Appears in *Journal of Computer and System Sciences*, **50**/2 pp. 274–295 (1995).

Effective Noether Irreducibility Forms and Applications*

Erich Kaltofen

Department of Computer Science, Rensselaer Polytechnic Institute
Troy, New York 12180-3590; Inter-Net: `kaltofen@cs.rpi.edu`

Abstract. Using recent absolute irreducibility testing algorithms, we derive new irreducibility forms. These are integer polynomials in variables which are the generic coefficients of a multivariate polynomial of a given degree. A (multivariate) polynomial over a specific field is said to be absolutely irreducible if it is irreducible over the algebraic closure of its coefficient field. A specific polynomial of a certain degree is absolutely irreducible, if and only if all the corresponding irreducibility forms vanish when evaluated at the coefficients of the specific polynomial. Our forms have much smaller degrees and coefficients than the forms derived originally by Emmy Noether. We can also apply our estimates to derive more effective versions of irreducibility theorems by Ostrowski and Deuring, and of the Hilbert irreducibility theorem. We also give an effective estimate on the diameter of the neighborhood of an absolutely irreducible polynomial with respect to the coefficient space in which absolute irreducibility is preserved. Furthermore, we can apply the effective estimates to derive several factorization results in parallel computational complexity theory: we show how to compute arbitrary high precision approximations of the complex factors of a multivariate integral polynomial, and how to count the number of absolutely irreducible factors of a multivariate polynomial with coefficients in a rational function field, both in the complexity class $\mathcal{NC}$. The factorization results also extend to the case where the coefficient field is a function field.

Table of Contents

*This material is based on work supported in part by the National Science Foundation under Grant No. CCR-90-06077 and under Grant No. CDA-88-05910. Some of the results presented here were first announced at the *Purdue Conference on Algebraic Geometry and Its Applications*, held in honor of S. Abhyankar's 60th birthday in June 1990. An extended abstract of this paper appears in the Proc. 1991 ACM Symp. Theory Comput., ACM Press, 54–63 (May 1991). Several improvements, especially to §9, were made while the author was on sabbatical leave at the Department of Computer Science at the University of Toronto in Spring 1991.

1. Introduction

Emmy Noether proved in 1922 that one can test a multivariate polynomial over an arbitrary field for irreducibility over the algebraic closure of that coefficient field by arithmetic in the coefficient field itself; that is, the problem is a purely rational question. More precisely, she established the existence of finitely many integral polynomials in the indeterminate coefficients of a generic multivariate polynomial of a given degree, the so-called *irreducibility forms*, such that a specific polynomial is absolutely reducible, or possibly of smaller degree, if and only if all the irreducibility forms vanish on its coefficients. For coefficient fields of positive characteristic, the integer coefficients of the forms are to be taken modulo the characteristic (Noether 1922). Schmidt (1976) has analyzed Noether's construction and obtained estimates on the degrees and coefficient sizes of these forms. Since Noether's proof is based on elimination theory applied to the coefficients of a possible factorization, it appears unavoidable using her approach that the degrees of the forms could be less than single exponential in the degree of the polynomial under consideration.

The development of polynomial-time multivariate polynomial factorization algorithms has lead to new approaches for absolute irreducibility testing and factorization (Heintz and Sieveking 1981), (Davenport and Trager 1981), (Chistov and Grigoryev 1983), (Trager 1984, Chapter 3, Section 2), (Dicrescenzo and Duval 1984), (Kaltofen 1985b), (von zur Gathen 1985), (Dvornicich and Traverso 1987), and (Bajaj et al. 1989). Our 1985 algorithm, in fact, leads to an absolute irreducibility test based solely on coefficient field arithmetic, at least for perfect fields. The same has also been established for Duval's approach using the lazy evaluation model for algebraic number arithmetic (Duval 1990). A minor modification to our 1985 algorithm and the well-known technique of transcendental field extensions for enforcing the input specifications makes it possible to derive irreducibility forms from our algorithm. As a consequence, we have an absolute irreducibility test that uses only rational field operations for any coefficient field. Note that irreducibility over an arbitrary coefficient field itself cannot be decided by arithmetic alone[1] (van der Waerden 1930). It is the objective of this article to derive effective bounds on the degrees and coefficient sizes of these new irreducibility forms. To this end, we need to analyze the degree and coefficient size growth when executing the algorithm on generic inputs; that is, polynomials in which the coefficients are indeterminates themselves. If d is the total degree of the n-variate polynomials considered, then as a crude estimate (see Theorem 7 for the precise values) our forms have degree $O(d^6)$ with integer coefficients with $O((d^7 + d^6 n) \log d)$ digits, and there are $2^{(d+n)^{O(1)}}$ such forms.

The analysis of our algorithms for generic inputs is important not only for the size bounds of the derived forms, but also for the bit complexity of the algorithms themselves. While in the papers cited earlier the algorithmic bit complexity is always stated with respect to a particular coefficient field data structure, say an algebraic extension of the rational numbers in Kronecker representation, we can deduce from our size estimates for generic inputs complexity statements for abstract coefficient fields. We suppose that all arithmetic operations, that is $+$, $-$, $\times$, $\div$, and $= 0?$, on field elements of a given bit-size can be performed in time polynomial in that size. The conclusion then is that our absolute irreducibility test is also of polynomial-time bit complexity; that is, the size of all intermediate values stays

[1] This fact is fully studied in Fröhlich and Shepherdson (1955). The reference to van der Waerden's foreseeing article was brought to my attention by Joachim von zur Gathen.

polynomially bounded. Of course, the actual element representation must be canonical with respect to the arithmetic operations,[2] and the bit-size of the result of an arithmetic operation must only grow as a linear function in the combined bit-sizes of the operands. An example for the latter would be the bound

$$\text{bit-size}(a \times b) = O(\text{bit-size}(a) + \text{bit-size}(b) + 1).$$

The effective irreducibility forms have consequences to effective versions of at least two more theorems. One, already derived in Noether's 1922 article, is a theorem by Ostrowski (1919) on mapping an absolutely irreducible polynomial with algebraic number coefficients into a finite field by taking the coefficient modulo a prime ideal in the algebraic number ring. We derive effective upper bounds on the first rational prime p that preserves absolute irreducibility for any prime ideal lying above p, and for the last prime that might violate good reduction. Furthermore, we derive a corresponding theorem for extensions by algebraic functions.

It also follows from the Noether irreducibility forms that a polynomial whose coefficients are sufficiently near to the coefficients of an absolute irreducible polynomial has to remain absolutely irreducible. Using our effective forms, we can derive a lower bound in terms of the degree and absolute values of the coefficients, assuming that they lie in an algebraic number ring, of the largest common distance to each coefficient such that absolute irreducibility is preserved.

The effective estimates in our theorems are facilitated by a new effective version of the Hilbert irreducibility theorem: substituting affine linear forms in two variables for the variables in a multivariate irreducible polynomial over a perfect field can be shown to preserve irreducibility in almost all cases (Hilbert 1892, Theorem on bottom of p. 117). In fact, irreducibility is not preserved with probability $2d^4/\text{card}(S)$, where d is the degree of the multivariate preimage and $\text{card}(S)$ is the cardinality of the set S from which the coefficients for the bivariate linear forms are uniformly selected. The proof of the theorem is purely algebraic, based on the multivariate factorization algorithm in (Kaltofen 1985a) and a substitution used in (Kaltofen and Trager 1990). The failure probability comes within a constant factor to the one proven by Bajaj et al. (1989) for the case that the coefficients are complex numbers, who use the geometry of the corresponding complex algebraic variety.

We also give two complexity theoretic applications of our effective size analyses. First, we consider the problem of computing arbitrary precision floating point approximations to the complex factors of multivariate integer polynomials. The computational complexity class to which our algorithms are to belong is the class $\mathcal{NC}$ of Boolean circuits of poly-logarithmic delay and polynomial gate count (see (Cook 1985) for a definition of this class). Since the multivariate problem is a generalization of the univariate one, the problem of finding arbitrary precision approximations to the complex roots of a univariate integer polynomial must be established to be in $\mathcal{NC}$. In fact, our solution reduces the multivariate problem to the univariate one, which has recently been solved (Neff 1990).

[2] A famous counter-example otherwise is that of computing polynomial GCDs using quotient field arithmetic without reducing numerators and denominators by a common factor, which results in exponential bit complexity for an algorithm with quadratic arithmetic complexity (Knuth 1981, p. 414, Eq. (27)).

Our parallel algorithms are based on a new representation for elements in algebraic number fields. It is based on the "lazy factorization" model of algebraic numbers, introduced by Dicrescenzo and Duval (1987), that modifies the Kronecker model of representing algebraic numbers in a polynomial algebra modulo a minimal polynomial by allowing reducible defining equations for the algebraic numbers generating the number fields. This model, however, is not an abstract data type for a field: one cannot generally test elements for equality. We amend this model — in the spirit of Collins (1975) — by associating with each number field generator a complex high precision floating point number that isolates a root of the defining equation (cf. (Lombardi 1989)). We now can treat the coefficient number field as an abstract field and apply the modern theory of multivariate factorization (Kaltofen and Trager 1990) or sparse polynomial interpolation (Ben-Or and Tiwari 1988) to such polynomials. Thus we can obtain, for instance, arbitrary precision approximations to all sparse complex factors of a sparse multivariate integral polynomial, within a randomized version of the complexity class $\mathcal{NC}$. The constructed Boolean circuit has a delay that is of the order of a polynomial in the *logarithm* of the number of variables, the coefficient size, the number of non-zero monomials in the input and in the sparse factors, and of the number of digits in the precision. Using our effective theorem on absolute irreducibility within a neighborhood, we can even guarantee that the approximate factors cannot split further over the complex numbers.

The second result considers the problem of counting the number of factors of a multivariate polynomial whose coefficients lie in a rational function field over the rational numbers. We show how to enumerate all absolutely irreducible factors within $\mathcal{NC}$ by employing our function field counterpart of the effective Ostrowski theorem. With the lazy factorization model for algebraic extensions of a rational function field it becomes similarly possible to compute high order truncated power series approximations to the coefficients of the absolutely irreducible factors of a multivariate polynomial with rational function coefficients.

Notation: The symbols $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{C}$, denote the sets of integers, rational numbers, and complex numbers, respectively. By $\overline{\mathsf{K}}$ we denote the algebraic closure of a field K, and by $\mathrm{QF}(\mathsf{D})$ the field of quotients of an integral domain D. We use the symbols := and =: to define new mathematical objects (the new quantities being on the side of the colon), and we use the symbols $\leftarrow$ and $\rightarrow$ as assignment operators in program code. When describing algorithms, we typeset the actual algorithmic instructions in *slanted font*, and to further distinguish it from the commentary explanations, we use imperative mode.

For a multivariate polynomial

$$f(X_1, \ldots, X_n) = \sum_{e_1 \geq 0, \ldots, e_n \geq 0} q_{e_1,\ldots,e_n} X_1^{e_1} \cdots X_n^{e_n},$$

$\deg(f) := \max\{e_1 + \cdots + e_n \mid q_{e_1,\ldots,e_n} \neq 0\}$ always denotes its total degree. If the coefficients $q_{e_1,\ldots,e_n}$ are complex numbers and $|q_{e_1,\ldots,e_n}|$ their absolute value, we have the notion of a p-norm,

$$\|f\|_p := \left(\sum_{e_1 \geq 0, \ldots, e_n \geq 0} |q_{e_1,\ldots,e_n}|^p \right)^{1/p}.$$

In particular, $\|f\|_\infty = \max_{e_1,\ldots,e_n}\{|q_{e_1,\ldots,e_n}|\}$. We shall say that either f factors *over* K or that f factors *in* $\mathsf{K}[X_1, \ldots, X_n]$. Finally, we will use the operator mod in two ways, first to

indicate a congruence, as in $f \equiv g \pmod{h}$, where f, g, h are univariate polynomials, for instance, and second as the function that computes the canonical representative $(f \bmod h)$ of f with respect to h, say the remainder of the univariate polynomial f divided by h.

2. Factoring over the Algebraic Closure

In the following we review the multivariate factorization algorithms presented in (Kaltofen 1985a and 1985b), with the slight generalization to arbitrary characteristic for the coefficient field K. The algorithms require a good starting point for the used Newton root approximation algorithm, and therefore restrict the input polynomials somewhat. We will show in §5 how this input restriction can be removed by preconditioning.

The first algorithm is the one presented in (Kaltofen 1985a) for factoring over the coefficient field.

Algorithm *Factorization over the Coefficient Field*

Input: $f(x,y) \in \mathsf{K}[x,y]$ monic in x, $d := \deg_x(f)$, K an arbitrary field, such that the resultant

$$\mathrm{Res}_x(f(x,0),\, \partial f(x,0)/\partial x) \neq 0. \tag{1}$$

Output: Either f will be certified to be irreducible in $\mathsf{K}[x,y]$; or the algorithm returns a list of irreducible polynomial factors of $f(x,y)$.

The idea of the algorithm is to compute the approximation of a root of $f(x,y)$ in $\overline{\mathsf{K}}[[y]]$, and then find the corresponding minimal polynomial in $\mathsf{K}[x,y]$.

Set the maximum order of the approximation needed,

$$\ell_{\max} \leftarrow 2\,(d-1)\,\deg_y(f).$$

For all roots $\zeta_i \in \overline{\mathsf{K}}$ of $f(x,0) \in \mathsf{K}[x]$ Do Steps N and L.

Step N: Let $\mathsf{L}_i := \mathsf{K}(\zeta_i)$.

Set the initial points for the Newton iteration

$$\alpha_{i,0} \leftarrow \zeta_i \in \mathsf{L}_i, \quad \beta_{i,0} \leftarrow \frac{1}{(\partial f/\partial x)\,(\alpha_{i,0},0)} \in \mathsf{L}_i.$$

Notice that $(\partial f/\partial x)(\alpha_{i,0},0) \neq 0$ because of the input assumption (1).

We now perform Newton iteration with quadratic convergence (see (Lipson 1983, Chapter IX, §3.3)).

For $j \leftarrow 0, \ldots, \lfloor \log_2(\ell_{\max}) \rfloor$ Do {

$$\alpha_{i,j+1} \leftarrow \Big(\alpha_{i,j} - \beta_{i,j} f(\alpha_{i,j}, y)\Big) \bmod y^{2^{j+1}};$$

$$\beta_{i,j+1} \leftarrow \left(2\beta_{i,j} - \frac{\partial f}{\partial x}(\alpha_{i,j+1}, y)\beta_{i,j}^2\right) \bmod y^{2^{j+1}}.$$

Notice that $\alpha_{i,j+1}$ and $\beta_{i,j+1}$ are polynomials in $\mathsf{L}_i[y]$ with

$$f(\alpha_{i,j+1}, y) \equiv 0 \pmod{y^{2^{j+1}}}, \quad \beta_{i,j+1}\,\frac{\partial f}{\partial x}(\alpha_{i,j+1}, y) \equiv 1 \pmod{y^{2^{j+1}}}. \quad \}$$

Set the approximated root

$$\alpha_i \leftarrow \alpha_{i,\lfloor \log_2(\ell_{\max})\rfloor+1} \bmod y^{\ell_{\max}+1} \in \mathsf{L}_i[y].$$

Next, we compute powers of α_i.
For $\mu \leftarrow 0, \ldots, d-1$ *Do*

$$\sum_{k=0}^{\ell_{\max}} a_{i,k}^{(\mu)} y^k \leftarrow (\alpha_i^\mu \bmod y^{\ell_{\max}+1}), \quad \textit{where } a_{i,k}^{(\mu)} \in \mathsf{L}_i.$$

Step L: We now find the lowest degree polynomial in $\mathsf{K}[x,y]$ whose root is α_i.
For $m \leftarrow 1, \ldots, d-1$ *Do*

{Here we try to find a polynomial in $\mathsf{K}[x,y]$ of degree m in x that α_i satisfies to a certain order.

Set the needed order of approximation

$$\ell \leftarrow \deg_y(f)(m+d-1).$$

We examine whether the equation

$$\alpha_i^m + \sum_{\mu=0}^{m-1} h_{i,\mu}(y)\alpha_i^\mu \equiv 0 \pmod{y^{\ell+1}},$$

has a solution for $h_{i,\mu}(y) \in \mathsf{K}[y]$ with $\deg(h_{i,\mu}) \le \deg_y(f)$. By choosing an indeterminate 'Ansatz' for the coefficients of $h_{i,\mu}$,

$$h_{i,\mu}(y) =: \sum_{\delta=0}^{\deg_y(f)} u_{i,\mu,\delta}\, y^\delta, \quad u_{i,\mu,\delta} \in \mathsf{K},$$

and collecting the coefficients of y^k, we are led to the following problem.
Solve the linear system over the field K,

$$a_{i,k}^{(m)} + \sum_{\mu=0}^{m-1} \sum_{\delta=0}^{\deg_y(f)} a_{i,k-\delta}^{(\mu)} u_{i,\mu,\delta} = 0, \quad a_{i,\nu}^{(\mu)} = 0 \textit{ for } \nu < 0, \tag{2}$$

for $0 \le k \le \ell$ *in the variables* $u_{i,\mu,\delta}$, $0 \le \mu \le m-1$, $0 \le \delta \le \deg_y(f)$. Notice that if the system (2) has a solution in K, then that solution is unique (see (Kaltofen 1985a), Theorem 1). *If the system has a solution, then set*

$$f_i(x,y) \leftarrow x^m + \sum_{\mu=0}^{m-1} \sum_{\delta=0}^{\deg_y(f)} u_{i,\mu,\delta} y^\delta x^\mu.$$

The polynomial $f_i(x,y)$ is now an irreducible factor of $f(x,y)$. *Check if* f_i *has been produced by a previous root* ζ_ι, $\iota < i$. *If not, add* f_i *to the list of irreducible factors.*

If the system (2) has no solution and $i = 1$ and $m = d - 1$, then designate f irreducible in $\mathsf{K}[x, y]$ and exit the algorithm. } □

The problem arises how to represent elements in L_i, including ζ_i, such that one can solve (2) over K. One solution, which leads to the original polynomial-time reduction result (Kaltofen 1985a), is to factor

$$f(z, 0) = \phi_1(z) \cdots \phi_r(z)$$

such that ϕ_i are irreducible factors in $\mathsf{K}[z]$. Then we can choose the Kronecker model

$$\mathsf{L}_i = \mathsf{K}[z]/(\phi_i(z)), \quad \zeta_i = z \bmod \phi_i(z), \tag{3}$$

and represent elements in L_i in

$$\mathsf{K} + \mathsf{K}z + \cdots + \mathsf{K}z^{\deg(\phi_i)-1} \subset \mathsf{K}[z].$$

Notice that all conjugates of ζ_i are represented in this way. With this representation the system (2) can be converted to a linear system over K.

It is observed in (Kaltofen 1985b) that algorithm Factorization over the Coefficient Field can be easily modified to an algorithm for factoring over the algebraic closure $\overline{\mathsf{K}}$. The only change one has to make is that one solves (2) over L_i instead of K. This is because one can change to input specification to factoring over $\overline{\mathsf{K}}$ without affecting the rest of the algorithm. For completeness, we write down the procedure.

Algorithm *Factorization over the Algebraic Closure*

Input: $f(x, y) \in \mathsf{K}[x, y]$ monic in x, $d := \deg_x(f)$, K an arbitrary field, such that the resultant

$$\mathrm{Res}_x(f(x, 0),\ \partial f(x, 0)/\partial x) \neq 0.$$

Output: Either f will be certified to be absolutely irreducible; or the algorithm returns a list of absolutely irreducible, not necessarily distinct, polynomial factors of $f(x, y)$,

$$f_i(x, y) \in \mathsf{L}_i[x, y] \text{ with } \mathsf{L}_i := \mathsf{K}(\zeta_i),$$

where ζ_i, $1 \leq i \leq d$, are the roots of $f(x, 0)$ in $\overline{\mathsf{K}}$.

For all roots $\zeta_i \in \overline{\mathsf{K}}$ of $f(x, 0) \in \mathsf{K}[x]$ Do Steps N and L.

Step N: *Perform Step N of the algorithm Factorization over the Coefficient Field given above.*

Step L: We now find the lowest degree polynomial in $\mathsf{L}_i[x, y]$, whose root is α_i.

For $m \leftarrow 1, \ldots, d - 1$ Do

{Here we try to find a polynomial in $\mathsf{L}_i[x, y]$ of degree m in x that α_i satisfies to a certain order.

Set the needed order of approximation

$$\ell \leftarrow \deg_y(f)(m + d - 1).$$

We examine whether the equation

$$\alpha_i^m + \sum_{\mu=0}^{m-1} h_{i,\mu}(y)\alpha_i^\mu \equiv 0 \pmod{y^{\ell+1}},$$

has a solution for $h_{i,\mu}(y) \in \mathsf{L}_i[y]$ with $\deg(h_{i,\mu}) \leq \deg_y(f)$. This again leads to a linear system, now over L_i.
Solve the linear system over the field L_i,

$$a_{i,k}^{(m)} + \sum_{\mu=0}^{m-1} \sum_{\delta=0}^{\deg_y(f)} a_{i,k-\delta}^{(\mu)} u_{i,\mu,\delta} = 0, \quad a_{i,\nu}^{(\mu)} = 0 \text{ for } \nu < 0, \tag{4}$$

for $0 \leq k \leq \ell$ *in the variables* $u_{i,\mu,\delta}$, $0 \leq \mu \leq m-1$, $0 \leq \delta \leq \deg_y(f)$. Again, if (4) has a solution, the solution is unique. *If the system has a solution in* L_i, *then set*

$$f_i(x,y) \leftarrow x^m + \sum_{\mu=0}^{m-1} \sum_{\delta=0}^{\deg_y(f)} u_{i,\mu,\delta} y^\delta x^\mu$$

and exit the loop. At this point, $f_i \in \mathsf{L}_i[x,y] \subset \overline{\mathsf{K}}[x,y]$ is an absolutely irreducible factor of f. *If the system has no solution and* $i = 1$ *and* $m = d-1$, *then designate* f *absolutely irreducible and exit the algorithm.* } □

As in the previous algorithm, the representation of the fields $\mathsf{L}_i = \mathsf{K}(\zeta_i)$ is left open. If we choose the Kronecker model (3) as their representations, we can solve (4) by arithmetic over K. In (Kaltofen 1989b) we further discuss how this method can reduce the problem of finding all distinct absolutely irreducible factors of $f(x,y)$ to the problem of factoring in $\mathsf{K}[z]$; in particular, we show how one and the same factor that is produced simultaneously by different ϕ_{i_1} and ϕ_{i_2}, or different roots of ϕ_i, can be identified.

The Kronecker representation (3) requires the factorization of $f(z,0)$ and therefore does not yield an absolute irreducibility test based on arithmetic alone. In (Kaltofen 1985b) we remove this requirement. Essentially, we perform the algorithm simultaneously for all L_i, that is, in

$$\mathsf{K}[z]/(f(z,0)) \cong \mathsf{K}[z]/(\phi_1(z)) \oplus \cdots \oplus \mathsf{K}[z]/(\phi_r(z))$$

in place of in each separate L_i. This model of algebraic number field arithmetic, which means algebraic number addition, subtraction, multiplication, division, and zero-testing, has been formalized by Dicrescenzo and Duval (1987): an algebraic number ζ is represented by a not necessarily irreducible, but squarefree, defining equation

$$\psi(z) \in \mathsf{K}[z], \quad \psi(\zeta) = 0.$$

Elements $\beta \in \mathsf{K}(\zeta)$ are represented as elements in the algebra $\mathsf{K}[z]/(\psi(z))$. The element β is not zero if

$$\mathrm{GCD}_z(\beta, \psi) = 1,$$

interpreting β as an element in $\mathsf{K}[z]$. In that case, β can be inverted by computing the Euclidean scheme

$$\sigma\beta + \tau\psi = 1, \quad \sigma, \tau \in \mathsf{K}[z], \quad \sigma = \beta^{-1}.$$

If β and ψ are not relatively prime in $\mathsf{K}[z]$, then, according to Dicrescenzo and Duval (loc. cit.), the computation has to split. If ζ is a root of $\mathrm{GCD}(\beta, \psi)$, then the element β is zero, otherwise it is not zero. In both cases, we obtain new defining equations for ζ. We call

this representation of algebraic number fields the *lazy factorization model*. Algorithm 3 in (Kaltofen 1985b) essentially realizes this model for algorithm Factorization over the Algebraic Closure, using the even more restrictive complexity class $\mathcal{NC}$. We observe that, due to our input assumption, no zero-test needs to be performed in Step N, since the only division is by

$$(\partial f(x,0)/\partial x)(z) \pmod{f(z,0)}.$$

In order to obtain Noether irreducibility forms, we need one additional modification to our algorithms (see (Kaltofen 1985b, Algorithm 2)). The point is that (4) is solvable for $m = d-1$ for all L_i, hence for the direct product. For reasons of deriving irreducibility forms, we can also drop the monicity assumption, but then we must increase the needed order of series approximation of a root slightly.[3]

Algorithm *Absolute Irreducibility Test*

Input: As in algorithm Factorization over the Algebraic Closure.
Output: True or false, depending whether f is irreducible in $\overline{\mathsf{K}}[x,y]$.

Set the maximum order of the approximation needed,

$$\ell_{\max} \leftarrow (2d-1)\ \deg_y(f).$$

Step N: Let $\mathsf{R} := \mathsf{K}[z]/(f(z,0)$.
Set the initial points for the Newton iteration

$$\alpha_0 \leftarrow z \bmod f(z,0) \in \mathsf{R}, \quad \beta_0 \leftarrow \frac{1}{\rho}\, t(z) \bmod f(z,0),$$

where $t(z)$ is the coefficient of Euclidean scheme for the resultant

$$s(z)\, f(z,0) + t(z)\, \frac{\partial f(x,0)}{\partial x}(z) = \mathrm{Res}_z \left(f(z,0),\ \frac{\partial f(x,0)}{\partial x}(z) \right) =: \rho \in \mathsf{K}.$$

Notice that because of the input assumption, $\rho \neq 0$.
Perform Newton iteration as in Step N of algorithm Factorization over the Coefficient Field, now over the ring R *in place of* L_i. We thus obtain a single approximate root $\alpha \in \mathsf{R}[y]$. The coefficients of the truncated powers of this root are computed as
For $i \leftarrow 0, \ldots, d-1$ Do

$$\sum_{0 \le k \le \ell_{\max}} a_k^{(i)} y^k \leftarrow (\alpha^i \bmod y^{\ell_{\max}+1}), \quad a_k^{(i)} \in \mathsf{R}.$$

[3] In the proof of Theorem 1 in (Kaltofen 1985a, pp. 478–479), the estimate for the degree of s_j is to be increased by d, since u_I there is then of degree d, and not equal to 1.

Step L: We try to find a polynomial in $\mathsf{R}[x,y]$ of degree $m_{\max} := d-1$ in x that α satisfies to order $\ell_{\max}$. We examine whether the equation

$$\sum_{i=0}^{m_{\max}} h_i(y)\alpha^i \equiv 0 \pmod{y^{\ell_{\max}+1}},$$

has a non-zero solution for $h_i(y) \in \mathsf{R}[y]$ with $\deg(h_i) \le \deg_y(f)$. We are led to the following linear system over R, arising from the coefficients of y^k in an indeterminate 'Ansatz' for the coefficients of the minimal polynomial:

$$\sum_{i=0}^{m_{\max}} \sum_{l=0}^{\deg_y(f)} a_{k-l}^{(i)} u_{i,l} = 0, \quad a_l^{(i)} \in \mathsf{R},\ a_l^{(i)} = 0 \text{ for } l < 0, \tag{5}$$

for all $0 \le k \le \ell_{\max}$ in the variables $u_{i,l}$, $0 \le i \le m_{\max}$, $0 \le l \le \deg_y(f)$. We solve (5) by further refining the unknows and coefficients to elements in K,

$$u_{i,l} = \sum_{\iota=0}^{d-1} u_{i,l,\iota} z^\iota \quad \text{and} \quad a_l^{(i)} = \sum_{\iota=0}^{d-1} a_{l,\iota}^{(i)}\, z^\iota,\ a_{l,\iota}^{(i)} \in \mathsf{K}.$$

First, *compute the reduced terms*

$$b_{\delta,0} + b_{\delta,1} z + \cdots + b_{\delta,d-1} z^{d-1} \leftarrow z^\delta \bmod f(z,0),\ \delta \ge d,\ b_{\delta,\iota} \in \mathsf{K}.$$

Collecting the coefficients of $y^k z^j$, we obtain the following linear forms:

$$\sum_{i=0}^{m_{\max}} \sum_{l=0}^{\deg_y(f)} \left(\sum_{\iota=0}^{j} a_{k-l,j-\iota}^{(i)} u_{i,l,\iota} + \sum_{\delta=d}^{2d-2} \sum_{\iota=0}^{\delta} b_{\delta,j} a_{k-l,\delta-\iota}^{(i)} u_{i,l,\iota} \right), \tag{6}$$

assuming that $u_{i,l,\iota} = 0$ and $a_{l,\iota}^{(i)} = 0$ for $l < 0$ or $\iota \ge d$.
If (6) has for the forms $0 \le k \le \ell_{\max}$, $0 \le j \le d-1$, a non-zero solution for the variables $u_{i,l,\iota}$, $0 \le i \le m_{\max}$, $0 \le l \le \deg_y(f)$, $0 \le \iota \le d-1$, then designate f as reducible over $\overline{\mathsf{K}}$. Otherwise, f is absolutely irreducible. □

3. Coefficient Growth Analysis

We now carry out the intricate task of analyzing how large intermediate coefficients in all variations of the algorithm can get. The main difference to the analysis in Kaltofen (1985a) is that we first estimate the norms and degrees of intermediate coefficients in terms of a generic input, that is when the coefficients of the input polynomial are independent variables. This modification will also yield the Noether irreducibility forms. Although the arguments are somewhat more involved, the analysis nonetheless follows essentially the ideas in Kaltofen (1985a), §6.

Let

$$f(x,y) = x^d + \sum_{e_1=0}^{d-1} \sum_{e_2=0}^{d-e_1} c_{e_1,e_2} x^{e_1} y^{e_2}$$

be a *generic* monic degree-d polynomial, $d \geq 2$, that is, its coefficients lie in the ring

$$\mathsf{D} := \mathbb{Z}[\ldots, c_{e_1,e_2}, \ldots].$$

By c's we denote the set of these indeterminate coefficients. All algorithms given in §2 compute in step N powers of a truncated power series for a root α of f in x,

$$\alpha^i \equiv \sum_{k=0}^{\ell_{\max}} a_k^{(i)} y^k \pmod{y^{\ell_{\max}+1}}, \tag{7}$$

where

$$a_k^{(i)} \in \mathrm{QF}(\mathsf{D})[z]/(f_0(z)), \quad f_0(x) := f(x,0) \in \mathsf{D}[x].$$

Notice that for a specific polynomial $f \in \mathsf{K}[x,y]$ we specialize the c's to the coefficient values and z to a root ζ of f_0.

To make our estimates, we use 1-norms of multivariate polynomials over $\mathbb{Z}$, which for a given polynomial are defined as the sum of the absolute values of its integral coefficients. Useful properties of this norm are

$$\|\varphi\,\psi\|_1 \leq \|\varphi\|_1\|\psi\|_1, \quad \|\varphi+\psi\|_1 \leq \|\varphi\|_1 + \|\psi\|_1 \quad \text{for all } \varphi,\psi \in \mathbb{Z}[X_1,\ldots,X_v].$$

Now and later we will need to reduce polynomials with a term z^j, $j \geq d$, modulo $f_0(z)$ to a polynomial of degree less than d in z. The following lemma shows how degrees and norms accumulate during such a reduction.

Lemma 1. *Let $\varphi \in \mathsf{D}[x,z]$, $j := \deg_z(\varphi) \geq d$. Then*

$$\deg_{c'\mathrm{s}}(\varphi \bmod f_0(z)) \leq (j+1-d) + \deg_{c'\mathrm{s}}(\varphi), \quad \|\varphi \bmod f_0(z)\|_1 \leq (d+1)^{j+2-d}\|\varphi\|_1.$$

Proof. Consider

$$z^j \bmod f_0(z) =: b_{j,0} + b_{j,1}z + \cdots + b_{j,d-1}z^{d-1},$$

where $b_{j,i} \in \mathsf{D}$. One obtains the bounds

$$\deg_{c'\mathrm{s}}(b_{j,\iota}) \leq j+1-d, \quad \|b_{j,\iota}\|_1 \leq (d+1)^{j+1-d} \tag{8}$$

by considering the $(j+1)\times(j+1)$ linear system for the unknown coefficients of the quotient and remainder in the polynomial division of z^j and $f_0(z)$:

$$\begin{pmatrix} \big| & & & & \\ \big| & \big| & \ddots & & \\ & & & \big| & \\ & & & 1 & \\ & & & & \ddots \\ & & & & 1 \end{pmatrix} \begin{pmatrix} * \\ * \\ \vdots \\ * \\ b_{j,d-1} \\ \vdots \\ b_{j,0} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \\ \vdots \\ \\ \\ 0 \end{pmatrix},$$

where the vertical strokes denote the coefficient vector of $f_0(z)$ in descending degree order. The stated bounds for $b_{j,\iota}$ follow easily from Cramer's rule and minor expansion on the

arising determinants; each of the first $j+1-d$ columns contains $d+1$ selectable positions. Furthermore, for the polynomial φ we obtain from (8),

$$\|\varphi \bmod f_0(z)\|_1 \le \|\varphi\|_1 + d\,(d+1)^{j+1-d}\|\varphi\|_1 < (d+1)^{j+2-d}\|\varphi\|_1. \quad \boxtimes$$

The referee points out that by solving the linear system given in the proof above by back-substitution, one may derive the sharper estimates

$$\|b_{j,\iota}\|_1 \le 2^{j-d} \quad \text{and} \quad \|\varphi \bmod f_0(z)\|_1 \le d\,2^{j+1-d}\|\varphi\|_1.$$

This estimate can be used to slightly improve the constant coefficients of powers of d in the exponents of some of the subsequent bounds for the 1-norms.

We will prove the estimate on the sizes of the arising coefficients for the linear systems of step L in three stages. First, we estimate the size of the coefficients of α, then the size of the coefficients of α^i, and third the size of the arising coefficients while solving the linear systems by Gaussian elimination. Again, we emphasize that the estimates are when executing the algorithms on a generic input, that is, for $\mathsf{K} = \mathrm{QF}(\mathsf{D})$.

Theorem 1. *For the polynomial*

$$\rho := \mathrm{Res}_x\left(f_0(x), \frac{\partial f_0(x)}{\partial x}\right) \in \mathsf{D}, \quad \deg_{c's}(\rho) \le 2d-1, \quad \|\rho\|_1 \le (2d)^{3d},$$

we have for all $k > 0$,

$$\bar{a}_k^{(1)} := \rho^{2k-1} a_k^{(1)} \in \mathsf{D}[z]/(f_0(z)),$$

and

$$\deg_{c's}(\bar{a}_k^{(1)}) \le (3d-2)\,(2k-1),$$

and

$$\|\bar{a}_k^{(1)}\|_1 \le (2d)^{(6d+2)\,(2k-1)} =: B_0(d,\,k).$$

Proof. The proof proceeds like the proof of Theorem 2 in Kaltofen (1985a). Set

$$f(x,y) =: \sum_{k\ge 0} f_k(x) y^k.$$

Starting from the factorization

$$\underbrace{(x-z)}_{=:g_0(x)}\, h_0(x) \equiv \underbrace{f(x,0)}_{f_0(x)} \pmod{f_0(z)},$$

one determines the coefficients

$$g_k(x), h_k(x) \in \mathrm{QF}(\mathsf{D})[z]/(f_0(z))[x]$$

of the terms y^k of the lifted factors,

$$\left(\sum_{k\ge 0} g_k(x) y^k\right)\,\left(\sum_{k\ge 0} h_k(x) y^k\right) = \sum_{k\ge 0} f_k(x) y^k,$$

with

$$\deg_x(g_k) = 0, \quad \deg_x(h_k) \leq d-2 \quad \text{for all } k > 0.$$

Setting

$$\hat{f}_k(x) := f_k(x) - \sum_{l=1}^{k-1} g_l \, h_{k-l}(x), \tag{9}$$

one obtains g_k and h_k as

$$g_0(x)\, h_k(x) + h_0(x)\, g_k(x) = \hat{f}_k(x). \tag{10}$$

Notice that $g_k = a_k^{(1)}$.[4] We estimate the norms and degrees of g_k and h_k inductively by estimating the solution to the linear system that corresponds to (10). The coefficient matrix of (10) is the Sylvester matrix of g_0 and h_0, its determinant their resultant. In particular, solving (10) by Cramer's rule one has to divide by this resultant. It is easily established (Kaltofen 1985, p. 482) that $\mathrm{Res}_x(g_0, h_0) = (\partial f_0/\partial x)(z) \in \mathsf{D}[z]$, hence

$$\frac{1}{\mathrm{Res}_x(g_0, h_0)} \equiv \frac{1}{\rho}\, r(z) \pmod{f_0(z)} \tag{11}$$

with

$$r(z)\frac{\partial f_0(x)}{\partial x}(z) + t(z) f_0(z) = \mathrm{Res}_x\left(\frac{\partial f_0(x)}{\partial x},\ f_0(x)\right) =: \rho, \tag{12}$$

where $\rho \in \mathsf{D}$ and $r(z) \in \mathsf{D}[z]/(f_0(z))$. From (12) it follows by Cramer's rule for linear systems with the Sylvester matrix of $\partial f_0(x)/\partial x$ and f_0 as coefficient matrix that

$$\deg_{c's}(\rho) \leq 2d-1, \quad \|\rho\|_1 \leq (2d-1)!\, d\,! < (2d)^{3d}. \tag{13}$$

Clearly (Brown and Traub 1971), the same bounds hold for the coefficients $r(z)$, or more precisely,

$$\deg_{c's}(r) < 2d-1, \quad \|r\|_1 \leq (2d-1)!\, d\,! < (2d)^{3d}. \tag{14}$$

This takes care of the division by the determinant of the linear system that corresponds to (10). We use minor expansion of the numerator along the right side vector in (10). Therefore, we also need a degree and norm bound for all $(d-1) \times (d-1)$ minors of the Sylvester coefficient matrix in (10). These we derive next. First, observe that

$$h_0(x) = \sum_{i=0}^{d-1} (c_{i+1,0} + c_{i+2,0} z + \cdots + c_{d-1,0} z^{d-2-i} + z^{d-1-i})\, x^i, \tag{15}$$

hence

$$\deg_{c's}(h_0) = 1, \quad \|h_0\|_1 < d^2.$$

[4] We essentially simulate the computation of α by linear multivariate Hensel lifting, which is a possible variant of what in effect amounts to multivariate linear Newton iteration.

Now, consider any $(d-1)\times(d-1)$ minor of the Sylvester matrix of g_0 and h_0 (see (15)) in x,

$$\begin{pmatrix} 1 & & & & & 1 \\ -z & 1 & & & & c_{d-1,0,}+z \\ & -z & 1 & & & c_{d-2,0}+c_{d-1,0}z+z^2 \\ & & -z & \ddots & & \vdots \\ & & & \ddots & 1 & c_{2,0}+\cdots+c_{d-1,0}z^{d-3}+z^{d-2} \\ & & & & -z & c_{1,0}+\cdots+c_{d-2,0}z^{d-3}+c_{d-1,0}z^{d-2}+z^{d-1} \end{pmatrix}. \tag{16}$$

Because of its special form, any such minor has linear degree in the c's and no more than degree $d-1$ in z. Its 1-norm as a polynomial in the c's and z is bounded by $d^2 2^d$ using minor expansion along the last column. Thus

$$T^{(\deg)} := 1 \quad \text{and} \quad T^{(\mathrm{norm})} := d^2 2^d \tag{17}$$

are uniform degree and norm bounds for all $(d-1)\times(d-1)$ minors of the coefficient matrix of (10).

We can now prove by induction on $k \geq 1$ the polynomiality conditions

$$\mathsf{D}[z] \ni \rho^{2k-1} g_k =: \bar{g}_k, \quad (\mathsf{D}[z])[x] \ni \rho^{2k-1} h_k =: \bar{h}_k, \tag{18}$$

that

$$\max\{\deg_{c'\mathrm{s}}(\bar{g}_k),\ \deg_{c'\mathrm{s}}(\bar{h}_k)\} \leq (2k-1)(3d-2), \tag{19}$$

and that

$$\max\{\|\bar{g}_k\|_1,\ \|\bar{h}_k\|_1\} \leq (2d)^{(6d+2)\,(2k-1)}. \tag{20}$$

Clearly, both inequalities imply the theorem, since $g_k = a_k^{(1)}$. We deal with the degree bound first. Let

$$C_k^{(\deg)} := \max\{\deg_{c'\mathrm{s}}(\bar{g}_k),\ \deg_{c'\mathrm{s}}(\bar{h}_k)\}$$

and let

$$D_k^{(\deg)} := \deg_{c'\mathrm{s}}(\bar{f}_k) \quad \text{with} \quad \bar{f}_k := \rho^{2k-2}\hat{f}_k;$$

we shall assume that in the definition (9) for $\hat{f}_k$, the products $g_l h_{k-l}$ are not reduced modulo $f_0(z)$. By the induction hypothesis for (18) we have

$$\bar{f}_k = \rho^{2k-2} f_k - \sum_{l=1}^{k-1} \bar{g}_l\, \bar{h}_{k-l} \ \in\ (\mathsf{D}[z])[x]. \tag{21}$$

In particular, for its degree in the c's we have by (13),

$$D_k^{(\deg)} \leq \max\{(2d-1)(2k-2)+1,\ \max_{1\leq l\leq k-1}\{C_l^{(\deg)} + C_{k-l}^{(\deg)}\}\}. \tag{22}$$

Now we solve (10) by Cramer's rule using minor expansion along the right side coefficient vector. All elements need to be divided by the determinant, which by (11) amounts to multiplication by $r(z)/\rho$. This already proves (18). Furthermore, we obtain for $k > 1$,

$$C_k^{(\deg)} \leq D_k^{(\deg)} + T^{(\deg)} + (3d-3), \tag{23}$$

where the accumulation by $3d-3$ is derived from a final reduction modulo $f_0(z)$: the degree in z of the unreduced numerator in the solution vector for the linear system derived from (10) is by Cramer's rule bounded by $2d-2$ (product of $\bar{g}_l \bar{h}_{k-l}$) plus $d-1$ (degree in z of the $(d-1)\times(d-1)$ minors of (16)) plus $d-1$ (degree in z of $r(z)$), which leads by Lemma 1 to an increment of $4d-4-(d-1)=3d-3$ for the reduced numerator. From (23) and (22) one derives (19) by induction on k. For $k=1$, the range of l in (21) is empty, so $D_1^{(\deg)}=1$ and $C_1^{(\deg)} \le 2+(d-1) \le 3d-2$ for $d \ge 2$. For $k>1$, we have

$$\begin{aligned} C_k^{(\deg)} &\le \max\{(2d-1)(2k-2)+1,\ (3d-2)(2(l+k-l)-2)\} + (3d-2) \\ &\le (3d-2)(2k-1). \end{aligned}$$

Second, we establish (20). The argument proceeds similarly; let

$$C_k^{(\mathrm{norm})} := \max\{\|\bar{g}_k\|_1,\ \|\bar{h}_k\|_1\} \quad \text{and let} \quad D_k^{(\mathrm{norm})} := \|\bar{f}_k\|_1.$$

Again we assume that $\bar{f}_k$ is not reduced modulo $f_0(z)$, while $\bar{g}_k$ and $\bar{h}_k$ are. By (21) we can bound $\|\bar{f}_k\|_1$, using

$$\|\rho^{2k-1} f_k\|_1 \le \|\rho\|_1^{2k-1} \|f_k\|_1$$

and (13),

$$D_k^{(\mathrm{norm})} \le (2d)^{3d(2k-1)}\ d + \sum_{l=1}^{k-1} C_l^{(\mathrm{norm})}\, C_{k-l}^{(\mathrm{norm})}. \tag{24}$$

From Cramer's rule applied to (10), we get from Lemma 1 and the fact that the degree in z of the numerator is $4d-4$ before reduction (see above),

$$\begin{aligned} C_k^{(\mathrm{norm})} &\le d\, T^{(\mathrm{norm})} D_k^{(\mathrm{norm})} \|r\|_1\ (d+1)^{3d-2} \\ &\le d^3 2^d (2d)^{3d} (d+1)^{3d-2} D_k^{(\mathrm{norm})} \\ &\le (2d)^{6d} D_k^{(\mathrm{norm})}, \end{aligned} \tag{25}$$

the second inequality by (17) and (14). The third inequality (25) is based on the estimates $d+1 \le \frac{3}{2}\, d$ for $d \ge 2$, hence

$$d^3 2^d (d+1)^{3d-2} \le \tfrac{4}{9} d\, (\tfrac{27}{32})^d\, (2d)^{3d}.$$

Lastly, $4/9\, d \le (32/27)^d$ for all $d \ge 2$. From (25) and (24), it follows easily by induction on k that

$$C_k^{(\mathrm{norm})} \le \tfrac{1}{2} \mathrm{Cat}_k\ (2d)^{(6d+1)\,(2k-1)}, \tag{26}$$

where $\mathrm{Cat}_k = \frac{1}{k}\binom{2k-2}{k-1}$ are the Catalan numbers. For $k=1$, we have $\bar{f}_1 = f_1$, hence $D_1^{(\mathrm{norm})} = d$, so by (25),

$$C_1^{(\mathrm{norm})} \le (2d)^{6d} d = \tfrac{1}{2}\, (2d)^{6d+1}.$$

For $k>1$ we get from (25), (24), and the induction hypothesis (26),

$$\begin{aligned} C_k^{(\mathrm{norm})} &\le (2d)^{3d\,(2k-1)+6d+1} + \tfrac{1}{4} (2d)^{(6d+1)\,(2k-2)+6d} \sum_{l=1}^{k-1} \mathrm{Cat}_l\, \mathrm{Cat}_{k-l} \\ &\le \tfrac{1}{4}\, (2d)^{(6d+1)\,(2k-1)} + \tfrac{1}{4}\, \mathrm{Cat}_k\, (2d)^{(6d+1)\,(2k-1)} \\ &\le \tfrac{1}{2}\, \mathrm{Cat}_k\, (2d)^{(6d+1)\,(2k-1)}. \end{aligned}$$

Equation (20) follows from the estimate $\mathrm{Cat}_k \le 4^k \le (2d)^{2k-1}$ for $d \ge 2$ and $k \ge 1$. $\boxtimes$

We now estimate the coefficients of powers of α.

Theorem 2. *Let ρ be as in Theorem 1. We have for all $1 \le i < d$ and $k > 0$ in (7),*

$$\bar{a}_0^{(i)} := a_0^{(i)} = z^i \in \mathsf{D}[z]/(f_0(z)), \quad \bar{a}_k^{(i)} := \rho^{2k-1} a_k^{(i)} \in \mathsf{D}[z]/(f_0(z)),$$

and

$$\deg_{c's}(\bar{a}_0^{(i)}) = 0, \quad \deg_{c's}(\bar{a}_k^{(i)}) \le (3d-2)\,(2k-1) + i - 1,$$

and

$$\|\bar{a}_0^{(i)}\|_1 \le 1, \quad \|\bar{a}_k^{(i)}\|_1 \le (k+1)^{i-1}(2d)^{(6d+2)(2k-1)+2(i-1)}.$$

Proof. The proof proceeds like the proof of Lemma 7 in (Kaltofen 1985a). Consider

$$a_k^{(i+1)} = \sum_{l=0}^{k} a_l^{(i)} a_{k-l}^{(1)},$$

or in term of the numerators,

$$\bar{a}_0^{(i+1)} = a_0^{(i+1)} = z^{i+1} \pmod{f_0(z)},$$

and for $k > 0$,

$$\bar{a}_k^{(i+1)} = \rho^{2k-1} a_k^{(i+1)} = \underbrace{\bar{a}_k^{(i)} a_0^{(1)}}_{l=k} + \underbrace{a_0^{(i)} \bar{a}_k^{(1)}}_{l=0} + \rho \sum_{l=1}^{k-1} \bar{a}_l^{(i)} \bar{a}_{k-l}^{(1)}. \tag{27}$$

The statement of the theorem for $\bar{a}_0^{(i)}$ follows from Lemma 1, while for $k > 0$ it follows by induction on i, observing that one has to reduce the products $\bar{a}_l^{(i)} \bar{a}_{k-l}^{(1)}$ modulo $f_0(z)$. For the degree estimate, we obtain from Theorem 1 and Lemma 1 for $k > 0$,

$$\begin{aligned}
&\deg_{c's}(\bar{a}_k^{(i+1)}) \\
&\quad \le \max\{\deg_{c's}(\bar{a}_k^{(i)}) + 1, && \text{case } l = k \\
&\qquad\quad \deg_{c's}(\bar{a}_k^{(1)}) + \deg_{c's}(a_0^{(i)}) + i, && \text{case } l = 0 \\
&\qquad\quad \max_{0<l<k}\{\deg_{c's}(\rho) + \deg_{c's}(\bar{a}_l^{(i)}) + \deg_{c's}(\bar{a}_{k-l}^{(1)})\} + d - 1\} && \text{case } 0 < l < k \\
&\quad \le \max\{(3d-2)(2k-1) + (i-1) + 1,\ (3d-2)(2k-1) + i, \\
&\qquad\quad \max_{0<l<k}\{(3d-2)(2l-1) + i - 1 + (3d-2)(2(k-l)-1) + (3d-2)\}\} \\
&\quad \le (3d-2)(2k-1) + i.
\end{aligned}$$

For the norm estimate, we obtain from Theorem 1 and Lemma 1, and the induction hypothesis for i, namely that for all $k > 0$,

$$\|\bar{a}_k^{(i)}\|_1 \le (k+1)^{i-1}(d+1)^{2(i-1)} B_0(d,k)$$

appealing to (27),

$$\begin{aligned}
\|\bar{a}_k^{(i+1)}\|_1 &\le \|\bar{a}_k^{(i)}\|_1\,(d+1)^2 && \text{case } l=k\\
&\quad + \|\bar{a}_k^{(1)}\|_1\,\|a_0^{(i)}\|_1\,(d+1)^{i+1} && \text{case } l=0\\
&\quad + \textstyle\sum_{l=1}^{k-1}\|\rho\|_1\,\|\bar{a}_l^{(i)}\|_1\,\|\bar{a}_{k-l}^{(1)}\|_1(d+1)^d && \text{case } 0<l<k\\
&\le (d+1)^2\,(k+1)^{i-1}\,(d+1)^{2(i-1)}\,B_0(d,k)\\
&\quad + (d+1)^{i+1}\,B_0(d,k)\\
&\quad + (d+1)^d(2d)^{3d}\textstyle\sum_{l=1}^{k-1}(l+1)^{i-1}\,(d+1)^{2(i-1)}\,B_0(d,l)\,B_0(d,k-l)\\
&\le 2\,(k+1)^{i-1}\,(d+1)^{2i}\,B_0(d,k)\\
&\quad + (k+1)^{i-1}\,(d+1)^{2i}\,B_0(d,k)\textstyle\sum_{l=1}^{k-1}1\\
&\le (k+1)^i(d+1)^{2i}B_0(d,k).\quad\boxtimes
\end{aligned}$$

Corollary 1. *For $i<d$ and $k\le d\,(2d-1)$, $\|\bar{a}_k^{(i)}\|_1\le(2d)^{24\,d^3}=:B_1(d)$.* $\square$

We now bound the size of any arising minor when solving the linear systems (2) and (4) of the factorization algorithms in §2, again using the generic input polynomial f. The coefficients of the linear forms under consideration are first brought onto the common denominator $\rho^{\max\{0,\,2k-1\}}$, that is,

$$\bar{a}_k^{(m)}+\sum_{\mu=0}^{m-1}\sum_{l=0}^{\min\{k,\,d\}}\rho^{\min\{2l,\,2k-1\}}\bar{a}_{k-l}^{(\mu)}u_{\mu,l}=0. \tag{28}$$

Hence, the coefficient matrix of the system has elements in $\mathsf{D}[z]/(f_0(z))$ that are to be evaluated at the coefficients of f and at $z=\zeta_i$, which is model dependent.

Theorem 3. *Let $\Delta\in\mathsf{D}[z]/(f_0(z))$ be any $I\times I$ minor of (28), $1\le I\le m(d+1)$; note that $m(d+1)$ is the number of unknowns in (2) and (28). Then*

$$\deg_{c'\mathrm{s}}(\Delta)\le 12\,d^3I,\quad \|\Delta\|_1\le(d+1)^{Id}I!\,B_1(d)^I.$$

Proof. Since $k\le\ell\le\ell_{\max}=2\,d\,(d-1)$, by Theorem 2 we have each coefficient of (28) bounded in degree by

$$(3d-2)\,(2\ell_{\max}-1)+m-1\le 12\,d^3-20\,d^2+6\,d,$$

and in 1-norm by $B_1(d)$ of Corollary 1, since the norm of ρ is bounded by $(2d)^{3d}$. By Lemma 1, the degree in the c's of the minor that is reduced by $f_0(z)$ grows by an additional term of $(I-1)\,(d-1)$, since its degree in z before reduction is $I\,(d-1)$. This term is absorbed by the negative lower order terms in the I^{th} multiple of the degree bound for each coefficient, which is a degree bound for the unreduced subminor. The 1-norm of the unreduced $I\times I$ minor is bounded by $I!\,B_1(d)^I$, which grows after reduction by Lemma 1 by a factor of $(d+1)^{I\,d}$. $\boxtimes$

The significance of this theorem does not lie in the actual estimates, which may be high, but in the conclusion that the algorithms Factorization over the Coefficient Field and Factorization over the Algebraic Closure have polynomial size growth in the arising

intermediate coefficients, independent what the model of algebraic number arithmetic is or what particular coefficient field K one has.

Somewhat better bounds are obtainable for algorithm Absolute Irreducibility Test. Consider the linear system derived from (5), each equation brought to a common denominator $\rho^{\max\{0,\,2k-1\}}$,

$$\sum_{i=0}^{d-1}\sum_{l=0}^{d}\left(\sum_{\iota=0}^{j}\rho^{\min\{2l,\,2k-1\}}a^{(i)}_{k-l,\,j-\iota}u_{i,\,l,\,\iota}+\sum_{\delta=d}^{2d-2}\sum_{\iota=0}^{\delta}b_{\delta,\,\iota}\rho^{\min\{2l,\,2k-1\}}a^{(i)}_{k-l,\,\delta-\iota}u_{i,\,l,\,\iota}\right)=0, \quad (29)$$

with $a^{(i)}_{l,\,\iota}=0$ and $u_{i,l,\,\iota}=0$ for $\iota\geq d$ or $l<0$; there is a linear form for each $0\leq j\leq d-1$ and $0\leq k\leq \ell_{\max}$, and a variable $u_{i,l,j}$ for each $0\leq i\leq d-1$, and $0\leq l\leq d$. Therefore, there are

$$M=M(d):=d\,(\ell_{\max}+1) \text{ equations and } N=N(d):=d^2(d+1) \text{ unknowns}$$

in (29).

Theorem 4. *Let $\Delta\in\mathsf{D}$ be any of the $\binom{M}{N}$ possible $N\times N$ maximal minors of (29). Then*

$$\deg_{c'\mathrm{s}}(\Delta)\leq 12d^6-2d^5-10d^4+4d^3 \quad \textit{and} \quad \|\Delta\|_1\leq(2d)^{34d^6}.$$

Proof. By Theorem 2 and Lemma 1, each coefficient of $u_{i,\,l,\,j}$ in (29) is bounded in degree by

$$d+(2d-1)\,2l+(3d-2)\,(2(k-l)-1)+d-2\leq(3d-2)\,2k,$$

which by minor expansion with $k\leq\ell_{\max}\leq(2d-1)d$ leads to the degree bound. The norm bound follows also by minor expansion, since each coefficient of $u_{i,\,l,\,j}$ is bounded by Theorem 2 and Lemma 1 in 1-norm by

$$d\,(d+1)^{d-1}\,(2d)^{3d\,2l}\,(k-l+1)^{d-2}(2d)^{(6d+2)(2(k-l)-1)+2d-2}\leq(2d)^{24d^3-4d^2},$$

where the factor d is the maximum number of coefficients to each $u_{i,\,l,\,\iota}$, and $(d+1)^{d-1}\geq\|b_{\delta,\,\iota}\|_1$. The norm bound follows from $N!\leq(2d)^{3N}$ and $(24d^3-4d^2)N+3N\leq 34d^6$. $\boxtimes$

4. Effective Hilbert Irreducibility

In order to enforce the input restriction (1) of our algorithms in §2, we need to generically translate arbitrary polynomials. This we shall discuss next. Let $d\geq 2$, $n\geq 2$, and let

$$f(X_1,\ldots,X_n)=\sum_{0\leq e_1+\cdots+e_n\leq d}q_{e_1,\ldots,e_n}X_1^{e_1}\cdots X_n^{e_n}\in\mathsf{K}[X_1,\ldots,X_n],$$

be a polynomial of total degree d over an arbitrary field K. Consider the polynomial

$$\varphi(x,y_2,\ldots,y_n):=f(x+v_1,y_2+w_2x+v_2,\ldots,y_n+w_nx+v_n)\in\mathsf{L}[x,y_2,\ldots,y_n]$$

where

$$\mathsf{L}:=\mathsf{K}(v_1,\ldots,v_n,\,w_2,\ldots,w_n)$$

and $v_1,\ldots,w_n$ are new indeterminants, i.e., algebraically independent elements over K.

Lemma 2. *φ is irreducible over $\overline{\mathsf{L}}$ if and only if f is irreducible over $\overline{\mathsf{K}}$.*

Proof. Clearly, if f factors over $\overline{\mathsf{K}}$, then the substitution

$$X_1 \leftarrow x + v_1,\ X_2 \leftarrow y_2 + w_2 x + v_2, \ldots, X_n \leftarrow y_n + w_n x + v_n$$

produces a factorization of φ over $\overline{\mathsf{K}}(v_1, \ldots, v_n,\ w_2, \ldots, w_n) \subset \overline{\mathsf{L}}$. On the other hand, if φ factors over $\overline{\mathsf{L}}$, the substitution

$$x \leftarrow X_1 - v_1,\ y_2 \leftarrow X_2 - w_2(X_1 - v_1) - v_2, \ldots, y_n \leftarrow X_n - w_n(X_1 - v_1) - v_n$$

produces a factorization of f over $\overline{\mathsf{L}}$. However, factorization over the algebraic closure is a purely rational question, as algorithm Absolute Irreducibility Test proves, for instance, and hence f must factor over $\overline{\mathsf{K}}$ already. $\boxtimes$

Now consider the leading coefficient of φ with respect to the single variable x,

$$l := \mathrm{ldcf}_x(\varphi) = \sum_{e_1 + \cdots + e_n = d} q_{e_1,\ldots,e_n} w_2^{e_2} \cdots w_n^{e_n}. \tag{30}$$

Since f has total degree d, l is a non-zero element in $\mathsf{K}[w_2, \ldots, w_n]$, and hence

$$\psi(x, y_2, \ldots, y_n) := \frac{1}{l}\,\varphi(x, y_2, \ldots, y_n) \in \mathsf{L}[x, y_2, \ldots, y_n]$$

is monic with respect to the single variable x.

Lemma 3. *Let*

$$r := \mathrm{Res}_x\left(\psi(x, 0, \ldots, 0),\ \frac{\partial \psi(x, 0, \ldots, 0)}{\partial x}\right) \in \mathsf{L}. \tag{31}$$

Then if $r = 0$, f factors over $\overline{\mathsf{K}}$.

Proof. The proof follows the arguments made in (Kaltofen 1985c). There are two cases to consider:
Case $\partial\psi(x, 0, \ldots, 0)/\partial x = 0$ (see also Lemma 5 in loc. cit.): We must have that K has positive characteristic p, and that for all term exponents $e_1, \ldots, e_n$ in f:

$$q_{e_1,\ldots,e_n} \neq 0 \Longrightarrow \forall\, i\colon p \text{ divides } e_i. \tag{32}$$

For suppose otherwise, namely that there is a term coefficient $q_{e_1,\ldots,e_n} \neq 0$ and an index i such that p does not divide e_i. Then the coefficient of x^{e_i} in $\psi(x, 0, \ldots, 0)$ is

$$\frac{1}{l(w_2, \ldots, w_n)}\, q_{e_1,\ldots,e_n} v_1^{e_1} \cdots v_{i-1}^{e_{i-1}} w_i^{e_i} v_{i+1}^{e_{i+1}} \cdots v_n^{e_n} + \cdots \neq 0,$$

resulting in a non-zero partial derivative, in contradiction to the assumption in this case. From (32) we infer that f is a p-th power of a polynomial over $\mathsf{K}(\ldots, \sqrt[p]{q_{e_1,\ldots,e_n}}, \ldots) \subset \overline{\mathsf{K}}$.
Case $\partial\psi(x, 0, \ldots, 0)/\partial x \neq 0$ and $r = 0$: In that case, the greatest common divisor

$$g := \mathrm{GCD}(\psi(x, 0, \ldots, 0),\ \partial\psi(x, 0, \ldots, 0)/\partial x),$$

computed in the domain $\mathsf{L}[x]$, must be a non-trivial divisor of $\psi(x, 0, \ldots, 0)$. But in fact by (30), ψ is a monic polynomial in $(\mathsf{K}(w_2, \ldots, w_n)[v_1, \ldots, v_n])[x]$, so g divides ψ also in $\mathsf{K}(w_2, \ldots, w_n)[x, v_1, \ldots, v_n]$. We write $g(x, v_1, \ldots, v_n)$ as a polynomial in that domain. Substituting $x \leftarrow X_1 - v_1$ and $v_i \leftarrow X_i - w_i(X_1 - v_1)$ for $2 \leq i \leq n$, we get that

$$g(X_1 - v_1, v_1, X_2 - w_2(X_1 - v_1), \ldots, X_n - w_n(X_1 - v_1)) \text{ divides } f(X_1, \ldots, X_n)$$

in $\mathsf{K}(v_1, w_2, \ldots, w_n)[X_1, \ldots, X_n]$. Since divisibility is a rational property, a suitable scalar multiple of the translated image of g must then actually be a factor of f in $\mathsf{K}[X_1, \ldots, X_n]$. ⊠

From now on, let us assume that f is absolutely irreducible. Now, consider for the elements

$$\nu_1, \ldots, \nu_n, \omega_2, \ldots, \omega_n \in \overline{\mathsf{K}}$$

the polynomial

$$\chi(x, y, z_2, \ldots, z_n) := f(x + \nu_1, \omega_2 x + z_2 y + \nu_2, \ldots, \omega_n x + z_n y + \nu_n) \in \overline{\mathsf{K}}[x, y, z_2, \ldots, z_n].$$

Lemma 4. *There exists a non-zero polynomial*

$$\Upsilon[v_1, \ldots, v_n, w_2, \ldots, w_n] \in \mathsf{K}[v_1, \ldots, v_n, w_2, \ldots, w_n], \quad \deg(\Upsilon) \leq 2d^2$$

such that

$$\begin{aligned}\Upsilon(\nu_1, \ldots, \omega_n) \neq 0 \Longrightarrow \operatorname{ldcf}_x(\chi) \in \overline{\mathsf{K}} \text{ and} \\ \operatorname{Res}_x(\chi(x, 0, z_2, \ldots, z_n), \partial\chi(x, 0, z_2, \ldots, z_n)/\partial x) \neq 0.\end{aligned}$$

Proof. The generic leading coefficient (30) and, by Lemma 3, the generic version of the resultant (31) cannot vanish, since f is absolutely irreducible. One chooses Υ to be the product of these generic polynomials. ⊠

From now on we shall assume that

$$\Upsilon(\nu_1, \ldots, \nu_n, \omega_2, \ldots, \omega_n) \neq 0, \tag{33}$$

although for the next lemma we only need monicity in x.

Lemma 5. *Assume that $\nu_1, \ldots, \omega_n$ satisfy (33). Then χ is irreducible in $\overline{\mathsf{K}}[x, y, z_2, \ldots, z_n]$.*

Proof. Assume χ factors. Since the leading coefficient of χ in the single variable x is an element in $\overline{\mathsf{K}}$, the factors must depend on x. Then substituting

$$x \leftarrow X_1 - \nu_1, z_2 \leftarrow (X_2 - \omega_2(X_1 - \nu_1) - \nu_2)/y, \ldots, z_n \leftarrow (X_n - \omega_n(X_1 - \nu_1) - \nu_n)/y$$

we obtain a factorization of f in $\overline{\mathsf{K}}(y)[X_1, \ldots, X_n]$, where all factors depend on some X_i. Now, since f does not depend on y, we can remove all negative powers of y, and obtain a factorization over $\overline{\mathsf{K}}$. ⊠

We are finally in the position of proving the main theorem of this section.

Theorem 5. *Assume that $\nu_1, \ldots, \omega_n$ satisfy (33). Then there exists a non-zero polynomial*

$$\Psi[z_2, \ldots, z_n] \in \overline{\mathsf{K}}[z_2, \ldots, z_n], \quad \deg(\Psi) \leq \tfrac{3}{2}\, d^4 - 2\, d^3 + \tfrac{1}{2}\, d^2,$$

such that for all $\eta_2, \ldots, \eta_n \in \overline{\mathsf{K}}$,

$$\Psi(\eta_2, \ldots, \eta_n) \neq 0 \Longrightarrow \chi(x, y, \eta_2, \ldots, \eta_n) = f(x + \nu_1, \omega_2 x + \eta_2 y + \nu_2, \ldots, \omega_n x + \eta_n y + \nu_n)$$
$$\text{is absolutely irreducible in } \overline{\mathsf{K}}[x, y].$$

Proof. By Lemma 5, χ is irreducible in $\overline{\mathsf{K}}(z_2, \ldots, z_n)[x, y]$. By Lemma 4, we can apply algorithm Factorization over the Coefficient Field of §2 to the monic version of χ,

$$\psi := \frac{1}{l}\, \chi \in \overline{\mathsf{K}}(z_2, \ldots, z_n)[x, y], \quad l := \mathrm{ldcf}_x(\chi) \in \overline{\mathsf{K}}.$$

The main point is now that, since $\psi(x, 0) \in \overline{\mathsf{K}}[x]$ does not depend on the z_i, the root ζ_1 used to construct the extension field L_1 of that algorithm is actually an element in $\overline{\mathsf{K}}$. Hence $\mathsf{L}_1 \subset \overline{\mathsf{K}}(z_2, \ldots, z_n)$, and the linear system (2) derived in Step L is unsolvable over L_1 for $m = d - 1$. This means that the augmented coefficient matrix of that system has higher rank than its coefficient matrix. Furthermore, $\partial\psi(x, 0)/\partial x \in \overline{\mathsf{K}}$, so all denominators used in the construction of this system are elements in $\overline{\mathsf{K}}$. Now, let $\Psi \in \overline{\mathsf{K}}[z_2, \ldots, z_n]$ be an $I \times I$ maximal non-zero minor of this augmented matrix. We have that if $\Psi(\eta_2, \ldots, \eta_n) \neq 0$, $\chi(x, y, \eta_2, \ldots, \eta_n)$ must be irreducible in $\overline{\mathsf{K}}[x, y]$. The latter follows simply from the fact that the algorithm Factorization over the Coefficient Field would fail to find a factor for $m = d-1$, since the corresponding image of (2) remains unsolvable over $\overline{\mathsf{K}}$.

We finish by estimating the degree of Ψ. Actually, we could use Theorem 3 and substitute ζ_1 for z and the coefficients of ψ for the c's to obtain the degree estimate $\deg(\Psi) \leq 12\, d^5$, but by redoing the degree analysis of the proof of Theorem 1, we can reduce the estimate to $O(d^4)$. We briefly describe the necessary changes, using the term z's for the indeterminates $z_2, \ldots, z_n$ in place of the c's. Making the appropriate changes in the necessary places, we have

$$\psi(x, y) = \sum_{k=0}^{d} \psi_k(x) y^k, \quad \psi_k \in (\overline{\mathsf{K}}[z'\mathrm{s}])[x],\ \deg_{z'\mathrm{s}}(\psi_k) \leq k;$$

$$\left(\sum_{k\geq 0} g_k(x) y^k\right)\ \left(\sum_{k\geq 0} h_k(x) y^k\right) = \sum_{k=1}^{d} \psi_k(x) y^k;$$

$$g_0(x) := x - \zeta_1, \quad g_k(x) = a^{(1)}_{1,k} \in \overline{\mathsf{K}}[z'\mathrm{s}] \text{ for all } k > 0;$$

$$h_0(x) = f_0(x)/g_0(x) \in \overline{\mathsf{K}}[x], \quad h_k(x) \in (\overline{\mathsf{K}}[z'\mathrm{s}])[x],\ \deg_x(h_k) = d - 2 \text{ for all } k > 0;$$

$$g_0(x) h_k(x) + h_0(x) g_k(x) = \widehat{\psi}_k(x) := \psi_k(x) - \sum_{l=1}^{k-1} g_l\, h_{k-l}(x) \in \overline{\mathsf{K}}[z'\mathrm{s}];$$

$$C^{(\deg)}_k := \max\{\deg_{z'\mathrm{s}}(g_k),\ \deg_{z'\mathrm{s}}(h_k)\}, \quad D^{(\deg)}_k := \deg_{z'\mathrm{s}}(\widehat{\psi}_k).$$

Since the Sylvester matrix of g_0 and h_0 is independent of the z's, we get $T^{(\deg)} = 0$ as a degree bound for the minors in Cramer's rule, so

$$D^{(\deg)}_k \leq \max\{k,\ \max_l\{C^{(\deg)}_l + C^{(\deg)}_{k-l}\}\}, \quad C^{(\deg)}_k \leq D^{(\deg)}_k,$$

which by induction yields $C_k^{(\deg)} \le k$. Then it is easy to establish also that $\deg_{z'\mathrm{s}}(a_{1,k}^{(\mu)}) \le k$. Since for $m = d-1$ there are d^2-1 unknown $u_{1,\mu,\delta}$ in (2), a maximal non-zero minor Ψ has dimension $I \le d^2$, and since for each k the corresponding row of coefficients have degree in the z's at most k, $0 \le k \le \ell_{\max}$,

$$\deg_{z'\mathrm{s}}(\Psi) \le \sum_{j=0}^{d^2-1} (\ell_{\max} - j) \le d\,(2d-2)\,d^2 - \frac{(d^2-1)\,d^2}{2}. \qquad \boxtimes$$

Note that the degree estimate comes quite close to that presented in Bajaj et al. (1989) for the case of complex coefficients, where a d^4 bound is presented by an algebraic-geometric argument.

It is clear from the arguments presented by von zur Gathen (1985), Lemma 4.2, that Theorem 5 can be modified to preserve irreducibility over K itself. However, von zur Gathen's proof leads to a degree estimate of order $2^{\Omega(d)}$ for the additional polynomial Ξ whose roots are to be avoided by ν_i, ω_j, and η_k, and since we wish to keep all estimates of order $d^{O(1)}$, we present a somewhat different and more restrictive argument.

Let $g \in \mathsf{K}[X_1, \ldots, X_n]$ be irreducible over the field K. Consider an absolute irreducible non-trivial factor $f(X_1, \ldots, X_n) \in \overline{\mathsf{K}}[X_1, \ldots, X_n]$ of g. By Theorem 5, if $\Upsilon(\nu_1, \ldots, \omega_n) \neq 0$ and then $\Psi(\eta_2, \ldots, \eta_n) \neq 0$, the bivariate polynomial

$$\psi_2(x, y) := f(x + \nu_1, \omega_2 x + \eta_2 y + \nu_2, \ldots, \omega_n x + \eta_n y + \nu_n)$$

will remain irreducible in $\overline{\mathsf{K}}[x, y]$. Now, assume that this is the case. The coefficients of f generate a finite algebraic extension of K,

$$f \in \mathsf{L}_s[X_1, \ldots, X_n], \quad \mathsf{L}_i := \mathsf{K}(\vartheta_1, \ldots, \vartheta_i),\ 1 \le i \le s,$$

where ϑ_i is algebraic over L_{i-1} with $\mathsf{L}_0 := \mathsf{K}$. Since g is irreducible over K, the tower of fields does not collapse; that is, $s \ge 1$. We define the norm of ψ_2 inductively: Let $\phi_s(t) \in \mathsf{L}_{s-1}[t]$ be the minimal polynomial of ϑ_s. Then writing ψ_2 as a polynomial in ϑ_s, $\psi_2(x, y, \vartheta_s)$, and letting $\vartheta_s^{(j)}$ denote all roots of ϕ_s, the norm of ψ_2 over L_s is defined as

$$\mathbf{N}_{\mathsf{L}_s}(\psi_2) := \mathbf{N}_{\mathsf{L}_{s-1}} \left(\prod_{j=1}^{\deg(\phi_s)} \psi_2(x, y, \vartheta_s^{(j)}) \right).$$

By the fundamental theorem on symmetric functions, $\mathbf{N}_{\mathsf{L}_s}(\psi_2) \in \mathsf{K}[x, y]$.

Lemma 6. *If ψ_2 is irreducible over L_s, then $\mathbf{N}_{\mathsf{L}_s}(\psi_2)$ is a power of an irreducible polynomial over K.*

Proof. Assume that $\mathbf{N}_{\mathsf{L}_s}(\psi_2) = h_1 h_2$, where h_2 and h_2 are two relatively prime polynomials in $\mathsf{K}[x, y]$. Furthermore, let $\gamma_2'(x, y)$ be an irreducible factor of

$$\gamma_2(x, y) := g(x + \nu_1, \omega_2 x + \eta_2 y + \nu_2, \ldots, \omega_n x + \eta_n y + \nu_n)$$

over K that is divisible by ψ_2 over L_s. Without loss of generality assume that h_1 is relatively prime to γ_2'. By the definition of the norm, there exist conjugates $\vartheta_1^{(j_1)}, \ldots, \vartheta_s^{(j_s)}$ such that

$$\psi_2^*(x, y) := \psi_2(x, y, \vartheta_1^{(j_1)}, \ldots, \vartheta_s^{(j_s)})$$

divides h_1. Also, since ψ_2 divides γ_2' over L_s, ψ_2^* divides γ_2' over an isomorphic copy of L_s, denote it by L_s^*. Therefore h_1 and γ_2' have a the common factor ψ_2^* over L_s^*, and therefore cannot be relatively prime over K itself, leading to a contradiction of our assumption. $\boxtimes$

Since g is irreducible over K and therefore divides $\mathbf{N}_{\mathsf{L}_s}(f)$, the image of g, $\gamma_2(x,y)$, must divide $\mathbf{N}_{\mathsf{L}_s}(\psi_2)$. Hence, γ_2 can only be a pure power of an irreducible polynomial over K. Now, if we can enforce

$$\mathrm{ldcf}_x(\gamma_2) \in \mathsf{K}, \quad \mathrm{Res}_x(\gamma_2(x,0), \partial\gamma_2(x,0)/\partial x) \neq 0,$$

then no multiple factor can occur, so γ_2 must be irreducible over K. Note that the condition on the resultant might fail for all evaluations, provided that K is a field of positive characteristic p and g is a p^{th} power over $\overline{\mathsf{K}}$; this is as in the first case in the proof of Lemma 3. This exceptional situation is impossible, for example, if K is a perfect field, since then each coefficient of g in K has a p^{th} root in K itself. Hence we have established the following theorem.

Theorem 6. *Let K be a perfect field. There exists a non-zero polynomial, depending on g only,*

$$\Xi \in \mathsf{K}[v_1, \ldots, v_n, w_2, \ldots, w_n], \quad \deg(\Xi) \leq 2\ \deg(g)^2,$$

such that

$$\left.\begin{array}{l} \Xi(\nu_1, \ldots, \nu_n, \omega_2, \ldots, \omega_n) \neq 0 \\ \text{and } \psi_2 \text{ absolutely irreducible} \end{array}\right\} \Longrightarrow \gamma_2 \text{ is irreducible over } \mathsf{K}.$$

Proof. Consider the generic versions

$$\gamma(x,y) := g(x + v_1, w_2 x + z_2 y + v_2, \ldots, w_n x + z_n y + v_n),$$

and $\lambda := \mathrm{ldcf}_x(\gamma) \in \mathsf{K}[w_2, \ldots, w_n]$. As in the proof of Lemma 3, we conclude that, since K is perfect and g is irreducible over K,

$$0 \neq \mathrm{Res}_x(\gamma(x,0), \partial\gamma(x,0)/\partial x) =: \rho \in \mathsf{K}[v_1, \ldots, v_n, w_2, \ldots, w_n].$$

We choose $\Xi := \lambda\rho$. Now $\Xi(\nu_1, \ldots, \omega_n) \neq 0$ implies that $\gamma_2(x,y)$ has no multiple factor, hence by the argument following the proof of Lemma 6 must irreducible over K. The degree estimate follows as in Lemma 4. $\boxtimes$

Combining Theorems 6 and 7 with techniques of (Kaltofen 1989a, Theorem 5.2), we obtain the following effective version of a Hilbert irreducibility theorem.

Corollary 2. *Let K be a perfect field, and suppose $g \in \mathsf{K}[X_1, \ldots, X_n]$. Randomly, select elements*

$$\nu_1, \ldots, \nu_n, \omega_1, \ldots, \omega_n, \eta_2, \ldots, \eta_n \in R \subset \mathsf{K}$$

uniformly from the set R. Then the following probability inequality holds:

$$\begin{aligned} &\mathrm{Prob}(g(x + \nu_1, \omega_2 x + \eta_2 y + \nu_2, \ldots, \omega_n x + \eta_n y + \nu_n) \in \mathsf{K}[x,y] \\ &\qquad \text{has the same number of unassociated}^5 \text{ irreducible factors over } \mathsf{K} \text{ as } g) \\ &\qquad\qquad \geq 1 - 2\ \deg(g)^4/\mathrm{card}(R). \end{aligned}$$ $\square$

Note that this Corollary improves the complexity and number of random bits needed in any of the randomized multivariate polynomial factorization algorithms (Kaltofen loc. cit.), (Kaltofen and Trager 1990).

5. Effective Noether Forms

Let $d \geq 2$, $n \geq 2$, and let

$$f(X_1, \ldots, X_n) = \sum_{0 \leq e_1 + \cdots + e_n \leq d} q_{e_1, \ldots, e_n} X_1^{e_1} \cdots X_n^{e_n} \in \mathsf{K}[X_1, \ldots, X_n]$$

be a polynomial of total degree d over an arbitrary field K. Consider the polynomial

$$\varphi_2(x, y) := f(x + v_1, w_2 x + z_2 y + v_2, \ldots, w_n x + z_n y + v_n) \in \mathsf{L}(z'\mathrm{s})[x, y],$$

where

$$\mathsf{L}(z'\mathrm{s}) := \mathsf{K}(v_1, \ldots, v_n, w_2, \ldots, w_n, z_2, \ldots, z_n).$$

Lemma 7. *The bivariate polynomial φ_2 is irreducible over $\overline{\mathsf{L}(z'\mathrm{s})}$ if and only if f is irreducible over $\overline{\mathsf{K}}$.*[6]

Proof. Clearly, if f factors over $\overline{\mathsf{K}}$, so does φ_2, even over $\overline{\mathsf{K}}(v_1, \ldots, z_n)$. So assume now that f is absolutely irreducible. By Lemma 5, φ_2 as a polynomial in x, y, $z_2, \ldots, z_n$ is irreducible over $\overline{\mathsf{L}}$, where

$$\mathsf{L} = \mathsf{K}(v_1, \ldots, v_n, w_2, \ldots, w_n).$$

For this and the next arguments, we suppose that the coefficients of f are elements in $\mathsf{L} \supset \mathsf{K}$. Note that absolute irreducibility is invariant to coefficient field extension. The assumptions to Theorem 5 are now satisfied with $\nu_1 = v_1, \ldots, \omega_n = w_n$. Therefore there exist elements $\eta_2, \ldots, \eta_n \in \mathsf{L}$, which is an infinite field, such that

$$\phi_2(x, y) := \varphi_2(x, y, \eta_2, \ldots, \eta_n)$$

remains irreducible over $\overline{\mathsf{L}}$. We now consider the values of the Noether forms on the coefficients of φ_2 and ϕ_2, which are both bivariate polynomials of degree d. Since ϕ_2 is absolutely irreducible, one such form, Φ_t, cannot vanish on the coefficients of ϕ_2. However, the coefficients of ϕ_2 are derived from those of φ_2 by evaluation of the z_i at η_i, hence Φ_t cannot vanish on the coefficients of φ_2 either. Again by the property of the Noether forms, φ_2 is irreducible over $\overline{\mathsf{L}(z'\mathrm{s})}$. $\boxtimes$

Note that condition (33) is crucial in this Lemma: a substitution that does not enforce squarefreeness at $y = 0$ may lead to a bivariate image that splits in $\overline{\mathsf{L}(z'\mathrm{s})}$, for example,

$$(X_1^2 - X_2 X_3)_{X_1 \leftarrow x, X_2 \leftarrow z_2 y, X_3 \leftarrow z_3 y} = (x + \sqrt{z_2 z_3}\, y)\,(x - \sqrt{z_2 z_3}\, y).$$

We can now establish our effective Noether irreducibility forms.

[5] Meaning those irreducible factors that differ by more than a scalar multiplier.

[6] This lemma was established jointly with John F. Canny.

Theorem 7. *There exists a finite set of polynomials*

$$\Phi_t(\ldots, c_{e_1,\ldots,e_n}, \ldots) \in \mathbb{Z}[\ldots, c_{e_1,\ldots,e_n}, \ldots],$$

such that

$$\forall\, t\colon \Phi_t(\ldots, q_{e_1,\ldots,e_n}, \ldots) = 0 \iff \begin{array}{l} f \text{ is reducible over } \overline{\mathsf{K}}, \\ \text{or } \deg(f) < d. \end{array}$$

If K *has positive characteristic, the coefficients of* Φ_t *are to be taken modulo this characteristic in the left side equality. Furthermore,*

$$\deg(\Phi_t) \le 12d^6 \quad \textit{and} \quad \|\Phi_t\|_1 \le (2d)^{12d^7+12d^6n+32d^6} =: B_2(d,\, n).$$

Proof. For the proof we write f as a generic d-degree polynomial,

$$f(X_1, \ldots, X_n) = \sum_{0 \le e_1+\cdots+e_n \le d} c_{e_1,\ldots,e_n} X_1^{e_1} \cdots X_n^{e_n} \in \mathsf{E}[X_1, \ldots, X_n],$$

where $\mathsf{E} := \mathbb{Z}[\ldots, c_{e_1,\ldots,e_n}, \ldots]$. The generic resultant corresponding to r in (31) of §4, denoted by ρ, now is an element in $\mathrm{QF}(\mathsf{E})(w_2, \ldots, w_n)[v_1, \ldots, v_n]$. In fact, multiplying it by λ^{2d-1}, where λ is the generic leading coefficient corresponding to l in (30) of §4, we obtain its numerator $\bar{\rho}$ as a polynomial,

$$\bar{\rho} \in \mathsf{E}[v_1, \ldots, v_n, w_2, \ldots, w_n].$$

Consider the following three sets of elements in E, the first two of which are

$$S_1 := \{c_{e_1,\ldots,e_n} \mid e_1 + \cdots + e_n = d\},$$
$$S_2 := \{\sigma \in \mathsf{E} \mid \sigma \text{ is a coefficient of a term in } v_1, \ldots, w_n \text{ of } \bar{\rho}\}.$$

For the third, we substitute in all Δ derived in Theorem 4 the coefficients of the polynomial corresponding to the generic version of $\psi_2 := \varphi_2/\mathrm{ldcf}_x(\varphi_2)$. Note that the generic version of $\mathrm{ldcf}_x(\varphi_2)$ is equal to λ. Let us denote by Δ'_s the rational functions resulting from this substitution, and let

$$D := 12d^6 - 2d^5 - 10d^4 + 4d^3$$

denote the degree bound in Theorem 4. We have

$$\Delta'_s \in \frac{1}{\lambda^D}\mathsf{E}[v_1, \ldots, v_n,\, w_2, \ldots, w_n,\, z_2, \ldots, z_n],$$

since each coefficient of the generic version of ψ_2 has as denominator λ. The third set is defined by

$$S_3 := \{\tau \in \mathsf{E} \mid \tau \text{ is a coefficient of a term in } v_1, \ldots, v_n,\ w_2, \ldots, w_n,\ z_2, \ldots, z_n \text{ of any of the } \lambda^D \Delta'_s.\}$$

We now can define our irreducibility forms as the set

$$\{\Phi_t \in \mathsf{E} \mid \exists c_{e_1,\ldots,e_n} \in S_1, \sigma \in S_2, \tau \in S_3\colon \Phi_t = c_{e_1,\ldots,e_n}\sigma\tau\}. \tag{34}$$

We first argue that (34) are Noether irreducibility forms. Take a specific f and substitute its coefficients $q_{e_1,\ldots,e_n}$ for the $c_{e_1,\ldots,e_n}$ into all Φ_t. If one of the resulting values in K is not zero, we conclude that by virtue of the inclusion of elements of the set S_1, f has degree d, hence $l \neq 0$; furthermore, $r \neq 0$, and a Δ'_s does not vanish on evaluation of its variables with the coefficient values in $\mathsf{L}(z'\mathrm{s})$. The former condition insures that the algorithm Absolute Irreducibility Test is applicable to ψ_2, and the later that ψ_2 will be certified absolutely irreducible over $\mathsf{L}(z'\mathrm{s})$, which by Lemma 7 establishes absolute irreducibility for f. Now suppose that all forms vanish on the coefficients of f. Then either $\deg(f) < d$, or $r = 0$ (since ψ is monic in x, r is the image of the generic resultant ρ), or $l \neq 0$, $r \neq 0$, and all Δ'_s vanish on the coefficients of ψ_2. In the second case, by Lemma 3, f is reducible over $\overline{\mathsf{K}}$, while in the third case ψ_2 will by the algorithm Absolute Irreducibility Test be determined reducible over $\overline{\mathsf{L}(z'\mathrm{s})}$, which by Lemma 7 means that so is f.

Finally, we estimate the degrees and coefficient sizes of Φ_t. We have by (30) and (31),

$$\deg_{c'\mathrm{s}}(\lambda) = 1, \quad \deg_{c'\mathrm{s}}(\bar{\rho}) \leq 2d-1 \Longrightarrow \deg_{c'\mathrm{s}}(\sigma) \leq 2d-1,$$

and, since the degree in the c's of the generic version of φ_2 is equal to 1, $\deg_{c'\mathrm{s}}(\tau) \leq D$. Hence, $\deg_{c'\mathrm{s}}(\Phi_t) \leq D + 2d$, which proves the degree estimate. The 1-norm of the generic version of φ_2, as a multivariate polynomial in the v_i, w_j, the c's, the z's, y, and x, is bounded by

$$\binom{d+n}{n} 3^d =: A \leq (2d)^{d+n},$$

because the 1-norm of the expanded products

$$(x+v_1)^{e_1}(z_2y + w_2x + v_2)^{e_2} \cdots (z_ny + w_nx + v_n)^{e_n}, \quad e_1 + \cdots + e_n \leq d,$$

is bounded by 3^d. Hence we have

$$\|\bar{\rho}\|_1 \leq (2d-1)!\, A^{2d-1} \Longrightarrow \|\sigma\|_1 \leq (2d-1)! A^{2d-1} \leq (2d)^{2d\,(d+n+1)} \text{ for all } \sigma \in S_2,$$

and for all $\tau \in S_3$,

$$\begin{aligned} \|\tau\|_1 &\leq \max\{\|\Delta\|_1 \mid \Delta \text{ as in Theorem 4}\}\, A^D \\ &\leq (2d)^{34d^6} (2d)^{(d+n)\,D} \\ &\leq (2d)^{12d^7 + 12d^6 n + 32d^6 - 2d^5 n}. \end{aligned}$$

The product of the the two bounds is clearly bounded by $B_2(d,n)$. $\boxtimes$

For the record, we give the number of polynomials Φ_t, in terms of D in the proof of Theorem 7 and M and N of Theorem 4.

$$\begin{aligned} \underbrace{\binom{d+n-1}{n-1}}_{\#\text{ of degree-}d\text{ terms in } f} &\times \underbrace{\binom{2d-1+2n-1}{2n-1}}_{\geq\#\text{ of } v_1,\ldots,w_n \text{ terms in } \bar{\rho}} \\ &\times \underbrace{\binom{M(d)}{N(d)}}_{\#\text{ of the } \Delta} \times \underbrace{\binom{D+3n-2}{3n-2}}_{\geq\#\text{ of } v_1,\ldots,z_n \text{ terms in } \Delta'_s} = 2^{(d+n)^{O(1)}}. \end{aligned}$$

6. Ostrowski Integers

We now derive an effective bound for the Ostrowski Theorem, using Theorem 7 and Noether's original argument. In this theorem, we have an absolutely irreducible degree-d polynomial

$$f(X_1, \ldots, X_n) = \sum_{e_1+\cdots+e_n \le d} q_{e_1,\ldots,e_n} X_1^{e_1} \cdots X_n^{e_n}$$

with $q_{e_1,\ldots,e_n} \in \mathbb{Z}[\xi]$, where ξ is an algebraic integer over $\mathbb{Q}$. Let the minimal polynomial of ξ be

$$g(z) \in \mathbb{Z}[z], \quad g(\xi) = 0, \quad \deg(g) = m.$$

Using the Kronecker model for the coefficients, and having eliminated a rational integer denominator, we denote by

$$\|f\|_{\infty,1} := \max_{e_1,\ldots,e_n} \{\|q_{e_1,\ldots,e_n}\|_1 \mid q_{e_1,\ldots,e_n} \text{ as a polynomial over } \mathbb{Z} \text{ of degree less than } m\}.$$

For an unramified rational prime p in $\mathbb{Q}(\xi)$, that is a prime that does not divide the discriminant of g, any prime ideal $\wp$ in the ring of (algebraic) integers $\mathcal{O}_{\mathbb{Q}(\xi)} \supset \mathbb{Z}[\xi]$ of $\mathbb{Q}(\xi)$ that contains, or as one says, lies above $p\,\mathbb{Z}$, is maximal, and hence $\mathsf{F}_\wp := \mathcal{O}_{\mathbb{Q}(\xi)}/\wp$ is a finite field. In fact, $\wp$ corresponds to an irreducible factor $g_1(z) \in \mathbb{Z}/(p)[z]$ of $g \bmod p$, such that

$$\wp = p\,\mathcal{O}_{\mathbb{Q}(\xi)} + g_1(\xi)\mathcal{O}_{\mathbb{Q}(\xi)},$$

where the coefficients of g_1 are taken as rational integers. By $f \bmod \wp$ we denote the polynomial where the coefficients $q_{e_1,\ldots,e_n}$ are mapped into $\mathsf{F}_\wp$ using the standard surjection.

Theorem 8. *There exists a positive integer C such that for any unramified rational prime integer p that does not divide C, for any prime ideal $\wp$ in $\mathbb{Q}(\xi)$ lying above p, $f \bmod \wp$ is absolutely irreducible as a polynomial over the field $\mathsf{F}_\wp$. Furthermore,*

$$C \le (\|g\|_2\, \|f\|_{\infty,1})^{12md^6} (2d)^{m(12d^7+12d^6n+32d^6)}.$$

Proof. Since f is absolutely irreducible, by Theorem 7 evaluating one of the forms Φ_t at the coefficients of f we must obtain a non-zero element $\vartheta \in \mathbb{Z}[\xi]$. Now, let

$$C := |\mathrm{Res}_z(g(z), h(z))| \quad \text{where} \quad \vartheta = h(\xi), h \in \mathbb{Z}[z].$$

Since g is irreducible, C is a non-zero integer. Clearly, for any prime p that does not divide C, and for any prime ideal $\wp$ lying above p, $(\vartheta \bmod \wp) \neq 0$ in $\mathsf{F}_\wp$. This means that the corresponding form Φ_t does not vanish on the coefficients of $f \bmod \wp$, implying its absolute irreducibility. It remains to estimate the size of C.

By Theorem 7,

$$\|h'\|_1 \le B_2(d,n)\, \|f\|_{\infty,1}^D, \quad D := 12\,d^6 \ge \deg(\Phi_t), \tag{35}$$

where $h'(\xi) = \vartheta$, but with the polynomial h' not reduced by g during the evaluation process of Φ_t, that is $\deg(h') \le (m-1)D$. Since

$$\mathrm{Res}_z(g(z), h'(z)) = \mathrm{Res}_z(g(z), h'(z) \bmod g(z)) = \pm C,$$

we need not reduce h' by dividing by g before estimating the resultant. Using a standard Hadamard determinant estimate, we obtain

$$\begin{aligned} C &\le \|g\|_2^{(m-1)D} \, \|h'\|_2^m \\ &\le (\|g\|_2 \, \|f\|_{\infty,1})^{mD} \, B_2(d,\, 2)^m. \qquad \boxtimes \end{aligned}$$

The reader may note that $\log(C) = (\log(\|g\|_2) \, \log(\|f\|_{\infty,1}) \, m\, d + n\, m\, d)^{O(1)}$. The first prime $p_{\min}$ for which absolute irreducibility of $(f \bmod \wp)$ is preserved for all prime ideals $\wp$ above $p_{\min}$ is of order $p_{\min} = O(\log(C))$. Note that in a less general way this was already established in (Kaltofen 1985b, §5).

The Ostrowski Theorem has a corresponding version for algebraic function fields (cf. Deuring (1941)). Suppose now that

$$f(X_1, \ldots, X_n) = \sum_{e_1+\cdots+e_n \le d} q_{e_1,\ldots,e_n}(y, \Theta) X_1^{e_1} \cdots X_n^{e_n}$$

is an absolutely irreducible polynomial over $\mathsf{K}(y, \Theta)$ with $q_{e_1,\ldots,e_n} \in \mathsf{K}[y, \Theta]$, where Θ is an algebraic function over the rational function field $\mathsf{K}(y)$. Let the minimal polynomial of Θ be

$$g(y, z) \in \mathsf{K}[y, z], \quad g(y, \Theta) = 0, \quad \deg_z(g) = m.$$

Without loss of generality, we may assume that $\mathrm{ldcf}_z(g) = 1$. For a value $p \in \overline{\mathsf{K}}$ we can naturally project $\mathsf{K}[y, \Theta]$ to $\mathsf{K}[\xi]$ where ξ is algebraic over K with $g(p, \xi) = 0$. We denote this projection by $\pi_{y \leftarrow p,\, \Theta \leftarrow \xi}$.

Theorem 9. *There exists a polynomial*

$$\Gamma \in \mathsf{K}[y], \quad \deg(\Gamma) \le 12\, m d^6 (\deg_y(f) + \deg_y(g)).$$

such that for all $p \in \overline{\mathsf{K}}$ and all roots ξ of $g(p, z)$,

$$\Gamma(p) \neq 0 \Longrightarrow \pi_{y \leftarrow p,\, \Theta \leftarrow \xi}(f) \text{ is irreducible in } \overline{\mathsf{K}}[X_1, \ldots, X_n].$$

Proof. Since f is absolutely irreducible, one of the forms Φ_t of Theorem 7 does not vanish on the coefficients of f, yielding a non-zero element $h'(y, \Theta) \in \mathsf{K}(y, \Theta)$. As in the proof of theorem 7,

$$\Gamma(y) := \mathrm{Res}_z(h'(y, z), g(y, z))$$

then is a non-zero element in $\mathsf{K}[y]$. Clearly, if $\Gamma(p) \neq 0$, Φ_t does not vanish on the coefficients of $\pi_{y \leftarrow p, \Theta \leftarrow \xi}(f)$, which proves absolute irreducibility. By Theorem 7,

$$\deg_y(h') \le \deg(\Phi_t) \deg_y(f) \quad \text{and} \quad \deg_z(h') \le \deg(\Phi_t)(m-1).$$

Hence,

$$\deg(\Gamma) \le \deg(\Phi_t)(m-1) \deg_y(g) + m \, \deg(\Phi_t) \deg_y(f). \qquad \boxtimes$$

7. Irreducibility in Neighborhoods

As in §6, for $d \geq 2$ and $n \geq 2$ let

$$f(X_1, \ldots, X_n) = \sum_{e_1+\cdots+e_n \leq d} q_{e_1,\ldots,e_n} X_1^{e_1} \cdots X_n^{e_n}$$

be an absolutely irreducible degree-d polynomial with $q_{e_1,\ldots,e_n} \in \mathbb{Z}[\xi]$, where ξ is an algebraic integer over $\mathbb{Q}$. Let the minimal polynomial of ξ be

$$g(z) \in \mathbb{Z}[z], \quad g(\xi) = 0, \quad \deg(g) = m.$$

Note that interpreting the algebraic number ξ as a complex number with real absolute value, we have the norm

$$\|f\|_\infty = \max_{e_1+\cdots+e_n \leq d}\{|q_{e_1,\ldots,e_n}(\xi)|\}.$$

In §6 we introduced the 1-norm of the coefficients of f as polynomials in ξ, $\|f\|_{\infty,1}$. It is not possible to bound that norm in terms of the ∞-norm: a huge linear integer relation of the powers of ξ may lead to a very small complex coefficient. However, if we can bound $q_{e_1,\ldots,e_n}(\xi^{(i)})$ for all conjugates of ξ, i.e., all roots of $g(z)$, such a relation can be established (Lenstra 1984, pp. 64–67):

$$\|q_{e_1,\ldots,e_n}\|_\infty \leq m(m-1)^{(m-1)/2}\, Q\, \|g\|_2^{m-1}\, |\mathrm{Disc}(g)|^{-1/2},$$

where $Q := \max\{|q_{e_1,\ldots,e_n}(\xi^{(i)})| \mid 1 \leq i \leq m\}$ and Disc is the polynomial discriminant operator

$$\mathrm{Disc}(g) = \frac{1}{\mathrm{ldcf}_z\, g(z)} \mathrm{Res}\left(g(z), \frac{\partial g(z)}{\partial z}\right).$$

It follows from Noether's irreducibility forms that there exists an $\varepsilon > 0$ such that every complex polynomial $\widetilde{f} \in \mathbb{C}[X_1, \ldots, X_n]$ of degree d with $\|f - \widetilde{f}\|_\infty < \varepsilon$ must remain absolutely irreducible. In this section we give an effective lower bound for the largest such ε.

Lemma 7. *Let $h(z) \in \mathbb{Z}[z]$ such that $h(\xi) \neq 0$. Then*

$$|h(\xi)| \geq \frac{1}{m}\, \|h\|_2^{1-m}\, \|g\|_2^{1-\deg(h)-m}$$

Proof. Since g is irreducible, by the assumption $h(\xi) \neq 0$ the following resultant must be a non-zero integer,

$$r := \mathrm{Res}_z(h, g) = \sigma(z)h(z) + \tau(z)g(z), \quad \deg(\sigma) < \deg(g).$$

By a Hadamard determinant inequality estimate (cf. Brown and Traub 1981)

$$\|\sigma\|_\infty \leq \|h\|_2^{m-1}\, \|g\|_2^{\deg(h)}.$$

From this it follows that

$$|h(\xi)| \geq \frac{1}{|\sigma(\xi)|} \geq \left(\|h\|_2^{m-1}\, \|g\|_2^{\deg(h)} \left(1 + \sum_{i=1}^{m-1} |\xi|^i\right)\right)^{-1}.$$

Our estimate follows from the inequality (Mignotte 1989, Ch. IV.3.3, p. 161)

$$|\xi| \leq \prod_{i=1}^{m} \max\{1,\, |\xi^{(i)}|\} \leq \|g\|_2. \qquad \boxtimes \tag{36}$$

Lemma 8. *Let* $\Phi \in \mathbb{C}[c_1, \ldots, c_J]$, $\deg(\Phi) =: D$, $\varepsilon > 0$, $\gamma_i, \widetilde{\gamma}_i, G \in \mathbb{C}$ *with*

$$\forall\, 1 \le i \le J\colon |\gamma_i| < G,\ |\widetilde{\gamma}_i| < G,\ |\gamma_i - \widetilde{\gamma}_i| < \varepsilon.$$

Then

$$|\Phi(\gamma_1, \ldots, \gamma_J) - \Phi(\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_J)| \le \varepsilon\, \|\Phi\|_1\, J\, D\, G^D.$$

Proof. Bound each term difference by

$$\begin{aligned}
|\gamma_1^{e_1} \cdots \gamma_J^{e_J} - \widetilde{\gamma}_1^{e_1} \cdots \widetilde{\gamma}_J^{e_J}| &= |(\gamma_1^{e_1} \cdots \gamma_J^{e_J} - \widetilde{\gamma}_1^{e_1}\gamma_2^{e_2} \cdots \gamma_J^{e_J}) + (\widetilde{\gamma}_1^{e_1}\gamma_2^{e_2} \cdots \gamma_J^{e_J} - \widetilde{\gamma}_1^{e_1}\widetilde{\gamma}_2^{e_2} \cdots \gamma_J^{e_J}) + \\
&\qquad \cdots + (\widetilde{\gamma}_1^{e_1} \cdots \widetilde{\gamma}_{J-1}^{e_{J-1}}\gamma_J^{e_J} - \widetilde{\gamma}_1^{e_1} \cdots \widetilde{\gamma}_J^{e_J})| \\
&\le |\gamma_1^{e_1} - \widetilde{\gamma}_1^{e_1}|\, |\gamma_2^{e_2} \cdots \gamma_J^{e_J}| + |\gamma_2^{e_2} - \widetilde{\gamma}_2^{e_2}|\, |\widetilde{\gamma}_1^{e_1}\gamma_3^{e_3} \cdots \gamma_J^{e_J}| + \\
&\qquad \cdots + |\gamma_J^{e_J} - \widetilde{\gamma}_J^{e_J}|\, |\widetilde{\gamma}_1^{e_1} \cdots \widetilde{\gamma}_{J-1}^{e_{J-1}}| \\
&\le J\,\varepsilon\, \max\nolimits_{1\le i\le J}\{e_i G^{e_i-1} \textstyle\prod_{j\ne i} G^{e_j}\} \\
&\le J\,\varepsilon\, DG^D. \quad \boxtimes
\end{aligned}$$

Theorem 10. *Suppose* $\widetilde{f} \in \mathbb{C}[X_1, \ldots, X_n]$, $n \ge 2$, *has degree* $d \ge 2$ *and*

$$\|f - \widetilde{f}\|_\infty < (2d)^{-12md^7 - 29mnd^6} \|f\|_{\infty,1}^{-12md^6} \|g\|_2^{-12md^6 - m + 1}.$$

Then $\widetilde{f}$ *is absolutely irreducible.*

Proof. Let $h' \in \mathbb{Z}[z]$ be as in the proof of Theorem 8. Since $h'(\xi) \ne 0$, by Lemma 7 and (35),

$$\begin{aligned}
|h'(\xi)| &\ge \frac{1}{m} \|h'\|_2^{1-m} \|g\|_2^{1-\deg(h')-m} \\
&\ge \frac{1}{m} B_2(d,n)^{1-m} \|f\|_{\infty,1}^{D(1-m)} \|g\|_2^{1-(m-1)\,D-m} =: \varepsilon_1,
\end{aligned}$$

where $D := 12d^6$ is a degree bound for all Φ_t in Theorem 7. Now, let $\varepsilon_0 := \|f - \widetilde{f}\|_\infty$. If $\varepsilon_0 < 1$ we have

$$\max\{\|f\|_\infty, \|\widetilde{f}\|_\infty\} \le \|f\|_\infty + 1 =: G.$$

Note that with (36) (see also the proof of Lemma 7) we can bound G in terms of $\|f\|_{\infty,1}$, namely

$$G \le \|f\|_{\infty,1} \|g\|_2^m.$$

The value of the irreducibility form Φ_t at the coefficients of f is $h'(\xi)$. If we denote by $\widetilde{\Phi}_t$ the value of that form at the coefficients of $\widetilde{f}$, we have by Lemma 8

$$|h'(\xi) - \widetilde{\Phi}_t| \le \varepsilon_0 \|\Phi_t\|_1 \binom{d+n}{n} DG^D. \tag{37}$$

Now, if we choose ε_0 so small that $|h'(\xi) - \widetilde{\Phi}_t| \le \varepsilon_1/2$, we are guaranteed, since $|h'(\xi)| > \varepsilon_1$, that $|\widetilde{\Phi}_t| \ge \varepsilon_1/2 > 0$. This implies by Theorem 7 that $\widetilde{f}$ is absolutely irreducible of degree d. Our estimate therefore follows from (37), namely

$$\begin{aligned}
\varepsilon_0 &\le \frac{\varepsilon_1}{2} \left(\|\Phi_t\|_1 \binom{d+n}{n} DG^D \right)^{-1} \\
&\le \frac{1}{2mD}\, 2^{-d-n} B_2(d,n)^{-m} \|f\|_{\infty,1}^{-Dm} \|g\|_2^{1-m\,D-m}. \qquad \boxtimes
\end{aligned}$$

Note that if $f \in \mathbb{Z}[X_1, \ldots, X_n]$, a distance

$$\|f - \widetilde{f}\|_\infty < (2d)^{-12d^7 - 29nd^6} (\|f\|_\infty + 1)^{-12d^6}.$$

can be derived.

8. Factoring over the Complex Numbers

We now present several complexity results for factoring multivariate polynomials over certain algebraically closed fields. Our results establish membership of the considered factorization problems in the complexity class $\mathcal{NC}$ (Cook 1985). In this section we shall deal with computing high precision complex approximations to the absolute irreducible factors of multivariate polynomials with rational or algebraic coefficients. In order to apply the algorithms of §2 to the $\mathcal{NC}$ setting we first need to modify the lazy factorization model for representing algebraic numbers, which is also discussed in §2.

Recall that in the lazy factorization model an algebraic number $\beta \in \mathsf{K}(\zeta)$ is represented by a residue modulo $\psi(z) \in \mathsf{K}[z]$ with $\psi(\zeta) = 0$. Now consider $\psi(z) = (z^2-2)(z^2-18) \in \mathbb{Q}[z]$, and assume that the computation has split and the resulting algebraic numbers of the two branches are

$$\beta_1 = z_1 \bmod z_1^2 - 2, \quad \beta_2 = z_2/3 \bmod z_2^2 - 18.$$

There are conjugates of both defining equations such that the resulting algebraic numbers both represent $\sqrt{2}$. Hence, we observe that the representation of an algebraic number in the lazy factorization model of $\mathsf{K}(\zeta)$ does not realize the full-fledged abstract data type of a field; by that we mean a representation that allows the addition, subtraction, multiplication, division and test for being zero of elements of $\mathsf{K}(\zeta)$. In fact, it is the zero test which in the lazy factorization model leads to a split in the computation, rather than to a yes/no outcome. In order to diagnose if one and the same absolutely irreducible factor arises in different branches of such a computation, we amend the lazy factorization model slightly.

The idea for our new representation is the following. Let K be an algebraic number field $\mathbb{Q}(\xi)$, ξ algebraic over $\mathbb{Q}$ with minimal polynomial $g \in \mathbb{Z}[w]$. We need to represent an element $\beta \in \mathsf{K}(\zeta)$, where ζ is algebraic over K. Let us assume first that we are given a squarefree integral polynomial $\psi(z) \in \mathbb{Z}[z]$ with $\psi(\zeta) = 0$. We now associate a complex rational $\widetilde{\zeta} \in \mathbb{Q}(\mathbf{i})$, $\mathbf{i} := \sqrt{-1}$, with ζ such that $\widetilde{\zeta}$ uniquely identifies a complex root of ψ. A standard way of doing this is to choose $\widetilde{\zeta}$ a sufficient approximation of $\zeta \in \mathbb{C}$, e.g.,

$$|\zeta - \widetilde{\zeta}\,| < \tfrac{\sqrt{3}}{2}\, |\mathrm{Disc}(\psi)|^{1/2}\, m^{-(m+2)/2} \|\psi\|_2^{1-m}, \quad m := \deg(\psi), \tag{38}$$

where Disc is the polynomial discriminant operator (see §7). Note that the middle expression in (38) is 1/2 of Mahler's (1964) root separation for ψ, hence for any conjugate $\zeta^* \in \mathbb{C}$ with $\psi(\zeta^*) = 0$ and $\zeta^* \neq \zeta$, the distance $|\zeta^* - \widetilde{\zeta}|$ is larger than that quantity. In order to find $\widetilde{\zeta}$ from the coefficients of ψ within the complexity class $\mathcal{NC}$ we make use of the recent result by Neff (1990).

If the coefficients of ψ are elements in $\mathbb{Q}(\xi)$, we can approximate the roots of the norm ψ with respect to the splitting field of $\mathbb{Q}(\xi)$,

$$\mathbf{N}_{\mathbb{Q}(\xi)}(\psi) := \mathrm{Res}_w(g(w), \psi(w,z)) \in \mathbb{Z}[z], \quad \psi \in \mathbb{Z}[w,z],\ \psi(\xi,\zeta) = 0.$$

In that case, the specific conjugate of ξ has to be isolated as well by a complex rational $\widetilde{\xi} \in \mathbb{Q}(\mathbf{i})$. Choosing both $\widetilde{\xi}$ and $\widetilde{\zeta}$ close enough to their corresponding complex numbers ξ and ζ, it is possible to decide which of the roots of the $\mathbf{N}_{\mathbb{Q}(\xi)}(\psi)$ are roots of $\psi(\xi, z)$ (Neff 1990, §3).[7]

An element $\beta \in \mathsf{K}(\zeta)$ is now represented by the triple

$$\chi(z) \in \mathsf{K}[z], \quad \psi(z) \in \mathsf{K}[z], \quad \widetilde{\zeta} \in \mathbb{Q}(\mathbf{i})$$

with $\beta = \chi(\zeta)$. As in the lazy factorization model, zero-testing requires the GCD computation $\gamma(z) := \mathrm{GCD}(\chi(z), \psi(z))$. Then $\beta = 0$ if and only if $\gamma(\zeta) = 0$, which can be checked using the approximate root $\widetilde{\zeta}$ (cf. Lemma 7). Non-zero elements can be inverted again using the Euclidean scheme

$$\sigma(z)\chi(z) + \tau(z)\psi(z) = \gamma(z),$$

and we get as the representation of β^{-1},

$$\sigma(z), \quad \psi(z)/\gamma(z), \quad \widetilde{\zeta} \in \mathbb{Q}(\mathbf{i}).$$

Arithmetic now has changed from the lazy factorization model in that the operands may have different defining equations, say $\beta_1 = \chi_1(\zeta)$ with $\psi_1(\zeta) = 0$ and $\beta_2 = \chi_2(\zeta)$ with $\psi_2(\zeta) = 0$. We can compute $\psi_3(z) \leftarrow \mathrm{GCD}(\psi_1(z), \psi_2(z))$ and then perform the arithmetic operations modulo ψ_3.

In conclusion, we have described a complete set of field operations for a particular representation of the field $\mathsf{K}(\zeta)$, all of which can be performed in $\mathcal{NC}$; a parallel computation of the Euclidean scheme items σ and τ is shown in (Borodin et al. 1982). We call this model for $\mathsf{K}(\zeta)$ the *single path lazy factorization model*. Note that the representation for β is not canonical, since we may use different defining equations ψ. More significantly, when using the $\mathcal{NC}$ polynomial GCD algorithm, it is not known how to put the coefficients of σ into canonical rational form, that is, we cannot reduce the numerator and denominator of the rational number coefficients of the elements in K. Of course, if we work within the complexity class $\mathcal{P}$, such constraints are not present.

Using this single path lazy factorization model for algebraic number fields, the effective estimates given in §3, and Neff's (loc. cit.) recent result on approximating complex roots of rational polynomials, we can now present several results on computing factorizations over the complex numbers.

Theorem 11. *For $f \in \mathbb{Q}(\xi)[X, Y] \subset \mathbb{C}[X, Y]$, where $\mathbb{Q}(\xi)$ is an algebraic number field in single path lazy factorization representation, algorithm Factorization over the Complex Numbers can compute all absolutely irreducible factors of f within the complexity class $\mathcal{NC}$. The representation of the factors over the fields $\mathbb{Q}(\xi, \zeta_i)$ will again be in the single path lazy factorization model.*

[7] We could also replace ψ by $\mathbf{N}_{\mathbb{Q}(\xi)}(\psi)$ in our representation. However, it has been argued that working with the tower of fields $\mathbb{Q} \subset \mathbb{Q}(\xi) \subset \mathbb{Q}(\xi, \zeta)$ rather than with a defining equation for ζ over $\mathbb{Z}$ keeps the rational coefficients much smaller (Abbott et al. 1986).

Proof. We apply algorithm Factorization over the Algebraic Closure of §2 to the squarefree and appropriately translated factors of f (see (Kaltofen 1985b, §2)). We briefly sketch the individual steps. First, one applies the parallel polynomial GCD algorithm (Borodin et al. 1982) to compute the content of f with respect to the variable X. Then one computes the squarefree decomposition of the primitive part of f using von zur Gathen's (1984) method. Finally, one translates $X \leftarrow x + \nu_1$ and $Y \leftarrow \omega x + y + \nu_2$, $\nu_1, \nu_2, \omega \in \mathbb{Z}$ to enforce (1) as in §4. The main problem is to factor a polynomial $f \in \mathbb{Q}(\xi)[x, y]$ that satisfies (1) and whose coefficients are in single path lazy factorization representation.

Clearly, algorithm Factorization over the Algebraic Closure can be executed in poly-log depth with respect to arithmetic in the fields L_i. Also by Theorem 2, the canonical representatives of all computed elements of L_i are bounded in size by a polynomial in $\deg(f)$ and $\|f\|_\infty$. Using the single path lazy factorization model for arithmetic in L_i, it remains to establish that the size of rational coefficients does not accumulate by repeated divisions. This is established by observing that divisions only occur twice: first, there are divisions by powers of $\mathrm{Res}_z(f(z,0), (\partial f/\partial x)(z,0)) \in \mathbb{Q}(\xi)$ in Step N. These divisions are accounted for by the analysis of the generic version of Step N in Theorem 1, where they correspond to division by powers of ρ. Second, a division occurs when solving the linear system (28). However, any of the poly-log algorithms computes such solutions by computing minors division free and then lastly dividing by a maximal non-singular minor (see (Borodin et al. 1982) and (Mulmuley 1987)). All other operations are additions, multiplications, and zero-tests, and do not contribute to size-growth in a non-canonical way. The theorem then follows from Theorem 3. ⊠

Theorem 11 leads to several corollaries, the first of which generalizes Neff's (1990) result to multivariate polynomials.

Corollary 3. *Given is a polynomial $f \in \mathbb{Z}[x, y]$ and a precision 2^{-E}. We can find, within the complexity class $\mathcal{NC}$ in terms of the problem size measure $\deg(f)\log(\|f\|_2)\,E$ exactly r absolutely irreducible polynomials $\widetilde{f}_j(x, y) \in \mathbb{Q}(\mathbf{i})[x, y]$ such that for any of the r absolutely irreducible factors $f_i(x, y) \in \mathbb{C}[x, y]$ of f we have a j_i with $\|f_i - \widetilde{f}_{j_i}\|_\infty < 2^{-E}$.*

Proof. Clearly, from the single path lazy factorization model we can by increasing the precision of the approximation of the identifying points $\widetilde{\zeta}_i$ for the fields L_i obtain the factors of f to any given precision 2^{-E}. It remains to establish that one can reach a precision at which non-associate factors must be separated. Note that different roots can lead to the same absolutely irreducible complex factor. The fairly standard separation analysis is carried out in (Kaltofen 1989b) not only for complex factors, but also for the corresponding real factors. Finally, by Theorem 10 we can approximate to a precision that guarantees the absolute irreducibility of the computed approximations. ⊠

The second corollary concerns multivariate factorization. In fact, in this setting it is very convenient to view the single path lazy factorization model as an abstract data type for a coefficient field, since the theory of obtaining sparse or concise representations of the factors, say by black boxes (Kaltofen and Trager 1989), is formulated for such abstract fields. The same is true of the theory of sparse interpolation (Ben-Or and Tiwari 1988), (Kaltofen and Lakshman 1988), (Zippel 1990), and (Karpinski et al. 1990). None of these algorithms take special care of divisions even though they might cause a potential size accumulation

problem when using non-canonical representations, such as the single path lazy factorization representation of algebraic numbers. However, by leading to $\mathcal{NC}$ results those problems can be definitely avoided, and inspection of the algorithms does prove it. For sake of brevity we shall not re-analyze all quoted algorithms from this point of view here, but only state a corollary, which is obtainable by the techniques in (Kaltofen and Trager 1989, Theorem 2).

Corollary 4. *Given is a sparse polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ with S non-zero monomials, a precision 2^{-E}, and a bound T. One can compute approximations to precision 2^{-E} of all irreducible complex factors of f with no more than T non-zero monomials within the randomized complexity class Monte-Carlo $\mathcal{RNC}$, i.e., the output is correct with probability no less than $1/2$, with respect to the problem size measure $n \deg(f) \log(\|f\|_\infty) E S T$.* $\square$

As a theoretical complexity result for factoring polynomials we feel this corollary truly stands out. It states that using polynomially many Boolean gates, one can compute an arbitrary precision approximation of all T-sparse complex factors of an S-sparse polynomial with n variables in time $(\log(n \deg f) + \log(E \log \|f\|_\infty) + \log(S T))^{O(1)}$.

9. The Function Field Case

In this section we investigate the case where the field of coefficients is a function field, which is special to the theory of factoring over the algebraic closure. We remark that for factorization over the coefficient field, transcendental extensions are, by a lemma of Gauss (1801, Article 42), equivalent to factorization with one additional variable. However, if we need to factor over an algebraic extension or the algebraic closure of the transcendental extension, the theory is more involved. Chistov (1987) gives a polynomial-time solution over finite algebraic extensions, and Abbott (1986) seriously studies which approaches are the best from a sequential and practical point of view, having efficient closed form integration of algebraic functions as his objective. Here we present a theoretical result with respect to the parallel complexity class $\mathcal{NC}$.

Our first approach is based on Theorem 9, which leads to the following theorem.

Theorem 12. *Given $f \in (\mathbb{Z}[z])[X, Y]$, the problem of determining the number of irreducible factors of f in $\overline{\mathbb{C}(z)}[X, Y]$ is within the complexity class $\mathcal{NC}$ with respect to the size measure* $\deg(f) \log(\|f\|_\infty)$.

Proof. Our proof is based on Theorem 9 and algorithm Factorization over the Algebraic Closure. The input specification (1) to that algorithm can be attained in the same way as was done at the beginning of the proof of Theorem 11. Therefore, let us suppose that $f \in (\mathbb{Z}[z])[x, y]$ has $\mathrm{ldcf}_x(f) \in \mathbb{Z}[z]$, which is equivalent to f being monic over $\mathbb{Q}(z)$, and that $f(x, 0)$ is squarefree. Now, let us denote by $\pi_{z \leftarrow p} \colon \mathbb{Z}[z] \to \mathbb{Z}$ the map evaluating z at $p \in \mathbb{Z}$. The idea is to count the number of irreducible factors in $\mathbb{C}[x, y]$ of $\pi_{z \leftarrow p}(f(x, y)) \in \mathbb{Z}[x, y]$. As we will show below, only for $P = \deg(f)^{O(1)}$ many $p \in \mathbb{Z}$ can the number of factors of the image polynomial $\pi_{z \leftarrow p}(f)$ be larger than that of f. Hence, the minimum of the number of complex factors of such images, letting p range through $P + 1$ values, must be the number of absolutely irreducible factors of f itself. One can count the number of complex factors of a polynomial in $\mathbb{Z}[x, y]$ in several ways, again staying within the complexity class $\mathcal{NC}$. For instance, we may use the algorithm by Bajaj et al. (1989), or we may use the method of Theorem 11.

It remains to derive a bound P. Consider the absolutely irreducible factors $f_i \in \overline{\mathbb{Q}(z)}[x,y]$, $1 \leq i \leq r$, of the preconditioned f. By algorithm Factorization over the Algebraic Closure for each f_i there exists a root Θ_i of $f(x,0)$ such that $f_i \in \mathbb{Q}(z,\Theta_i)[x,y]$. The map $\pi_{z \leftarrow p}$ extends to a ring homomorphism

$$\pi_{z \leftarrow p,\, \Theta_i \leftarrow \xi_i} : \mathbb{Z}[z,\, \Theta_i] \rightarrow \mathbb{Q}(\xi_i),$$

where ξ_i is any of the roots of the image $\pi_{z \leftarrow p}(g_i) \in \mathbb{Z}[x]$ of the minimal polynomial $g_i(x) \in (\mathbb{Z}[z])[x]$ of Θ_i. First, we need to argue that

$$\pi_{z \leftarrow p}(f) = \prod_{i=1}^{r} \pi_{z \leftarrow p,\, \Theta_i \leftarrow \xi_i}(f_i(x,y)),$$

where the right hand side product is taken in the splitting field of $\pi_{z \leftarrow p}(f(x,0))$, which contains each $\mathbb{Q}(\xi_i)$. It suffices to show that the maps $\pi_{z \leftarrow p, \Theta_i \leftarrow \xi_i}$ extend to a ring homomorphism from $\mathbb{Z}[\Theta_1, \ldots, \Theta_r] \subset \overline{\mathbb{Q}(z)}$ to $\mathbb{Z}[\xi_1, \ldots, \xi_r] \subset \mathbb{C}$. However, this is easily be demonstrated by building the map by successive extensions.

We finally designate those p for which $\pi_{z \leftarrow p,\, \Theta_i \leftarrow \xi_i}(f_i)$ remain irreducible in $\mathbb{C}[x,y]$. By Theorem 9, for any i there exists a polynomial

$$\Gamma_i \in \mathbb{Q}[z], \quad \deg(\Gamma) \leq 12 \deg_x(g_i) \deg_{x,y}(f)^6 (\deg_z(f) + \deg_z(g_i)),$$

such that $\Gamma_i(p) \neq 0$ implies precisely that. Therefore, P can be chosen the number of possible roots of all such Γ_i, which is bounded by

$$P \leq 24 \deg_x(f)^2 \deg_{x,y}(f)^6 \deg_z(f). \qquad \boxtimes$$

We note that the same approach can also be used in conjunction with Theorem 8 to count the number of complex irreducible factors of a polynomial in $\mathbb{Z}[X,Y]$ within complexity $\mathcal{NC}$; that without computing approximations to complex numbers, as in Corollary 3 to Theorem 11 or without computing Sturm sequences for parallel real algebraic number arithmetic, as in Bajaj et al. (1989). Furthermore, with Corollary 2 of §8 we can extend the statement of Theorem 12 to multivariate polynomials f, even with coefficients in an algebraic extension of $\mathbb{Q}(z)$.

A second approach is based on the single path lazy factorization model of §8 for algebraic extensions. In the case here the ground field K is the rational function field $\mathbb{Q}(y)$ and the algebraic element ζ is the algebraic function Θ. The single path model needs a unique identification of Θ among the conjugates of the monic squarefree defining equation $\psi(z) \in \mathbb{Z}[y,z]$. A natural idea is to use an initial segment of the Puiseux series expansion for Θ. We may also assume that the defining equation ψ remains squarefree at $y = 0$, translating $y = y' + \nu$ with $\nu \in \mathbb{Z}$ and using $\mathbb{Q}(y')$ as ground field, if necessary (see Chistov (1987) for how to avoid such a change of representation of $\mathbb{Q}(y)$). Then the Puiseux series for all roots of ψ in $\overline{\mathbb{Q}(y)}$ are power series, and we have actually shown in Step N of the Factorization algorithm of §2 how to compute truncated power series expansions in y from the roots of $\psi(0,z)$. The algebraic function Θ is thus identified by the constant term in its power series

expansion, $\xi \in \mathbb{C}$ with $\psi(0,\xi) = 0$. We will represent elements in the field $\mathbb{Q}(\xi)$ itself in the single path lazy factorization model.

In summary, the single path lazy factorization model represents an element $\Lambda \in \mathbb{Q}(y,\Theta)$ by the triple

$$\chi(z) \in \mathbb{Q}(y)[z], \quad \psi(y,z) \in \mathbb{Z}[y,z], \quad \widetilde{\xi} \in \mathbb{Q}(\mathbf{i}),$$

where $\psi(y,z)$ is monic in z and $\psi(0,z)$ is squarefree, with the meaning that $\Lambda = \chi(\Theta)$, $\psi(y,\Theta) = 0$, and that $\widetilde{\xi}$ identifies a root $\xi \in \mathbb{C}$ of $\psi(0,z)$ such that

$$\Theta = \xi + a_1 y + a_2 y^2 + \cdots, \quad a_i \in \mathbb{C}.$$

Since the pair $\psi(0,z) \in \mathbb{Z}[z]$ and $\widetilde{\xi}$ can be used to represent elements of $\mathbb{Q}(\xi)$ in the single path lazy factorization model, we may compute by Theorem 11

$$\Theta = \xi + a_1 y + \cdots + a_\ell y^\ell \pmod{y^{\ell+1}}, \quad a_k \in \mathbb{Q}(\xi),$$

within complexity $\mathcal{NC}$.

Using this representation for a field $\mathbb{Q}(y,\Theta)$, we can now establish a fact that corresponds to the statement of Corollary 3 to Theorem 11. At issue is how to distinguish equal degree non-associate absolutely irreducible factors of $f \in \mathbb{Z}[y][X_1,X_2]$, whose coefficients lie in the fields $\mathsf{L}_i = \mathbb{Q}(y,\Theta_i)$. By multiplying through with a common denominator of all such factors (cf. Theorem 3), we may suppose that the coefficients of the factors actually lie in $\mathbb{Z}[y,\Theta]$ and that they have the same leading coefficient. Theorem 3 also produces both a bound on the degrees in y and the 1-norms of the factor coefficients as polynomials in y and Θ. We now can separate distinct factors by computing high precision approximations of their coefficients both in terms of high order truncated power series expansions and high precision rational approximations of the complex term coefficients in the series. In the analysis of how precise these approximations need to be in order that the zero-tests on approximations in $\mathbb{Q}(\mathbf{i})[y]$ of elements in $\mathbb{Z}[y,\Theta_i]$ give correct results, we can follow the approach in (Kaltofen 1989).

The argument there proceeds in two steps. First, an upper bound for the size of the coefficients of minimal polynomials of all factor coefficients is derived. If the coefficients of the same term in two factors are unequal, then the product of the corresponding minimal polynomials must be squarefree. Factor coefficients may also be distinguished by conjugation, in which case one only considers the corresponding minimal polynomial. The second step uses Mahler's root separation measure (38) (see §8) with the size bounds obtained for the product of any two minimal polynomials to determine a separating precision. The corresponding approach to function fields requires the derivation of the bounds corresponding to the ones presented in (Kaltofen 1989, §3 and §5) as well as a separation lemma in the case of approximations in $\mathbb{Q}(\mathbf{i})[y]$ of elements in $\mathbb{C}[[y]]$ that are roots of squarefree polynomials in $\mathbb{Z}[y,z]$. Since not all roots of the minimal polynomial for a factor coefficient may be plain power series, we may bound the absolute value of the complex coefficients in the power series expansions of the actual factor coefficient by plugging a power series expansion of Θ_i into the factor coefficient in L_i in lazy factorization representation, and then by appealing to the estimates of Theorem 3. We shall omit the straight-forward but laborious estimates.

Literature Cited

Abbott, J. A., "Factorization of polynomials over algebraic function fields," *Doctoral Thesis*, Univ. Bath, England, 1988.

Abbott, J. A., Bradford, R. J., and Davenport, J. H., "The Bath algebraic number package," *Proc. 1986 ACM Symp. Symbolic Algebraic Comp.*, pp. 250–253 (1986).

Bajaj, C., Canny, J., Garrity, T., and Warren, J., "Factoring rational polynomials over the complexes," *Proc. ACM-SIGSAM 1989 Internat. Symp. Symbolic Algebraic Comput.*, pp. 81–90 (1989).

Ben-Or, M. and Tiwari, P., "A deterministic algorithm for sparse multivariate polynomial interpolation," *Proc. 20th Annual ACM Symp. Theory Comp.*, pp. 301–309 (1988).

Borodin, A., von zur Gathen, J., and Hopcroft, J. E., "Fast parallel matrix and GCD computations," *Inf. Control* **52**, pp. 241–256 (1982).

Brown, W. S. and Traub, J. F., "On Euclid's algorithm and the theory of subresultants," *J. ACM* **18**, pp. 505–514 (1971).

Chistov, A. L., "Efficient factorization of polynomials over a local field," *Soviet Math. Doklady (AMS Translation)* **37**/2, pp. 430-433 (1987).

Chistov, A. L. and Grigoryev, D. Yu., "Subexponential-time solving of systems of algebraic equations I," *LOMI Preprints* **E-9-83**, USSR Acad. Sci., Steklov Math. Inst., Leningrad, 1983.

Collins, G. E., "Quantifier elimination for real closed fields by cylindrical algebraic decomposition," in *Proc. 2nd GI Conf. Automata Theory Formal Lang.*, Springer Lec. Notes Comp. Sci. **33**; pp. 515–532, 1975.

Cook, S. A., "A taxonomy of problems with fast parallel algorithms," *Inf. Control* **64**, pp. 2–22 (1985).

Davenport, J. and Trager, B., "Factorization over finitely generated fields," *Proc. 1981 ACM Symp. Symbolic Algebraic Comput.*, pp. 200–205 (1981).

Deuring, M., "Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers," *Math. Zeitschrift* **47**, pp. 643–654 (1941).

Dicrescenzo, C. and Duval, D., "Computation on curves," *Proc. EUROSAM 1984, Springer Lect. Notes Comput. Sci.* **174**, pp. 100-107 (1984).

Dicrescenzo, C. and Duval, D., "Le système D5 de calcul formel avec des nombres algébriques," *Chapter 1 of the Doctoral Thesis by D. Duval*, Univ. Grenoble, 1987. In French.

Duval, D., "Absolute factorization of polynomials: a geometric approach," *SIAM J. Comput.* **20**/1, pp. 1–21 (1991).

Dvornicich, R. and Traverso, C., "Newton symmetric functions and the arithmetic of algebraically closed fields," in *Proc. AAECC-5*, Springer Lect. Notes Comput. Sci. **356**; pp. 216–224, 1987.

Fröhlich, A. and Shepherdson, J. C., "Effective procedures in field theory," *Phil. Trans. Roy. Soc., Ser. A* **248**, pp. 407–432 (1955/56).

von zur Gathen, J., "Parallel algorithms for algebraic problems," *SIAM J. Comp.* **13**, pp. 802–824 (1984).

von zur Gathen, J., "Irreducibility of multivariate polynomials," *J. Comp. System Sci.* **31**, pp. 225–264 (1985).

Gauss, C. F., *Disquisitiones Arithmeticae*; G. Fleischer, Jun., Leipzig, 1801.

Grigoriev, D. Yu., Karpinski, M., and Singer, M. F., "Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields," *SIAM J. Comput.* **19**/6, pp. 1059–1063 (1990).

Heintz, J. and Sieveking, M., "Absolute primality of polynomials is decidable in random polynomial-time in the number of variables," *Proc. ICALP '81, Springer Lec. Notes Comp. Sci.* **115**, pp. 16–28 (1981).

Hilbert, D., "Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten," *J. reine angew. Math.* **110**, pp. 104–129 (1892).

Kaltofen, E., "Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization," *SIAM J. Comp.* **14**/2, pp. 469–489 (1985a).

Kaltofen, E., "Effective Hilbert irreducibility," *Information and Control* **66**, pp. 123–137 (1985c).

Kaltofen, E., "Fast parallel absolute irreducibility testing," *J. Symbolic Comput.* **1**, pp. 57–67 (1985b). Misprint corrections: *J. Symbolic Comput.* **9**, p. 320 (1989).

Kaltofen, E., "Factorization of polynomials given by straight-line programs," in *Randomness and Computation*, Advances in Computing Research **5**, edited by S. Micali; JAI Press, Greenwhich, Connecticut, pp. 375–412, 1989a.

Kaltofen, E., "Computing the irreducible real factors and components of an algebraic curve," *Applic. Algebra Engin. Commun. Comput.* **1**/2, pp. 135–148 (1989b).

Kaltofen, E. and Lakshman Yagati, "Improved sparse multivariate polynomial interpolation algorithms," *Proc. ISSAC '88, Springer Lect. Notes Comput. Sci.* **358**, pp. 467–474 (1988).

Kaltofen, E. and Trager, B., "Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators," *J. Symbolic Comput.* **9**/3, pp. 301–320 (1990).

Knuth, D. E., *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms, Ed. 2*; Addison Wesley, Reading, MA, 1981.

Lenstra, A. K., "Polynomial-Time Algorithms for the Factorization of Polynomials," *Ph. D. Thesis*, Univ. Amsterdam, Amsterdam, Holland, January 1984.

Lipson, J., *Elements of Algebra and Algebraic Computing*; Addison-Wesley Publ., Reading, Mass., 1981.

Lombardi, H., "Algèbre élémentaire en temps polynomial," *Thèse Doctorat*, Université de Franche-Comté, Besançon, France, June 1989. In French.

Mahler, K., "An inequality for the discriminant of a polynomial," *Michigan Math. J.* **11**, pp. 257–262 (1964).

Mignotte, M., *Mathématiques pour le calcul formel*; Presses Universitaires de France, Paris, 1989.

Mulmuley, K., "A fast parallel algorithm to compute the rank of a matrix over an arbitrary field," *Combinatorica* **7**, pp. 101–104 (1987).

Neff, C. A., "Specified precision polynomial root isolation is in NC," *Proc. 31st Annual Symp. Foundations Computer Sci.*, pp. 152–162 (1990).

Noether, E., "Ein algebraisches Kriterium für absolute Irreduzibilität," *Math. Ann.* **85**, pp. 26–33 (1922).

Ostrowski, A., "Zur arithmetischen Theorie der algebraischen Größen," *Nachrichten d. Akademie d. Wissenschaften in Göttingen, math.-physik. Klasse*, pp. 279–298 (1919).

Schmidt, W. M., *Equations over finite fields. An elementary approach*; Springer Lect. Notes Math. **536**; Springer Verlag, New York, N. Y., 1976.

Trager, B. M., "Integration of algebraic functions," *Ph.D. Thesis*, MIT, 1984.

van der Waerden, B. L., "Eine Bemerkung über die Unzerlegbarkeit von Polynomen," *Math. Ann.* **102**, pp. 738–739 (1930). In German.

Zippel, R., "Interpolating polynomials from their values," *J. Symbolic Comput.* **9**/3, pp. 375–403 (1990).