Factorization of polynomials by transcendental evaluation

Marc-Paul van der Hulst
ITW, Universiteit van Amsterdam, The Netherlands

Arjen K. Lenstra
Department of Computer Science, The University of Chicago

Abstract. A new polynomial-time algorithm for the factorization of polynomials in two variables with rational coefficients is presented. The algorithm works by replacing one of the variables by an approximation of a transcendental number. It generalizes recent results by Kannan, Lenstra, Lovász [KLL] and Schönhage [Sch2]. Asymptotically the algorithm improves on the running times of previously published methods.

Introduction

It is only a few years ago that the first polynomial-time algorithm for the factorization of primitive polynomials with integral coefficients was presented [LLL]. Since that time many generalizations, applications, and even improvements of the original algorithm were published (among others [CG, Kal, KLL, Len, Sch2, vzG]).

An especially interesting result was obtained independently by Kannan, Lenstra, Lovász [KLL] and Schönhage [Sch2]. They showed that the minimal polynomial of an algebraic number can be found in polynomial time, which immediately implied another polynomial-time factorization algorithm for polynomials in $\mathbf{Z}[X]$. As Schönhage noticed, this approach to polynomial factoring, which was already suggested in [LLL], led to a considerable improvement of the worst-case running time. Therefore, it would be interesting to generalize the faster algorithm to polynomials in more variables, to get faster polynomial-time algorithms for these factoring problems as well.

The method from [KLL, Sch2], however, does not generalize in the same obvious way to more variables as was the case with the original algorithm from [LLL]. For polynomials in one variable we can compute the complex roots up to any precision that we want, and given such an approximated root we compute its minimal polynomial; for polynomials in more than one variable that approach makes no sense.

In this paper we show that we can apply the same trick for polynomials in two variables, if we first replace one of the variables by a transcendental number. After this substitution we can again compute approximations to the complex roots of the resulting univariate polynomial, and look for the minimal polynomial (over some transcendental extension of $\mathbf{Q}$) of one of the approximated roots. The fact that we have chosen a transcendental evaluation point then guarantees that this minimal polynomial corresponds to an irreducible factor of the original bivariate polynomial.

For the running time analysis of our algorithm it is important to have strictly positive lower bounds for polynomials in $\mathbf{Z}[Y]$ when evaluated in a transcendental number. Such a lower bound is called a *transcendence measure* of the transcendental number, and for many transcendental numbers a transcendence measure is known. The running time of our algorithm strongly depends on the transcendence measure of the chosen transcendental number. There exist transcendental numbers (like for instance π) which make the algorithm asymptotically faster than any other known algorithm for the factorization of bivariate polynomials. See also Remark (3.3).

The new method can be generalized to polynomials in more than two variables by application of *simultaneous transcendence measures*. As was the case with the generalizations of the $\mathbf{Z}[X]$-algorithm [Len], the practical importance of the resulting algorithm becomes rather questionable. For two variables it is not unlikely that the algorithm may prove to have practical significance.

1. Preliminaries

For a polynomial $g = \sum_i \sum_j g_{ij} X^i Y^j \in \mathbf{C}[X, Y]$ we denote by $\delta_X g$ and $\delta_Y g$ its *degree* in X and Y respectively, by $|g| = (\sum_{i=0}^{\delta_X g} \sum_{j=0}^{\delta_Y g} |g_{ij}|^2)^{1/2}$ its *length*, and by $g_{\max} = \max_{0 \le i \le \delta_X g,\, 0 \le j \le \delta_Y g} |g_{ij}|$ its *height*.

(1.1) Definition. For a transcendental number λ we define its *transcendence measure* B_λ as a positive function B_λ: $\mathbf{N} \times \mathbf{N} \to \mathbf{R}$ such that $|g(\lambda)| > B_\lambda(n, H)$ for all non-trivial polynomials $g \in \mathbf{Z}[Y]$ satisfying $\delta_Y g \le n$ and $g_{\max} \le H$.

(1.2) Example. In [Cij] transcendence measures for many well known transcendental numbers are given. For e we have $B_e(n, H) = e^{-c_1 n^2 (n + \log H)}$, and for π we have $B_\pi(n, H) = e^{-c_2 n (n + \log H)(1 + \log n)^2}$, for effectively computable constants $c_1 > 0$ and $c_2 > 0$ (cf. Remark (3.3)).

For the rest of this section we denote by f a primitive polynomial in $\mathbf{Z}[X, Y]$ with $\delta_X f = n > 0$, $\delta_Y f = m > 0$ and height $f_{\max}$. The idea of our algorithm to determine the irreducible factors of f in $\mathbf{Z}[X, Y]$ is as follows: replace the variable Y in $f(X, Y) \in \mathbf{Z}[X, Y]$ by a transcendental number λ, and look for a factorization of $f(X, \lambda)$ in $\mathbf{Q}(\lambda)[X]$. Because λ is transcendental, $\mathbf{Q}(\lambda)$ is isomorphic to $\mathbf{Q}(Y)$, so that the factorization of $f(X, \lambda)$ in $\mathbf{Q}(\lambda)[X]$ automatically yields a factorization of $f(X, Y)$ in $\mathbf{Q}(Y)[X]$. It then follows from Gauss' lemma that this factorization in $\mathbf{Q}(Y)[X]$ is essentially a factorization in $\mathbf{Z}[X, Y]$.

By $\lambda \in \mathbf{R}$ we denote a transcendental number with transcendence measure B_λ and $|\lambda| < 1/2$. Obviously, we cannot work with λ, but we will have to work with some approximation $\bar{\lambda}$ to λ. Therefore, we denote by $\bar{\lambda}_k \in \mathbf{Q}$ for $0 \le k \le m$ approximations to λ^k (where $\bar{\lambda}_0 = 1$).

The polynomial $f_{\bar{\lambda}} \in \mathbf{Q}[X]$ is defined as the polynomial that we get from f by replacing Y^k by $\bar{\lambda}_k$ for $1 \le k \le m$. In the algorithm we will work with $f_{\bar{\lambda}}$ instead of $f(X, \lambda)$. Consequently, we will not be approximating a root of $f(X, \lambda)$, but instead a root of the approximated polynomial $f_{\bar{\lambda}}$. We may assume that $f_{\bar{\lambda}}$ has a root with absolute value at most 1 (see Section 2). Namely, otherwise we consider the polynomial $X^n f(1/X, Y)$ instead of f. We now investigate how close λ should be approximated to be able to approximate a root of $f(X, \lambda)$.

(1.3) Lemma. *(cf. [Ost, Appendix A]) Let* $f = \sum_{i=0}^n f_i X^i$, $\bar{f} = \sum_{i=0}^n \bar{f}_i X^i \in \mathbf{C}[X]$ *be two polynomials of degree* $n > 0$ *and let* $\Delta = \max_{0 \le i \le n} |f_i - \bar{f}_i|$. *Suppose that* $\bar{f}$ *has a root* $\beta \in \mathbf{C}$ *satisfying* $|\beta| \le 1$. *Then there exists a zero* $\alpha \in \mathbf{C}$ *of* f *such that*

$$|\beta - \alpha| \le \left(\frac{(n+1)\Delta}{|f_n|} \right)^{1/n}.$$

Proof. Because $f(X)-\bar{f}(X) = \sum_{i=0}^{n}(f_i-\bar{f}_i)X^i$, we get $|f(\beta)| \leq \Delta\sum_{i=0}^{n}|\beta|^i$. Also, $|f(\beta)| = |f_n|\prod_{i=1}^{n}|\beta-\alpha_i|$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the zeros of f. The lemma easily follows. □

(1.4) **Corollary.** *Let f, n, m, $f_{\max}$, λ, B_λ, $\bar{\lambda}_k$, and $f_{\bar{\lambda}}$ be as above, and let s be a positive integer. If*

$$|\lambda^k-\bar{\lambda}_k| \leq \frac{B_\lambda(m, f_{\max})}{2^{sn+n}(n+1)mf_{\max}} \text{ for } 1 \leq k \leq m, \tag{1.5}$$

then a 2^{-s-1}-approximation of a zero of absolute value at most 1 of $f_{\bar{\lambda}}$ is a 2^{-s}-approximation of a zero of $f(X, \lambda)$.

Proof. Let $f(X, \lambda) = \sum_{i=0}^{n}f_iX^i$, and $f_{\bar{\lambda}}(X) = \sum_{i=0}^{n}\bar{f}_iX^i$. According to Lemma (1.3) it suffices to prove that

$$\left(\frac{(n+1)\max_i|f_i-\bar{f}_i|}{|f_n|}\right)^{1/n} < 2^{-s-1}.$$

To prove this we notice that $|f_n| > B_\lambda(m, f_{\max})$ and that $\max_i|f_i-\bar{f}_i| \leq f_{\max}\sum_{k=1}^{m}|\lambda^k-\bar{\lambda}_k|$. The proof now follows from (1.5). □

Let s be a positive integer such that

$$(1+2^{-s})^n \leq 2, \tag{1.6}$$

and let $\bar{\lambda}_k$ for $1 \leq k \leq m$ be chosen such that (1.5) holds. Suppose that we have computed a 2^{-s-1}-approximation $\bar{\alpha} \in \mathbf{Q}(i)$, $|\bar{\alpha}| \leq 1$, to a root of absolute value at most 1 of $f_{\bar{\lambda}}$. According to Corollary (1.4), $\bar{\alpha}$ is a 2^{-s}-approximation to a root $\alpha \in \mathbf{C}$ of $f(X, \lambda)$; it follows that $|\alpha| \leq 1+2^{-s}$. Furthermore, let $\beta_{jk} \in 2^{-s}\mathbf{Z}[i]$ for $0 \leq j \leq n$ and $0 \leq k \leq m$ be approximations to $\alpha^j\lambda^k$ (where $\beta_{00} = 1$).

By $h \in \mathbf{Z}[\lambda][X]$ we denote the minimal polynomial of α, so h divides $f(X, \lambda)$, and h is irreducible. (So, h is the minimal polynomial in $\mathbf{Q}(\lambda)[X]$ of α normalized in such a way that h is contained in $\mathbf{Z}[\lambda][X]$ and such that h is of minimal degree in λ.) We identify this polynomial h with the polynomial in $\mathbf{Z}[X, Y]$ which is obtained by replacing λ by Y. This means that $h \in \mathbf{Z}[X, Y]$ is an irreducible factor of $f \in \mathbf{Z}[X, Y]$ such that $h(\alpha, \lambda) = 0$.

For a polynomial $g = \sum_j\sum_k g_{jk}X^jY^k \in \mathbf{Z}[X, Y]$ satisfying $\delta_Xg \leq n$ and $\delta_Yg \leq m$, we denote $g_\beta = \sum_{j=0}^{n}\sum_{k=0}^{m}g_{jk}\beta_{jk} \in 2^{-s}\mathbf{Z}[i]$, where $g_{jk} = 0$ for $\delta_Xg < j \leq n$ or $\delta_Yg < k \leq m$.

We will need an upper bound on $|g(\alpha, \lambda)-g_\beta|$.

(1.7) **Lemma.** *Let n, m, λ, s, α, β_{jk}, and g be as above. If*

$$|\alpha^j\lambda^k-\beta_{jk}| \leq 2^{-s+1} \tag{1.8}$$

for $0 \leq j \leq n$ and $0 \leq k \leq m$, then

$$|g(\alpha, \lambda)-g_\beta| \leq 2^{-s+1}g_{\max}(nm+n+m).$$

Proof. Immediate. □

The following lemma gives a minimum for $|g(\alpha, \lambda)|$ when $g(\alpha, \lambda) \neq 0$.

(1.9) **Lemma.** *Let f, n, m, $f_{\max}$, λ, B_λ, s, α, h, and g be as above, and suppose that h does not divide g. Then*

(1.10) $$|g(\alpha, \lambda)| > \frac{B_\lambda(N_{f,g}, B_{f,g})}{4nB_{f,g}},$$

where $B_{f,g} = (e^{n+m} f_{\max} g_{\max} (n+1)(m+1)^2)^n$ *and* $N_{f,g} = 2nm$.

Proof. If $\delta_X g = 0$ then $g(\alpha, Y) = g(Y) \in \mathbf{Z}[Y]$, so that (1.10) follows from $g(\lambda) > B_\lambda(\delta_Y g, g_{\max})$.

Now let $\delta_X g > 0$. Because h is irreducible and h does not divide g we have that gcd$(h, g) = 1$. This implies that there exists a non-zero polynomial $R \in \mathbf{Z}[Y]$ and polynomials $a, b \in \mathbf{Z}[X, Y]$ such that $a \cdot h + b \cdot g = R$, satisfying $\delta_Y R \leq m\delta_X g + n\delta_Y g \leq N_{f,g}$, $\delta_X a \leq \delta_X g - 1$, $\delta_Y a \leq m(\delta_X g - 1) + n\delta_Y g$, $\delta_X b \leq n-1$, $\delta_Y b \leq m\delta_X g + (n-1)\delta_Y g$. Here we used that $\delta_X h \leq n$ and $\delta_Y h \leq m$ because h divides f.

Another consequence of the fact that h divides f is that

$$h_{\max} \leq e^{n+m} f_{\max}$$

[Gel]. From [GG] we then find

(1.11) $$R_{\max} \leq |R| \leq B_{f,g},$$

so that

(1.12) $$|R(\lambda)| > B_\lambda(N_{f,g}, B_{f,g}).$$

From $|\alpha|^j \leq (1+2^{-s})^n \leq 2$ (cf. (1.6)) and $|\lambda| < 1/2$ we derive

$$|b(\alpha, \lambda)| \leq b_{\max} \sum_{j=0}^{n-1} \sum_{k=0}^{N_{f,g}} |\alpha^j||\lambda^k| \leq 4nb_{\max}.$$

Combined with (1.12) this implies (1.10), because (1.11) also holds with R replaced by b, and because $b(\alpha, \lambda) \cdot g(\alpha, \lambda) = R(\lambda)$ (so that $b(\alpha, \lambda) \neq 0$). □

Define $\overline{g}$ as the $((n+1)(m+1)+2)$-dimensional vector $(g_{00}, g_{01}, \ldots, g_{nm}, 2^s \cdot \mathrm{Re}(g_\beta), 2^s \cdot \mathrm{Im}(g_\beta))^T \in \mathbf{Z}^{(n+1)(m+1)+2}$. By $|\overline{g}|$ we denote the Euclidean length of the vector $\overline{g}$.

Finally we show how s should be chosen.

(1.13) **Lemma.** *Let f, n, m, λ, B_λ, s, α, β_{jk}, h, and g be as above. Suppose that s is chosen in such a way that*

(1.14) $$2^s \geq \frac{2^{(nm+3(n+m)+2)/2}|f|(n+1)^2(m+1)^2 8nB}{B_\lambda(2nm, B)},$$

where $B = (e^{n+m} 2^{(nm+3(n+m)+2)/2} f_{\max} |f| (n+1)^2(m+1)^3)^n$. *Then*

$$|\overline{h}| < 2^{n+m+1}|f|(n+1)(m+1)$$

and if

$$|\overline{g}| < 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1)$$

then h divides g.

Proof. First remark that (1.14) implies that (1.6) holds. This implies that Lemma (1.9) may be applied.

Because h divides f we have $\delta_X h \leq n$ and $\delta_Y h \leq m$ so that $|\overline{h}|$ is well defined, and from [Mah] we have

$$h_{\max} \leq |h| \leq 2^{n+m}|f|.$$

Combined with $h(\alpha, \lambda) = 0$ and Lemma (1.7) the upper bound on $|\bar{h}|$ follows:

$$\begin{aligned} |\bar{h}|^2 &= |h|^2 + 2^{2s}|h_\beta|^2 \\ &\leq (2^{n+m}|f|)^2 + 2^{2s}(2^{-s+1}2^{n+m}|f|(nm+n+m))^2 \\ &= (2^{n+m}|f|)^2(1+4(nm+n+m)^2) \\ &< (2^{n+m+1}|f|(n+1)(m+1))^2. \end{aligned}$$

Now assume that $|\bar{g}| < 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1)$. Because $|\bar{g}|^2 = |g|^2 + 2^{2s}|g_\beta|^2$ we find

$$g_{\max} \leq |g| < 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1) \tag{1.15}$$

and

$$2^s|g_\beta| < 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1). \tag{1.16}$$

From Lemma (1.7) it follows that

$$|g(\alpha, \lambda)| \leq 2^{-s+1}g_{\max}(nm+n+m) + |g_\beta|.$$

Combining this with (1.15) and (1.16) we find

$$\begin{aligned} |g(\alpha, \lambda)| &\leq 2^{-s}2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1)(2(nm+n+m)+1) \\ &< 2^{-s+1}2^{(nm+3(n+m)+2)/2}|f|(n+1)^2(m+1)^2 \end{aligned}$$

and with (1.14)

$$|g(\alpha, \lambda)| \leq \frac{B_\lambda(2nm, B)}{4nB}. \tag{1.17}$$

From (1.15) it follows that $B > (e^{n+m}f_{\max}g_{\max}(n+1)(m+1)^2)^n$, so that it follows from (1.17) that $g(\alpha, \lambda)$ does not satisfy (1.10). Lemma (1.9) therefore yields that h divides g. □

(1.18) Let $n_0, m_0 \in \mathbf{Z}_{\geq 0}$ be such that $n_0 \leq n$ and $m_0 \leq m$, and let $M = n_0(m+1)+m_0+1$. We will regard the lattice $\mathbf{Z}^M$ as the set of polynomials $g = \sum_j \sum_k g_{jk} X^j Y^k \in \mathbf{Z}[X, Y]$ for which

i) $\delta_X g \leq n_0$,
ii) $\delta_Y g \leq m$,
iii) $g_{n_0 k} = 0$ for $m_0+1 \leq k \leq m$.

We embed $\mathbf{Z}^M$ into $\mathbf{Z}^{(n+1)(m+1)}$ by adding zero coefficients to g and writing $g = \sum_{j=0}^{n} \sum_{k=0}^{m} g_{jk} X^j Y^k$. The M-dimensional lattice L contained in $\mathbf{Z}^{(n+1)(m+1)+2}$ is then defined as $\{\bar{g} \mid g \in \mathbf{Z}^M\}$, where $\bar{g}$ is defined as $(g_{00}, g_{01}, \ldots, g_{nm}, 2^s \cdot \mathrm{Re}(g_\beta), 2^s \cdot \mathrm{Im}(g_\beta))^T$. For $\bar{z} \in L$ we denote by z the polynomial in $\mathbf{Z}[X, Y]$ satisfying i), ii), and iii), consisting of the first M coordinates of $\bar{z}$. (Of course, L can also be seen as a lattice in $\mathbf{Z}^{M+2}$.)

Let $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_M$ be a reduced basis for L [LLL, (1.4), (1.5)]. According to [LLL, (1.11)] we have

$$|\bar{b}_1| \leq 2^{(M-1)/2}|\bar{z}|, \tag{1.19}$$

for every $\bar{z} \in L$, $\bar{z} \neq 0$, where || denotes the ordinary Euclidean length.

(1.20) **Lemma.** *Let f, n, m,λ, B_λ, s, h, n_0, m_0, M, L, and $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_M$ be as above such that (1.14) holds.*

i) If $\bar{h} \notin L$ then

$$|\overline{b}_1| \geq 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1).$$

ii) If M is minimal such that $\overline{h} \in L$, then $h = \pm b_1$ and in particular

$$|\overline{b}_1| < 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1).$$

Proof. If $\overline{h} \notin L$ then for all $\overline{x} \in L$, $\overline{x} \neq 0$, the polynomial h cannot divide x. Because of (1.14), Lemma (1.13) then yields that $|\overline{b}_1| \geq 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1)$. This proves i).

We now prove ii). If $\overline{h} \in L$ then $|\overline{b}_1| \leq 2^{(M-1)/2}|\overline{h}|$ according to (1.19), so that with (1.14) and the upper bound on $|\overline{h}|$ from Lemma (1.13) we find $|\overline{b}_1| < 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1)$. This implies, again by Lemma (1.13), that h divides b_1. Because M is minimal such that $\overline{h} \in L$ it follows that $b_1 = d \cdot h$ for some $d \in \mathbf{Z}_{\neq 0}$, and because $\overline{h} \in L$ and $\overline{b}_1$ is contained in a basis for L we conclude that $d = \pm 1$. □

2. The algorithm

Let $f \in \mathbf{Z}[X, Y]$ with $\delta_X f = n$ and $\delta_Y f = m$ be primitive. In this section we present an algorithm to compute an irreducible factor of f that is based on Lemma (1.20).

(2.1) First select a transcendental number $\lambda \in \mathbf{R}$, $|\lambda| < 1/2$, for which a transcendence measure B_λ is known and such that the bits of λ can be computed efficiently. Take $s \in \mathbf{Z}$ minimal such that (1.14) holds, and compute $\overline{\lambda}_k \in \mathbf{Q}$ for $0 \leq k \leq m$ such that (1.5) holds (where $\overline{\lambda}_0 = 1$). Define $f_{\overline{\lambda}} \in \mathbf{Q}[X]$ by replacing Y^k in $f(X, Y)$ by $\overline{\lambda}_k$ for $0 \leq k \leq m$. It may be assumed that $f_{\overline{\lambda}}$ has a root of absolute value at most 1 (otherwise replace $f_{\overline{\lambda}}(X)$ by $X^n f_{\overline{\lambda}}(1/X)$). This can be decided by means of the splitting circle method (see [Sch1]).

Next, apply the algorithm from [Sch1] to compute a 2^{-s-1}-approximation $\overline{\alpha}$ to a zero of absolute value at most 1 of $f_{\overline{\lambda}}$. Denote by $\alpha \in \mathbf{C}$ a root of $f(X, \lambda)$ such that $\overline{\alpha}$ is a 2^{-s}-approximation to α (Corollary (1.4)). Compute $\beta_{jk} \in 2^{-s}\mathbf{Z}(i)$ for $0 \leq j \leq n$ and $0 \leq k \leq m$ (where $\beta_{00} = 1$) such that (1.8) holds. Notice that in order to achieve this, one has to compute sufficiently precise approximations to the powers of α.

Finally determine the irreducible $h \in \mathbf{Z}[X, Y]$ such that $h(\alpha, \lambda) = 0$. This is done as follows. For $n_0 = 1, 2, \ldots, n-1$ in succession, and for each value of n_0 for $m_0 = 0, 1, \ldots, m$ in succession do the following. Put $M = n_0(m+1)+m_0+1$, and define the M-dimensional lattice L contained in $\mathbf{Z}^{(n+1)(m+1)+2}$ as in (1.18). Compute a reduced basis $\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_M$ for L by means of the basis reduction algorithm [LLL, Section 1]. Stop for the smallest M for which $|\overline{b}_1| < 2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1)$ and put $h = \pm b_1$ (where b_1 is defined as in (1.18)). If this does not occur for any of the M values, then put $h = f$.

This finishes the description of Algorithm (2.1).

(2.2) **Remark.** The condition in the last step of Algorithm (2.1) follows from the results of the previous section. If $\overline{h} \notin L$, i.e. M is still too small, then $\overline{b}_1$ has length at least $2^{(nm+3(n+m)+2)/2}|f|(n+1)(m+1)$ according to Lemma (1.20).

3. Running time analysis

Obviously the running time of Algorithm (2.1) strongly depends on the transcendence measure B_λ of the transcendental number λ chosen in (2.1). We analyse the running time for the choice $\lambda = \pi-3$, so that $|\lambda| < 1/2$ and $B_\lambda(n, H) = e^{-cn(n+\log H)(1+\log n)^2}$ for some $c > 0$ (cf. Example (1.2)). This implies that s can be chosen such that

(3.1) $$s = O((n^3m^2+n^2m\log|f|)\log^2(nm)) .$$

According to [Sch1] a 2^{-s-1}-approximation $\bar{\alpha}$ to a root of absolute value at most one of $f_{\bar{\lambda}}$, where the $\bar{\lambda}_k$ satisfy (1.5), can be computed in $O(n^2(\max(s, n\log|f_{\bar{\lambda}}|)^{1+\epsilon}))$ bit operations. With $\log|f_{\bar{\lambda}}| = O((n^4m^2+n^3m\log|f|)\log^2(nm))$ (cf. (1.5) and (3.1)) this yields

$$O(n^2((n^5m^2+n^4m\log|f|)\log^2(nm))^{1+\epsilon})$$

bit operations to compute $\bar{\alpha}$.

Let G denote an upper bound for the Gramian determinants of the initial bases of the lattices considered in (2.1). From the proof of [LLL, (1.26)] and [LLL, (1.37)] we find that all applications of the basis reduction algorithm can be done in $O(\bar{n}^3m^3\log G)$ operations on integers having $O(\log G)$ binary bits, where $\bar{n} = \delta_Xh$. An upper bound on $\log G$ follows for this type of lattice from [Sch2, lemma (6.1)], namely

$$G \leq (1+2^{2s}\bar{M})^2$$

(where $\bar{M} \leq \bar{n}(m+1)+m+1$), so that, with (3.1)

$$\log G = O((n^3m^2+n^2m\log|f|)\log^2(nm)).$$

Therefore

$$O(\bar{n}n^2m^3((n^3m^2+n^2m\log|f|)\log^2(nm))^{2+\epsilon})$$

bit operations suffice to compute h (clearly, this number of bit operations also suffice to compute the $\bar{\lambda}_k$) .

Because $|f/h| \leq 2^{n+m}|f|$ [Mah], the complete factorization of f can be found in

$$O(n^3m^3((n^3m^2+n^2m\log|f|)\log^2(nm))^{2+\epsilon})$$

bit operations.

(3.2) **Remark.** The running time of our algorithm can be improved by a factor nm if we use Schönhage's speed-up of the basis reduction algorithm [Sch2]. Because the analogue of [LLL, (1.37)] does not hold for this modified basis reduction algorithm, the formulation of Algorithm (2.1) should be changed. Instead of taking $M = m+2, m+3, \ldots$ up to at most $n(m+1)$ in succession, we have to double the dimension each time no short vector is found. This method is described in detail in [LLL, (3.3)] (cf. [LLL, (3.10)]).

(3.3) **Remark.** Throughout this paper the transcendental number λ can be replaced by any algebraic number γ of sufficiently high degree, like for instance a sufficiently large integer (or a sufficiently small rational number). It is not difficult to see that the proofs are essentially unaffected by this change, and that the resulting algorithm has a slightly better running time (namely, the same running time without the $\log(nm)$ factors). This also implies that we do not have to worry about the actual size of the constant c involved in the transcendence measure of λ, because this constant does not occur in the new formulae.

Choosing such an alternative evaluation point γ for Y might however change the factorization of $f(X, \gamma)$. Because all factors of $f(X, Y)$ have height bounded by $2^{n+m}|f|$, we can restrict our attention to factors of $f(X, \gamma)$ that satisfy this same upper bound on their height, i.e. vectors in L with entries in absolute value at most $2^{n+m}|f|$ in the first M coordinates. It follows from the adapted version of Lemma (1.13) that we then only find those factors of $f(X, \gamma)$ that correspond to factors of $f(X, Y)$.

Generalization to polynomials in more than two variables follows in the obvious way.

References

CG A.L. Chistov, D.Yu. Grigoryev, Polynomial-time factoring of the multivariable polynomials over a global field, Lomi, preprint E-5-82, Leningrad 1982.

Cij P.L. Cijsouw, Transcendence measures, Ph.D. Thesis, University of Amsterdam, 1972.

Gel A.O. Gel'fond, Transcendental and algebraic numbers, Dover Publ., New York 1960.

GG A.J. Goldstein, R.L. Graham, A Hadamard-type bound on the coefficients of a determinant of polynomials, SIAM Rev. **16** (1974), 394-395.

Kal E. Kaltofen, On the complexity of factoring polynomials with integer coefficients, Ph.D. Thesis, Rensselaer Polytechnic Institute, 1982.

KLL R. Kannan, A.K. Lenstra, L. Lovász, Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers, Proceedings 16th STOC, 1984.

Len A.K. Lenstra, Polynomial-time algorithms for the factorization of polynomials, Ph.D. Thesis, University of Amsterdam, 1984.

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

Mah K. Mahler, On some inequalities for polynomials in several variables, J. London Math. Soc. **37** (1962), 341-344.

Ost A.M. Ostrowski, Solution of equations and systems of equations, Academic Press, New York 1966.

Sch1 A. Schönhage, The fundamental theorem of algebra in terms of computational complexity, Preliminary report, Math. Inst. Univ. Tübingen, 1982.

Sch2 A. Schönhage, Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm, 11th Colloquium on automata, languages and programming, Lecture notes in computer science 172, Springer Verlag, Berlin, 1984, 436-447.

vzG J. Von Zur Gathen, Hensel and Newton methods in valuation rings, Math. Comp. **42**, (1984), 637-661.