline{0}}(x) = \bar{h}(0,\ldots,0,x) \in \mathbf{Z}[x]$. First notice that, since $f_{\underline{0}}$ is squarefree, $0 \neq R = \mathrm{res}(g_{\underline{0}},h_{\underline{0}}) \in \mathbf{Z}$ and hence $1/|R| \le 1$ meaning that we can set $S(f_{\underline{0}}) = 1$. Secondly,

$$|b_{\underline{j},m}| \le |g_{\underline{j}}| \le (4v)^{|\underline{j}|}(N(f)\,T(f_{\underline{0}}))^{2|\underline{j}|-1} \le (4v)^{2d}(N(f)\,T(f_{\underline{0}}))^{4d-1}$$

because of lemma 6 and $|\underline{j}| = |\underline{p}| \le 2d$. Finally,

$$R^{2|\underline{j}|-1} b_{\underline{j},m} \in \mathbf{Z} \text{ and } R^{2|\underline{j}|-1} \le R^{4d-1} < (2T(f_{\underline{0}}))^{4d-1},$$

the last inequality by lemma 5c. In summary,

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

and

$$|R^{4d-1}\, t_{\underline{p},m}| < (4v)^{2d}(2N(f)\,T(f_{\underline{0}})^2)^{4d-1} = \frac{1}{2} B_5(f).$$

From lemma 9 we now conclude that for any integer at least $B_5(f)$

$$t_{\underline{p},m}(y_1,cy_1,y_3,\ldots,y_v) \neq 0.$$

Therefore $h(y_1,cy_1,y_3,\ldots,x)$ contains a non-zero monomial in y_1, y_3 ,…, y_v of total degree

larger than d and cannot be a polynomial factor of $f(y_1, cy_1, y_3,\ldots,x)$, 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 bounds $c_1,\ldots, c_{v-1}$ such that for the sequence of polynomials $f_1 = f$,

$$f_2(y_1,y_3,\ldots,x) = f_1(y_1,c_1y_1,y_3,\ldots,x),$$

$$f_3(y_1,y_4,\ldots,x) = f_2(y_1,c_2y_1,y_4,\ldots,x),\ldots,$$

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

we have $c_i \geq B_5(f_i)$ for all $1 \leq i \leq v-1$. 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 $f = h_1h_2$ then

$$g(y_1,x) = h_1(y_1,c_1y_1,\ldots,c_{v-1}y_1,x)\ h_2(y_1,c_1y_1,\ldots,c_{v-1}y_1,x).$$

One can prove theorem 3 for the more general substitution $y_2 = c\,y_1^s$, 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 substitution 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, Theorem 4]).

The type of substitution $y_2 = c\,y_1^s$ 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 section 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 section 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, Sec. 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: Does there exist a polynomial $p(d,v)$ and an infinite sequence of polynomials $f(x_1,\ldots,x_v) \in \mathbf{Z}[x_1,\ldots,x_v]$ with the following property: Any f in the sequence contains less than $p(d(f),v)$ monomials with non-zero coefficients where

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

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 non-zero 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 strongely effective version of the Hilbert Irreducibility Theorem.

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

Acknowledgement

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 section 3 were computed on the MACSYMA system.

References

[1] Brown, W.S.: On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors. J. ACM **18,** 478-504 (1971).

[2] Brown, W.S., Traub, J.F.: On Euclid's Algorithm and the Theory of Subresultants. J. ACM **18,** 505-514 (1971).

[3] Chistov, A.L., Grigoryev, D.Y.: Polynomial-Time Factoring of the Multivariable Polynomials over a Global Field. Lomi preprint E-5-82, Leningrad 1982.

[4] Dörge, K.: Zum Hilbertschen Irreduzibilitätssatz. Mathematische Annalen **95,** 84-97 (1926).

[5] Franz, W.: Untersuchungen zum Hilbertschen Irreduzibilitätssatz. Math. Zeitschr. **33,** 275-293 (1931).

[6] Gantmacher, F. R.: Matrix Theory, vol. 1. New York: Chelsea 1959.

[7] von zur Gathen, J.: Factoring Sparse Multivariate Polynomials. Proc. 1983 Symp. Foundations Comp. Sci. IEEE, 172-197 (1983).

[8] von zur Gathen, J., Kaltofen, E.: A Polynomial-Time Algorithm for Factoring Multivariate Polynomials Over Finite Fields. Proc. 1983 Internat. Conference on Automata, Languages and Programming. Springer Lec. Notes Comp. Sci. **154**, 250-263.

[9] Gel'fond, A. O.: Transcendental and Algebraic Numbers. New York: Dover Publ. 1960.

[10] Hardy, G. H., Wright, E.M.: An Introduction to the Theory of Numbers, 5th ed. Oxford Univ. Press 1979.

[11] Hilbert, D.: Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. Journal für die reine und angewandte Mathematik **110,** 104-29 (1892).

[12] Kaltofen, E.: A Polynomial Reduction from Multivariate to Bivariate Integral Polynomial Factorization. Proc. 1982 ACM Symp. Theory Comp., 261-266.

[13] Kaltofen, E.: A Polynomial-Time Reduction from Bivariate to Univariate Integral Polynomial Factorization. Proceedings 23rd Symposium on Foundations of Computer Science. IEEE, 57-64 (1982).

[14] Kaltofen, E.: On the Complexity of Factoring Polynomials with Integer Coefficients. Ph.D. thesis, Rensselaer Polytechnic Institute, December 1982.

[15] Kaltofen, E.: On the Complexity of Finding Short Vectors in an Integer Lattice. Proc. 1983 European Comp. Algebra Conf. Springer Lec. Notes Comp. Sci., to appear.

[16] Knuth, D. E.: The Art of Computer Programming, vol.2, Seminumerical Algorithms, 2nd ed. Reading, MA: Addison Wesley 1981.

[17] Kronecker, L.: Grundzüge einer arithmetischen Theorie der algebraischen Grössen. J. f. d. reine u. angew. Math. **92,** 1-122 (1882).

[18] Kung, H. T., Traub, J. F.: All Algebraic Functions Can Be Computed Fast. J. ACM **25,** 245-260 (1978).

[19] Landau, S.: Factoring Polynomials over Algebraic Number Fields is in Polynomial Time. SIAM J. Comp., to appear.

[20] Lenstra, A.K.: Factoring Polynomials over Algebraic Number Fields. Manuscript 1982.

[21] Lenstra, A.K.: Factoring Multivariate Polynomials over a Finite Field. Proc. 1983 ACM Symp. Theory Comp., 189-192.

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

[23] McClellan, M. T.: The Exact Solution of Systems of Linear Equations with Polynomial Coefficients. J. ACM **20,** 563-588 (1973).

[24] Mignotte, M.: An Inequality about Factors of Polynomials. Math. Comp. **28,** 1153-1157 (1974).

[25] Moses, J., Yun, D. Y. Y.: The EZGCD Algorithm. Proc. 1973 ACM National Conf., 159-166.

[26] Musser, D. R.: Multivariate Polynomial Factorization. J. ACM **22,** 291-308 (1976).

[27] Trager, B. M.: Algebraic Factoring and Rational Function Integration. In Jenks, R. (ed.): Proc. ACM Symp. on Symbolic and Algebraic Comp. 1976. ACM, 219-226.

[28] van der Waerden, B. L.: Modern Algebra, vol.1. Engl. transl. by F. Blum. New York: Ungar Publ. 1953.

[29] Wang, P. S.: An Improved Multivariate Polynomial Factoring Algorithm. Math. Comp. **32,** 1215-1231 (1978).

[30] Wang, P. S., Trager, B. M.: New Algorithms for Polynomial Square-free Decomposition over the Integers. SIAM J. Comp. **8,** 300-305 (1979).

[31] Weinberger, P. J., Rothschild, L. P.: Factoring Polynomials over Algebraic Number Fields. ACM Trans. Math. Software **2,** 335-350 (1976).

[32] Yun, D. Y. Y.: On Squarefree Decomposition Algorithms. In Jenks, R. (ed.): Proc. ACM Symp. on Symbolic and Algebraic Comp. 1976. ACM, 26-35.

[33] Yun, D. Y. Y.: On the Equivalence of Polynomial GCD and Squarefree Factorization Problems. Proc. MACSYMA Users' Conf. 77. Washington, D.C.: NASA 1977, 65-70.

[34] Zassenhaus, H.: Polynomial Time Factoring of Integral Polynomials. ACM SIGSAM Bulletin **15,** 6-7, (May 1981).

[35] Zippel, R. E.: Probabilistic Algorithms for Sparse Polynomials. Ph.D. thesis, MIT 1979.

References