Fast Parallel Absolute Irreducibility Testing*

Erich Kaltofen

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

Abstract

We present a fast parallel deterministic algorithm for testing multivariate integral polynomials for absolute irreducibility, that is irreducibility over the complex numbers. More precisely, we establish that the set of absolutely irreducible integral polynomials belongs to the complexity class *NC* of Boolean circuits of polynomial size and logarithmic depth. Therefore it also belongs to the class of sequentially polynomial-time problems. Our algorithm can be extended to compute in parallel one irreducible complex factor of a multivariate integral polynomial. However, the coefficients of the computed factor are only represented modulo a not necessarily irreducible polynomial specifying a splitting field. A consequence of our algorithm is that multivariate polynomials over finite fields can be tested for absolute irreducibility in deterministic sequential polynomial time in the size of the input. We also obtain a sharp bound for the last prime p for which, when taking an absolutely irreducible integral polynomial modulo p, the polynomial's irreducibility in the algebraic closure of the finite field of order p is not preserved.

Keywords: Absolute Irreducibility, Polynomial-Time Complexity, Parallel Algorithm.

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

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

This paper appears in the Journal of Symbolic Computation, vol. 1, nr. 1, pp. 57-67 (1985).

1. Introduction

The determination of the irreducibility of a polynomial with coefficients in a unique factorization domain is an old problem. Recently, several new algorithms for univariate and multivariate factorization over various coefficient domains have been proposed within the framework of sequential polynomial-time complexity. For the coefficients being rational numbers, the first solutions are due to Lenstra et al. (1982) in the univariate and to Kaltofen (1982, 1983) in the dense multivariate case. It seems natural to ask whether any of these algorithms can be converted to a parallel one. Unfortunately, for rationals as coefficients, all algorithms developed so far utilize the construction of a short vector in an integral lattice, a process which seems to resist a parallel approach. (Cf. von zur Gathen (1983a) where the problem is related to integer GCD computation.)

In this paper we primarily consider irreducibility over the complex numbers. An integer polynomial is said to be absolutely irreducible if it remains irreducible when one allows the coefficients of factors to be complex. For example, $x^2 + y^3$ is absolutely irreducible whereas $x^2 + y^2 = (x + iy)\,(x - iy)$ is not. We first observe that all previously known sequential algorithms such as Noether's criterion (1922), the multivariate Hensel algorithm (cf. Davenport, Trager (1981)) and the elimination algorithm by Heintz, Sieveking (1981) are exponential in the degrees of the input polynomials. For this problem, however, we shall do much better than just giving an algorithm polynomial in the input degree. Our algorithm is a parallel one which runs in polynomial-time in the logarithm of the degree of the input polynomial and the logarithm of the coefficient length. It needs polynomially many processors thus showing that ABSOLUTE IRREDUCIBILITY $\in NC \subset P$. (Cf. Cook (1981) for a definition of the class NC and its relation to the class of sequential polynomial-time algorithms P.) We wish to remark that this seems to be the first parallel and deterministic irreducibility test for polynomials over any of the usual coefficient domains. If the coefficients lie in a finite field, parallel factorization procedures are known for small characteristic but the algorithms are probabilistic except the irreducibility test (cf. von zur Gathen (1983a)).

Our parallel computation model is uniform Boolean circuits which means that we also account for the length of intermediately computed integers. We make extensive use of recently developed parallel algorithms for integer and polynomial arithmetic (cf. Reif (1983)), computing matrix determinants, solving singular linear systems over the rational numbers, computing polynomial greatest common divisors (cf. Borodin et al. (1982)) and computing squarefree polynomial factors (cf. von zur Gathen (1983a)).

We can extend our algorithm to find in parallel an irreducible complex factor of a given multivariate integral polynomial. It is not quite clear what the correct representation of such complex coefficients should be. We only can represent them as polynomials modulo a not-necessarily irreducible integral polynomial whose splitting field defines an algebraic extension over which the input polynomial factors. If we could isolate a root of an integral polynomial to high precision in parallel† then we could also obtain an arbitrarily high approximation of the coefficients of our factor.

A further application of our methods is a new proof with a sharpened bound of a theorem by Ostrowski (1919) stating the following: An absolutely irreducible integral polynomial remains absolutely irreducible modulo all but finitely many prime numbers. Known upper bounds for the largest prime making the modular polynomial reducible seem to have been exceedingly large, e.g. a triple exponential bound in the degree of the polynomial is given in Schmidt (1976). We derive a bound which is of polynomial length in the degree.

It is a consequence of Noether's (1922) theorem on the existence of reducibility-forms that one can test a polynomial over an arbitrary field for absolute irreducibility by field arithmetic alone, that is addition, subtraction, multiplication and division as well as testing elements to be equal to zero. We remark that our algorithm for absolute irreducibility also needs only the field operations and thus is not only restricted to the rational coefficient case. One interesting consequence is that we can give a sequential deterministic algorithm which tests a multivariate polynomial over a finite field for absolute irreducibility in polynomial-time of the total degree and the logarithm of the order of the field. The corresponding parallel algorithm is unfortunately a probabilistic one. But we view the sequential result a step towards solving the open question of how to deterministically test multivariate polynomials over finite fields for irreducibility.

In this paper we restrict ourselves to bivariate polynomials though we will mention in the conclusion how to generalize our results to more than two variables. Section 2 contains some prerequisite algorithms and a theorem, section 3 the irreducibility test and section 4 the extension to finding a factor. Section 5 presents a new proof and an effective bound for Ostrowski's theorem.

Notation: By $\mathbf{Z}$ we denote the integers, by $\mathbf{Q}$ the rationals and by $\mathbf{C}$ the complex numbers. $\bar{F}$ denotes the algebraic closure of a field F. $D[y, x]$ denotes the polynomials in y and x over D, $D[[y]]$ the domain of formal power series in y over D; $\deg_x(f)$ denotes the highest degree of x in $f \in D[y, x]$ and $\deg(f)$ the total degree of f. The coefficient of the highest power of x in f, a polynomial in y, is referred to as the leading coefficient of f in x and will be denoted by $\mathrm{ldcf}_x(f)$. We call f monic in x if $\mathrm{ldcf}_x(f)$ is a unit of D. As is well-known, $D[y, x]$ is a unique factorization domain (UFD) provided that D is a UFD. In this case the content of $f \in D[y, x]$ in x, $\mathrm{cont}_x(f)$, is the greatest common divisor (GCD) of all coefficients of $f(x)$ as elements in $D[y]$.

The infinity norm of $f \in \mathbf{C}[y, x]$, the maximum of the absolute values of the coefficients of f, will be denoted by $|f|$. The squareroot of the sum of squares of the coefficients of f, the square norm of f, will be denoted by $|f|_2$.

Let $f(y, x)$ and $g(y, x) \in D[y, x]$. By $\mathrm{res}_x(f, g)$ we denote the resultant of f and g with respect to the indeterminate x. As is well-known, $\mathrm{res}_x(f, g) \neq 0$ if and only if $\mathrm{GCD}(f, g) \in$

† To my knowledge it has not been rigorously established that one can quickly approximate a complex root of a polynomial in parallel.

$D[y]$. Furthermore, there exist polynomials $s(y, x)$, $t(y, x) \in D[y, x]$, $\deg_x(s) < \deg_x(g)$, $\deg_x(t) < \deg_x(f)$ such that

$$s(y, x)\ f(y, x) + t(y, x)\, g(y, x) = \mathrm{res}_x(f, g).$$

2. Preliminary Results

The overall structure of our algorithm will be quite similar to the reduction in Kaltofen (1983). We first transform f such that $f(0, x)$ is squarefree and f is monic in x. For this we can adopt algorithm 1 in Kaltofen (1983) which works briefly as follows:

1. Check that $\mathrm{cont}_x(f) = 1$. This is a GCD computation of all coefficients of x in f which are polynomials in y. If $\mathrm{cont}_x(f) \neq 1$ then f is reducible.

2. Check that $f(y, x)$ is squarefree, i.e. $\mathrm{GCD}(f, \partial f/\partial x) = 1$. We can also, as we will need in section 4, determine a squarefree factor of f quickly in parallel.

3. Make f monic in x by replacing f by the monic polynomial

   $$\hat{f}(y, x) = \mathrm{ldcf}_x(f)^{\deg_x(f)-1} f\left(y, \frac{x}{\mathrm{ldcf}_x(f)} \right).$$

   Notice that f is absolutely irreducible if and only if $\hat{f}$ is. In fact, if $\hat{g}(y, x)$ is a factor of $\hat{f}(y, x)$ then $\hat{g}(y, \mathrm{ldcf}_x(f)\, x)$ divided by its content is one for f.

4. Find an integer w with $|w| \leq \deg_x(\hat{f})\deg_y(\hat{f})$ such that $\hat{f}(w, x)$ remains squarefree, and replace $\hat{f}$ by $\bar{f}(y, x) = \hat{f}(w + y, x)$. Such an integer w must exist and we find it by testing in parallel for all integers in the given range whether $\mathrm{GCD}(f(w, x), \partial f/\partial x(w, x) = 1$.

We now outline the irreducibility test for $\bar{f}$, first over an arbitrary field F in which $\bar{f}(0, x)$ has a root (cf. Kaltofen (1983), Algorithm 2):

Algorithm 1:
[Given $f(y, x) \in F[y, x]$ monic in x, $f(0, x)$ squarefree, F an arbitrary field, and given $a_0 \in F$ such that $f(0, a_0) = 0$, this algorithm determines an irreducible factor of f over F:]

```
(N) [Compute approximation of root in $F[[y]]$:]
    $n \leftarrow \deg_x(f)$; $d \leftarrow \deg_y(f)$; $K \leftarrow (2n-1)d$.
    By Newton iteration, calculate $a_1, \ldots, a_K \in F$ such that $f(y, a_0 + a_1 y + \cdots + a_K y^K) \equiv 0$ mod $y^{K+1}$. $\alpha \leftarrow a_0 + \cdots + a_K y^K$.

(L) [Find minimal polynomial of $\alpha$ in $F[y, x]$:]

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

    FOR $i \leftarrow 1, \ldots, n-1$ DO
        Try to solve the equation

            $$\alpha^{(i)} + \sum_{j=0}^{i-1} u_j(y)\alpha^{(j)} \equiv 0 \bmod y^{K+1}$$
```

for polynomials $u_j \in F[y]$ with $\deg(u_j) \le d$. This equation leads to a linear system over F in $K + 1$ equations and $i(d+1)$ unknown coefficients of u_j. If there exists a solution then $x^i + \sum_{j=0}^{i-1} u_j(y) x^j$ divides $f(y, x)$. (Cf. Kaltofen (1983), Theorem 3; the solution is also unique.) In this case RETURN ("reducible").

[At this point, the FOR loop has not found a factor:] RETURN ("irreducible"). □

This algorithm supplies us with a theorem which will be of crucial importance for our irreducibility test.

Theorem 1: Let $f(y, x) \in \mathbf{Z}[y, x]$ be monic in x such that $f(0, x)$ is squarefree. Furthermore, let F be a subfield of $\mathbf{C}$ in which $f(0, x)$ possesses a root. Then f is absolutely irreducible if and only if f is irreducible in $F[y, x]$.

Proof: Obviously irreducibility over F is necessary for that over $\mathbf{C}$. Assume f were reducible in $\mathbf{C}$. Then algorithm 1 will find a factor of f in $\mathbf{C}[y, x]$ provided we replace F by $\mathbf{C}$ throughout the algorithm. However, we may choose $a_0 \in F \subseteq \mathbf{C}$ which automatically forces the a_i (see algorithm 2, step (N)), and later the (unique!) solution for the linear system to remain in F. Thus the factor found over $\mathbf{C}$ is in fact an element of $F[y, x]$. □

We will use an algorithm very similar to the previous algorithm for the absolute irreducibility test. First of all, we observe that if we had an irreducible factor $t(x)$ of $f(0, x)$ we could choose $F = \mathbf{Q}[z]/(t(z))$ in algorithm 1. Using the sequential polynomial-time factorization procedure this immediately shows that *absolute irreducibility can be decided in polynomial-time*. However, we want to construct a parallel solution and, at the current moment, there seems to be no fast parallel algorithm for finding t.

3. Testing Polynomials in $\mathbf{Z}[y, x]$ for Absolute Irreducibility

In this section we present an algorithm which when given a polynomial $f(y, x) \in \mathbf{Z}[y, x]$ monic in x such that $f(0, x)$ is squarefree determines in $(\log \deg(f) + \log\log|f|)^{O(1)}$ steps whether f is absolutely irreducible using $(\deg(f)\ \log|f|)^{O(1)}$ processors thus showing that ABSOLUTE IRREDUCIBILITY $\in NC$.

We use the idea of algorithm 1 but work in a ring R with zerodivisors in which $f(0, x)$ has a root. The choice is $R = \mathbf{Q}[z]/(f(0, z))$ and we construct our algorithm such that we never need to invert a zerodivisor in R. The detailed description follows now:

Algorithm 2:
[Given $f(y, x) \in \mathbf{Z}[y, x]$ monic in x, $f(0, x)$ squarefree, this algorithm determines whether f is absolutely irreducible.]

```
(I)   [Initialize:] $n \leftarrow \deg_x(f)$; $d \leftarrow \deg_y(f)$;
      By determinant formulas compute polynomials $s(z), t(z) \in \mathbf{Z}[z]$ such that

          $s(z)\, f(0, z) + t(z)\, \frac{\partial f}{\partial x}(0, z) = \rho = \mathrm{res}_z(f(0, z), \frac{\partial f}{\partial x}(0, z))$

      and $\deg(t) < \deg(f)$. [Since $f(0, x)$ is squarefree, $\rho$ is an integer not equal to zero.]
      $\alpha_0 \leftarrow z \bmod f(0, z) \in R = \mathbf{Q}[z]/(f(0, z))$; $\beta_0 \leftarrow \frac{1}{\rho} t(z) \in R$.
      [Notice that $f(0, \alpha_0) = 0$ and $\frac{1}{f'(0, \alpha_0)} = \beta_0$ in $R$, where $f'$ denotes $\frac{\partial f}{\partial x}$.]
      FOR $j$ in $\{0, \ldots, n\}$ DO $\alpha_0^{(j)} \leftarrow \alpha_0^{\,j} \in R$.

(N)   [Approximate a root of $f(y, x)$ in $R[[y]]$:]

      [Order of approximation:] $K \leftarrow (2n - 1)d$.

      FOR $i \leftarrow 0, \ldots, \lfloor \log_2(K) \rfloor$ DO

            $\alpha_{i+1} \leftarrow (\alpha_i - \beta_i\, f(y, \alpha_i)) \bmod y^{2^{i+1}}$.

            [At this point $\alpha_{i+1}$ is an approximation of a root of $f$ to order $y^{2^{i+1}}$. Notice that
            $f(y, \alpha_i) \bmod y^{2^{i+1}}$ is a multiple of $y^{2^i}$ and moreover can be quickly computed using
            $\alpha_i^{(j)}$.]

            FOR $j$ in $\{2, \ldots, n\}$ DO $\alpha_{i+1}^{(j)} \leftarrow \alpha_{i+1}^{\,j} \bmod y^{2^{i+2}}$.
                  [Notice that $\alpha_{i+1}^{(j)}$ is, as the $j$-th power of a root of $f$, only correct to order
                  $y^{2^{i+1}-1}$. We need twice as many terms the next time we substitute into $f$. One
                  can compute these powers in parallel by binary exponentiation though this is
                  not the fastest way possible (cf. Reif (1983)).]
```

$\beta_{i+1} \leftarrow (2\beta_i - f^{'}(y, \alpha_{i+1})\beta_i^2) \bmod y^{2^{i+1}}$.

[At this point, $\beta_{i+1}\ f'(y, \alpha_{i+1}) \equiv 1 \bmod y^{2^{i+1}}$. Again $f'(y, \alpha_{i+1})$ can be quickly computed using ${\alpha_{i+1}}^{(j)} \bmod y^{2^{i+1}}$.]

FOR j in $\{0, \ldots, n-1\}$ DO $\alpha^{(j)} \leftarrow {\alpha_{i+1}}^{(j)} \bmod y^{K+1}$.
[The index $i = \lfloor \log_2 K \rfloor$, hence $\alpha^{(j)}$ is the correct K-th order approximation of the j-th power of a root of f. Notice that ${\alpha_{i+1}}^{(1)} = \alpha_{i+1}$.]

(L) [Find a polynomial in $R[y, x]$ for which $\alpha^{(1)}$ is a root:]
Examine whether the equation

$$\alpha^{(n-1)} + \sum_{i=0}^{n-2} u_i(y)\alpha^{(i)} \equiv 0 \bmod y^{K+1} \tag{1}$$

is solvable for polynomials $u_i(y) \in R[y]$ such that $\deg(u_i) \le d$. Let $u_i(y) = \sum_{s=0}^{d} u_{is} y^s$ and let

$$\alpha^{(i)} = \sum_{k=0}^{K} a_k^{(i)} y^k, \quad a_k^{(i)} \in R.$$

Then (1) leads to the linear system

$$a_k^{(n-1)} + \sum_{i=0}^{n-2} \sum_{s=0}^{d} a_{k-s}^{(i)} u_{is} = 0 \tag{2}$$

for $k = 0, \ldots, K$ in the variables $u_{is} \in R$, $i = 0, \ldots, n-2$, $s = 0, \ldots, d$. We solve (2) by further refining the unknowns to polynomials in $\mathbf{Q}[z]/(f(0, z))$.† Let $u_{is} = \sum_{j=0}^{n-1} u_{isj} z^j$, $a_k^{(i)} = \sum_{j=0}^{n-1} a_{kj}^{(i)} z^j$ and let $z^\lambda \equiv \sum_{j=0}^{n-1} c_{\lambda j} z^j \bmod f(0, z)$ with $\lambda = n, \ldots, 2n-2$, $c_{\lambda j} \in \mathbf{Z}$. Then the coefficient of z^l, $0 \le l \le n-1$, for each equation in (2) is, setting $a_{kj}^{(i)}$ and u_{isj} to 0 for $j \ge n$,

$$a_{kl}^{(n-1)} + \sum_{i,s} \left(\sum_{j=0}^{l} a_{k-s,l-j}^{(i)} u_{isj} + \sum_{\lambda=n}^{2n-2} \sum_{j=0}^{\lambda} c_{\lambda l}\, a_{k-s,\lambda-j}^{(i)} u_{isj} \right) \tag{3}$$

which is a linear expression in u_{isj} and which must vanish on a solution of (2). This leads to a linear system over $\mathbf{Q}$ in $p = n(K+1)$ equations and $q = n(n-1)(d+1)$ unknowns. If this system has a solution, we return "f is reducible in $\mathbf{C}$", otherwise, we return "f is absolutely irreducible". □

The reader can find a proof that step (N) computes a K-th order approximation of a root of f in Lipson (1982), Sec.3.3. The correctness of algorithm 2 now hinges on the following theorem.

Theorem 2: The linear system (2) (resp. (3)) has a solution in R (resp. $\mathbf{Q}$) if and only if $f(y, x)$ factors over $\mathbf{C}$.

† Thanks go to Joachim von zur Gathen for pointing out this approach.

Proof: If: Let $t_1 \cdots t_r$ be the factorization of $f(0, x)$ into irreducibles. By p_j we denote the projection from R onto $F_j = \mathbf{Q}[z]/(t_j(z))$, $1 \le j \le r$. Then for $\alpha \equiv \alpha^{(1)}$, $p_j(\alpha) = \sum_{k=0}^{K} p_j(a_k^{(1)})y^k$ is the K-th order approximation for a root of $f(y, x)$ in $F_j[[y]][x]$. Now assume that $f(y, x)$ splits over $\mathbf{C}$. Since $f(0, x)$ has a root in F_j, by theorem 1 $f(y, x)$ splits in $F_j[y, x]$. Therefore, the minimal polynomial $g_j(y, x) \in F_j[y, x]$ for $p_j(\alpha)$ has degree $n_j < n$. Let $g(y, x) \in R[y, x]$ be the unique polynomial (by the Chinese Remainder Theorem) such that

$$p_j(g(y, x)) = x^{n-1-n_j} g_j(y, x) \text{ for } 1 \le j \le r.$$

Since $p_j(g(y, \alpha)) \equiv 0 \bmod y^{K+1}$ in $F_j[[y]]$ for all $1 \le j \le r$, $g(y, \alpha) \equiv 0 \bmod y^{K+1}$ in $R[[y]]$ and hence its coefficients solve (2).

Only if: Assume (2) admits a solution, i.e. there exists a polynomial $g(y, x) \in R[y, x]$ of degree $n - 1$ such that $g(y, \alpha) \equiv 0 \bmod y^{K+1}$. Let $g_1(y, x) = p_1(g(y, x))$ and let $\rho(y) = \mathrm{res}_x(f, g_1)$ over F_1. There exist polynomials $s(y, x)$ and $t(y, x) \in F_1[y, x]$ such that

$$\rho(y) = s(y, x)\, f(y, x) + t(y, x)\, g_1(y, x).$$

Therefore

$$\rho(y) = s(y, p_1(\alpha)) f(y, p_1(\alpha)) + t(y, p_1(\alpha)) g_1(y, p_1(\alpha)) \equiv 0 \bmod y^{K+1}.$$

But $\deg_y(f)$, $\deg_y(g_1) \le d$ and hence $\deg(\rho(y)) \le (2n - 1)d$. Thus $\rho(y) = 0$ and the $\mathrm{GCD}(f, g_1)$ in $F_1[y, x]$ is non-trivial. This GCD is, of course, a factor of $f(y, x)$ in $\mathbf{C}[y, x]$. □

We finally furnish a count for the number of arithmetic operations in $\mathbf{Q}$ as well as bounds for the intermediately computed numerators and denominators. The inversion of $f'(0, \alpha_0)$ is a determinant computation and can be performed in parallel in $O(\log^2(n))$ steps. Each ring operation in R costs no more than the normalization, that is the final remainder step modulo $f(0, z)$, which can be done in parallel in $O(\log^2(n))$ operations in $\mathbf{Q}$, though this again could be improved. As said before, we compute $\alpha_{i+1}^j \bmod y^{2^{i+2}}$ by binary exponentiation. However, we perform the normalization only after the exponentiation. Since $\deg_z(\alpha_{i+1}^j) \le n^2$ and the degree in y can be kept below $2^{i+2} = O(K)$ throughout the exponentiation process, computing the powers of $\alpha_{i+1} \bmod y^{2^{i+2}}$ can be accomplished in parallel in $O(\log^2(n) \log(K))$ operations in $\mathbf{Q}$. Therefore, step (N) takes $O(\log^2(n) \log^2(K))$ parallel arithmetic steps.

The bounds for the occurring rationals in step (N) follow from the elaborate analysis in Kaltofen (1983), Sec. 6. There we prove† that in (3) for $n \ge 4$

$$\begin{array}{ll} \rho^{2K-1}\ a_{kj}^{(i)} \in \mathbf{Z} \text{ [Lemma 7]}, & \\ & 0 \le i, j \le n-1,\ 0 \le k \le K \\ |\rho^{2K-1}\ a_{kj}^{(i)}| \le (2n|f|)^{4Kn^3} \text{ [(8)]} & \end{array}$$

and

† Actually, the given proof is modulo an irreducible factor of $f(0, x)$ but this fact is never used. The bounds work for any factor and we use this also in section 4.

$$|\rho| = |\mathrm{res}(f(0, z), \frac{\partial f}{\partial x}(0, z))| \le (2n|f|)^{n^3} \text{ [(6)]}.$$

In fact, all intermediate numerators and denominators of rational coefficients are bounded that way. It is easy to find a bound for $|c_{\lambda j}|$, e.g. $|c_{\lambda j}| \le |f|_2^n \le (n|f|)^n$. The approach is to investigate the linear system arising from the identity $x^\lambda = q(x) f(0, x) + r(x)$, $\deg(r) < n$, where the coefficients of q and r are the unknowns and apply Cramer's rule and Hadamard's determinant inequality. Thus the integer arithmetic of step (N) consumes $O((\log \deg(f) + \log \log |f|)^2)$ steps which is again not the best upper bound and thus binary complexity of step (N) is crudely bounded by

$$O(\log^6(\deg\ f) + \log^4(\deg\ f) \log^2(\log |f|)). \tag{4}$$

Step (L) is deciding the solvability of a linear, non-square system in $q = n(n-1)(d+1)$ unknowns and about twice as many equations whose coefficients are integers with $O(\deg^4(f) \log(|f|))$ digits. The parallel complexity given in (4) dominates this step as can be inferred from Borodin et al. (1984), Corollary 4.4, and Ibarra et al. (1980).

It should be clear that our methods are not restricted to polynomials over the integers, but work for any perfect coefficient field. (Perfectness of the field is required because of preprocessing step 2.) The most interesting case is then when the coefficients lie in a finite field GF(q). There are two peculiarities in this case. First, an element w such that $\hat{f}(w, x)$ remains squarefree may not exist in GF(q), as was necessary in the 4. preprocessing step. But it can be shown (cf. von zur Gathen, Kaltofen (1983), Sec. 4.2) that a small algebraic extension GF(q^m) can be constructed deterministically such that a $w \in$ GF(q^m) with the required property can be located. Since our input polynomial is to be tested for absolute irreducibility we do not lose generality by working over GF(q^m). Secondly, singular linear systems over finite fields can only be solved probabilistically in parallel (cf. Borodin et al. (1982)). That means, that the algorithm might fail to produce any decision, but that with diminishing probability. However, we can return to the sequential technique and thus get the following interesting result. Testing $f(y, x) \in \mathrm{GF}(q)[y, x]$ for irreducibility in the algebraic closure of GF(q) can be performed deterministically in $(\deg(f) \log(q))^{O(1)}$ binary steps. We mention this result, because testing f for irreducibility over GF(q) itself is not known to be in deterministic polynomial-time.

4. The Computation of an Irreducible Factor

In this section we show how to compute $g(y, x) \in \mathbf{C}[y, x]$ irreducible such that g divides $f(y, x) \in \mathbf{Z}[y, x]$. It should be clear from the preprocessing procedure as explained in section 2, that we only have to concern ourselves with f monic in x and $f(0, x)$ squarefree. We will represent $g \in R[y, x]$ where $R = \mathbf{Q}[z]/(\phi(z))$ with $\phi(z)$ some factor of $f(0, z)$. Moreover, g will be monic in x and division of f by g, thus always possible, will leave a zero remainder in $R[y, x]$. Therefore, if we evaluate the coefficients of g at any root of ϕ we get a factor of f in $\mathbf{C}[y, x]$. We also guarantee that for one root of ϕ the image of g under this evaluation is irreducible. We realize that one cannot speak properly of irreducibility over R since this domain is not necessarily a field.

We wish to observe that we know no fast parallel construction for the full factorization of $f(y, x)$ over $\mathbf{C}$. Even to determine how many factors f has over $\mathbf{C}$ yet escapes our attempts.

Algorithm 3:
[Given $f(y, x) \in \mathbf{Z}[y, x]$ monic in x, $f(0, x)$ squarefree, this algorithm determines $\phi(z) \in \mathbf{Z}[z]$ and $g(y, x) \in R[y, x]$, $R = \mathbf{Q}[z] / (\phi(z))$, such that g is a monic and irreducible factor of f.]

(I) − (N) as in algorithm 2.

(LF)

[Find a minimal polynomial for $\alpha^{(1)}$ in $R[y, x]$. It may become necessary in this step to restart the whole computation with R being replaced by a homomorphic image. Therefore, we initially set $\phi(z) = f(0, z)$.]

FOR I in $\{1, \ldots, n-1\}$ DO

Examine whether the equation

$$\alpha^{(I)} + \sum_{i=0}^{I-1} u_i(y)\alpha^{(i)} \equiv 0 \bmod y^{K+1} \tag{5}$$

is solvable for polynomials $u_i(y) \in R[y]$ such that $\deg(u_i) \le d$. As in step (L) of algorithm 2 this amounts to solving a linear system in $\deg(\phi)\,K$ equations and $\deg(\phi)\,(I-1)\,(d+1)$ unknowns over $\mathbf{Q}$.

Pick the smallest I for which (5) was solvable and denote it by I_0.
Compute one solution to (5) with $I = I_0$ and set $g(y, x) \leftarrow x^{I_0} + \sum_{i=0}^{I_0-1} u_i(y)x^i$.

Take the remainder $h(y, x) \in R[y, x]$ of $f(y, x)$ divided by $g(y, x)$ w.r.t. x. [Since g is monic in x, $h(y, x)$ is uniquely determined. The standard division algorithm shows that $\deg_y(h) \le (n - I_0 + 1)d$. However, R is not a field and we deem it necessary to explain a parallel procedure for performing this division.]
Compute the coefficients of $q(y, x)$ and $h(y, x) \in R[y, x]$ such that

$$f(y,x) = q(y,x)g(y,x) + h(y,x), \qquad \begin{array}{l} \deg_x(q) = n - I_0, \\ \deg_x(h) < I_0. \end{array}$$

Since q is monic in x and $\deg_y(q) \le (n - I_0)d$ this leads to a linear system in

$$\mu = ((n - I_0 + 1)d + 1)\, I_0 + ((n - I_0)d + 1)\, (n - I_0)$$

unknowns and $\nu \le ((n - I_0 + 1)d + 1)\, n$ equations over R. This system can be rewritten as a linear system in $\deg(\phi)\ \mu$ unknowns and $\deg(\phi)\ \nu$ equations over $\mathbf{Q}$ in exactly the same way as it was done in step (L).

IF $h = 0$ THEN RETURN($g(y,\ x) \in \mathbf{Q}[z]/(\phi)[y,\ x]$).
ELSE DO the following: For any coefficient $v_{i_0 s_0} \in R$ of $y^{s_0} x^{i_0}$ in $h(y,\ x)$ with $v_{i_0 s_0} \ne 0$ compute $\gamma(z) \leftarrow \mathrm{GCD}(\phi(z),\ v_{i_0 s_0}(z)) \in \mathbf{Z}[z]$. [We show below that $\gamma(z) \ne 0$. Then γ is a non-trivial factor of ϕ since also $\deg(v_{i_0 s_0}) < \deg(\phi)$.]
Replace ϕ by γ if $\deg(\gamma) \le \deg(\phi)/2$ and by ϕ/γ if $\deg(\gamma) > \deg(\phi)/2$. [The new ϕ has degree at most half of the old one.]
Project the coefficients of $\alpha^{(i)}$, $1 \le i \le n-1$, into the new $R = \mathbf{Q}[z]/(\phi)$ by taking them modulo the just obtained new ϕ. Then go back to step (LF). □

It should be clear that this algorithm runs in poly-logarithmic depth. Since the degree of ϕ is at least halved every time we restart at step (LF), this can happen at most $\lfloor \log_2(n) \rfloor$ times. We now prove its correctness. Let $\phi = t_1 \cdot\cdot\cdot t_r$ be the factorization of ϕ into irreducible polynomials. As in the proof of theorem 2, $F_j = \mathbf{Q}[z]/(t_j)$ are fields obtainable by projection from R via p_j. Now the minimal polynomial $g_j \in F_j[y,\ x]$ corresponding to $p_j(\alpha^{(1)})$ must divide $p_j(g)$. For we can conclude, as in the proof of theorem 2, that $\mathrm{GCD}(f(y,\ x),\ p_j(g)) \ne 1$. Therefore, by the same argument as in the proof of theorem 2,

$$I_0 = \max\ \{\ \deg(g_j)\ |\ 1 \le j \le r\}.$$

Let j_0 be such that $\deg(g_{j_0}) = I_0$. Then g is irreducible for $p_{j_0}(g)$ is irreducible over F_{j_0}. However, as pointed out in algorithm 1, g_{j_0} divides f, which means that $p_{j_0}(h) = 0$, or that t_{j_0} divides $v_{i_0 s_0}$ which finally proves that γ is non-trivial.

We wish to add the following observation. From g and ϕ one might, under fortunate circumstances, be able to obtain a factor in $\mathbf{Z}[y,\ x]$ of f. For were ϕ irreducible, then the *Norm* of g with respect to ϕ, that is the product of all conjugates σg of g, σ an automorphism of the splitting field of ϕ, must be the power of an irreducible polynomial in $\mathbf{Z}[y,\ x]$. The *Norm* can be computed by determining the resultant $\mathrm{res}_z(g,\ \phi(z))$. Even if ϕ is not irreducible, this resultant might turn out not to be a perfect power of f, in which case a factor can be extracted by divisions and GCD computations. That this phenomenon can really occur is easy to see. E.g. if $\deg(f)$ does not divide $\deg(\phi)\deg(g)$ the *Norm* of g cannot be a perfect power of f.

5. The Ostrowski-Noether Theorem

It is known at least since Noether (1922) that one can test a polynomial $f(x,y) \in F[x,y]$, F a field, for irreducibility over $\bar{F}$ by arithmetic operations in F alone. In fact, for any degree δ there exist polynomials

$$\phi_k(A_{00},\ldots,A_{ij},\ldots,A_{\delta 0}) \in \mathbf{Z}[A_{00},\ldots,A_{\delta 0}], \quad 0 \le k \le t,$$

such that $f(x,y) = \sum_{i+j\le\delta} a_{ij} x^i y^j$, $a_{ij} \in F$, is reducible over $\bar{F}$ or $\deg(f) < \delta$ if and only if for all $k = 0, \ldots, t$, $\phi_k(a_{00}, \ldots, a_{\delta 0}) = 0$, taking the coefficients of ϕ modulo the characteristic of F if that is positive. Noether calls the polynomial

$$\Phi_\delta(U, A_{00},\ldots,A_{\delta 0}) = \sum_{k=0}^{t} \phi_k(A_{00},\ldots,A_{\delta 0}) U^k$$

a *Reduzibilitaetsform* (reducibility-form) for δ. The existence of such a reducibility-form immediately implies the following theorem of Ostrowski (1919).

Theorem 3: Let K be a number field, O_K its ring of integers. Assume that $f(x,y) \in O_K[x,y]$ is absolutely irreducible. Then $f(x,y)$ modulo P remains absolutely irreducible over O_K/P for all but finitely many prime ideals P of O_K. □

In particular, if $K = \mathbf{Q}$ an absolute irreducible polynomial $f(x,y)$ remains absolutely irreducible modulo all but finitely many rational primes p. It is, however, not so easy to give a good lower bound B_f such that absolute irreducibility is preserved for all primes $p \ge B_f$. One such bound is calculated in Schmidt (1976), Corollary 2B, namely $B_f = (4|f|)^{(\delta+1)^{2^{\delta+1}}}$, $\delta = \deg(f)$. The following theorem establishes a much better bound whose proof is based on algorithm 2.

Theorem 4: Let $f(x,y) \in \mathbf{Z}[y,x]$ be monic in x, absolutely irreducible, with $\delta = \deg(f)$. Then f modulo p is absolutely irreducible over GF(p) for all primes p with

$$p \ge B_f = (2\,\delta\,|f|)^{10\,\delta^8}.$$

Proof: We, in fact, construct an integer B_f such that the above condition is true for all primes p which do not divide B_f. We execute algorithm 2 on input f but take all rationals modulo p. This is possible for all primes $p \nmid \rho$ since all intermediate denominators divide ρ^{2K-1} (see section 3). Since f is absolutely irreducible, the linear system (3) has no solution, that is the rank r of its augmented coefficient matrix must be larger than the rank of its coefficient matrix. Let Δ be an $r \times r$ submatrix with $\det(\Delta) \ne 0$. Assume that p does not divide the numerator of $\det(\Delta)$. Then f modulo p must be absolutely irreducible since the modulo p image of the linear system (3) is also unsolvable. It remains to estimate the numerator of $\det(\Delta)$. First we multiply each equation in (3) by its common denominator ρ^{2K-1}. Then the coefficient of the unknown u_{isj} is bounded by†

† Notice that though some intermediate bounds in Kaltofen (1983), Sec. 6, are worked out only for $n \ge 4$, further inspection shows that the bounds used are valid for all $n \ge 1$.

$$|\rho|^{2K-1} \left| a^{(i)}_{k-s,l-j} + \sum_{\lambda=n}^{2n-2} c_{\lambda l} a^{(i)}_{k-s,\lambda-j} \right| \le (2n|f|)^{5Kn^3},$$

which clearly bounds the constants in the system as well. Since $r \le \delta^3$, Hadamard's determinant inequality gives with $K \le 2\delta^2 - \delta$

$$|\det(\Delta)| \le \left(\delta^{3/2} (2n|f|)^{5Kn^3} \right)^{\delta^3} \le (2\delta|f|)^{10\delta^8 - 3\delta^7}.$$

Therefore, $B_f = |\rho \det(\Delta)|$ is bounded by $(2\delta|f|)^{10\delta^8}$. □

In theorem 4 we have assumed that f is monic in x. One can prove that for primes $p > B_f$ the preprocessing steps of section 2 remain valid when performed on f modulo p. A more important note is that modulo any prime p not dividing a certain integer $\le B_f$ absolute irreducibility will be preserved. This means that the first such prime is of order $O(\log B_f)$ and that actually small primes are quite likely to preserve absolute irreducibility.

6. Concluding Remarks

We have only presented our algorithm for two variables. There are several ways to extend it to many variables. The fastest among them is to use an effective version of the Hilbert Irreducibility Theorem, which was the approach by Heintz, Sieveking (1981). Other effective versions of this theorem can be found in von zur Gathen (1983b) and Kaltofen (1984). The result is a random parallel algorithm which runs in $(\log \mu + \log \deg(f) + \log \nu + \log\log|f|)^{O(1)}$ steps where μ is the number of monomials of the input polynomial f and ν the number of variables. If one wants a deterministic algorithm one can follow Kaltofen (1983), Algorithm 2, though the parallel version will only be polynomial in ν rather than $\log \nu$. However, this measure is still logarithmic in the input size provided we consider dense inputs.

In the meantime, Dicrescenzo, Duval (1984) have developed another absolute irreducibility test which may be a candidate for a polynomial-time solution. However, the most important conclusion of our work is that absolute irreducibility seems, in fact, an easier problem than irreducibility itself. The problem of how to concisely represent a full factorization of a polynomial over the algebraic closure of the coefficient domain remains to be addressed. In general, the proposed representations, e.g. by Loos (1982), of algebraic numbers in fields of large algebraic degree seem to consume too much space.

Future work on this subject is planned in two directions. D. Izraelevitz at Massachusetts Institute of Technology has already implemented a version of algorithm 1 using complex floating point arithmetic. Early experiments indicate that the linear systems computed in step (L) tend to be numerically ill-conditioned. How to overcome this numerical problem is an important question which we will investigate. Secondly, we will attempt to obtain good degree bounds for reducibility-forms following the approach laid out in theorem 4. Polynomial bounds would have important implications for effective Hilbert Irreducibility Theorems.

References

Borodin, A., von zur Gathen, J., Hopcroft, J. (1982). Fast parallel matrix and GCD computations. *Information and Control* 52, 241-256.

Borodin, A., Cook, S., Pippenger, N. (1984). Parallel computation for well-endowed rings and space-bounded probabilistic machines. *Information and Control*, to appear.

Cook, S. A. (1981). Towards a complexity theory of synchronous parallel computation. *L'Enseignement mathématique* 27, 99-124.

Davenport, J., Trager, B. (1981). Factorization over finitely generated fields. Proc. 1981 ACM Symp. Symbolic Algebraic Comp., 200-205.

Dicrescenzo, C., Duval, D. (1984). Computation on curves. Proc. EUROSAM 1984, *Springer Lec. Notes Comp. Sci.* 174, 100-107.

von zur Gathen, J. (1983a). Parallel algorithms for algebraic problems. Proc. 15th ACM Symp. Theory of Comp., 17-23.

von zur Gathen, J. (1983b). Factoring sparse multivariate polynomials. Proc. 24th IEEE Symp. Foundations Comp. Sci., 172-179.

von zur Gathen, J., Kaltofen, E. (1983). A polynomial-time algorithm for factoring multivariate polynomials over finite fields. Proc. 1983 Internat. Conf. Automata, Languages, Prog. *Springer Lec. Notes Comp. Sci.* 154, 250-263.

Heintz, J., Sieveking, M. (1981). Absolute primality of polynomials is decidable in random polynomial time in the number of variables. Proc. 1981 Internat. Conf. Automata, Languages, Prog. *Springer Lec. Notes Comp. Sci.* 115, 16-28.

Ibarra, O. H., Moran, M., Rosier, L. E. (1980). A note on the parallel complexity of computing the rank of order n matrices. *Inf. Proc. Letters* **11**, 162.

Kaltofen, E. (1982). A polynomial-time reduction from bivariate to univariate integral polynomial factorization. Proc. 23rd IEEE Symp. on Foundations of Comp. Sci., 57-64.

Kaltofen, E. (1983). Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. SIAM J. Comp., in press.

Kaltofen, E. (1984). Effective Hilbert irreducibility. Proc. EUROSAM 1984. *Springer Lec. Notes Comp. Sci.* 174, 277-284.

Lenstra, A. K., Lenstra, H. W., Lovász, L. (1982). Factoring polynomials with rational coefficients. *Math. Ann.* 261, 515-534.

Lipson, J. D. (1981). *Elements of algebra and algebraic computing*. Addison Wesley Publ. Comp., Reading Massachusetts.

Loos, R. (1982). Computing in algebraic extensions. *Computing*, Supplement 4, 173-187.

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

Ostrowski, A. (1919). Zur arithmetischen Theorie der algebraischen Grössen. Göttinger Nachrichten 1919, 279-296.

Reif, J. (1983). Logarithmic depth circuits for algebraic functions. Proc. 24th IEEE Symp. Foundations Comp. Sci., 138-144.

Schmidt, W.M. (1976). Equations over finite fields. An elementary approach. *Springer Lec. Notes Math.* 536.