Publ. Math. Debrecen
39 / 1-2 (1991), 163-169

Complexity investigations on decomposable form equations

By ATTILA PETHŐ* (Debrecen)

Let $\mathbf{Q}$ and $\mathbf{Z}$ denote the field of rational numbers and the ring of integers, respectively. Let $F(x_1,\dots,x_k) \in \mathbf{Z}[x_1,\dots,x_k]$ be a form of degree n. F is called *decomposable* if it factorizes into linear factors over some finite extension of $\mathbf{Q}$.

Let F be a decomposable form and $m \in \mathbf{Z}\setminus\{0\}$. Decomposable form equations of type

$$F(x_1,\dots,x_k) = m, \quad \text{in } x_1,\dots,x_k \in \mathbf{Z} \tag{1}$$

are of basic importance in the theory of diophantine equations, and have many applications in algebraic number theory. For basic results we refter to BOREVICH and SHAFAREVICH [1], SCHMIDT [7], [8], [9], GYŐRY [3], [4], EVERTSE and GYŐRY [2] and the references therein.

A decomposable form F is called *degenerate* if there exists an integer m such that (1) has infinitely many solutions. It is easy to see that all binary forms are decomposable, and by a result of Siegel [12] it is decidable without the factorization of F whether it is degenerate. For the sake of completeness, in Section 2 we also deal with binary forms.

In general we can decide, using the results of SCHMIDT [7] or EVERTSE and GYŐRY [2], whether F is degenerate, only if its factorization is known. The main goal of this paper is to give in Section 4, an algorithm for the factorization of F. In Section 5, we prove that the running time of the algorithm is bounded by $O(k^2n^6\log^2(2kn|F|)\log\log(2kn|F|))$, where $|F|$ denotes the height of the polynomial F.

In comparison with general methods for the factorization of multivariate polynomials, for example with the method of HULST and LENSTRA [5], our algorithm seems to be more realistic for this special problem.

I am very grateful for the referee for several suggestions which make the presentation more clear.

*Research supported by Hungarian National Foundation for Scientific Research Grant No. 273/86.

2. Binary forms

Theorem 1. *Let $F(x,y) = F_0x^n + F_1x^{n-1}y + \cdots + F_nx^n \in \mathbf{Z}[x,y]$. It is decidable in at most $O(n^2 \log^2 F' \log\log F')$ additions, subtractions, multiplications and divisions whether F is degenerate, where $F' = \max\{|F_0|, \ldots, |F_n|, 3\}$.*

PROOF. By a theorem of Siegel [12, Zweiter Teil], F is degenerate iff there exist integers a, b, c, d such that either

$$F(x,y) = a(bx+cy)^n \tag{2}$$

or n is even and

$$F(x,y) = a(bx^2+cxy+dy^2)^{n/2}, \tag{3}$$

with $c^2 - 4bd > 0$.

We shall analyse only the first alternative. We may assume that $(b,c) = 1$, hence $a = (F_0, \ldots, F_n)$, $b = \frac{F_0}{a} / \left(\frac{F_0}{a}, \frac{F_1}{na}\right)$ and $c = \frac{F_1}{an} / \left(\frac{F_0}{a}, \frac{F_1}{an}\right)$. So a, b and c can be computed in at most $O(n \log^2 F' \log\log F')$ operations using fast multiplication techniques.

Equations (2) is true iff $F(x,b) = ab^n(x+c)^n$. For the comparison of these two polynomials one needs at most $O(n^2 \log^2 F' \log\log F')$ operations. The analysis of (3) is similar and Theorem 1 is proved.

3. Auxiliary lemmas

In the sequel $|F|$ will denote the height of the polynomial $F \in \mathbf{Q}[x_1, \ldots, x_k]$, i.e. the maximum of the absolute values of the coefficients of F. Further $\underline{e}_t$ $(t = 1, \ldots, k-1)$ will denote the $k-1$–dimensional vector with t–th coordinate 1 and all other coordinates 0.

Lemma 1. *Let $F(x_1, \ldots, x_k)$ be a decomposable form of degree n such that $F(1,0,\ldots,0) = f_n \neq 0$. Take $L_3 = (4|F|)^{n(n-1)+1}$ and $L_t = L_3(L_3+1)^{t-3}$, $t = 3, \ldots, k$. Denote by $\alpha_{t,j}$ and $\beta_{t,j}$ the roots of the polynomials $F(x, \underline{e}_{t-1})$ and $F(x, 1, L_3, \ldots, L_t, 0, \ldots, 0)$, respectively, for $t = 2, \ldots, k$; $j = 1, \ldots, n$. Then*

$$|f_n|\ |\alpha_{t,j} - \alpha_{t,h}| \le 4|F|, \qquad 1 \le j,h \le n;\ 2 \le t \le k, \tag{4}$$

$$|\alpha_{t,j} - \alpha_{t,h}| \ge 4(4|F|)^{-n(n-1)} \tag{5}$$

hold for all $1 \le j,h \le n$; $2 \le t \le k$ such that $\alpha_{t,j} \neq \alpha_{t,h}$. Further,

$$|f_n|\ |\beta_{t,j} - \beta_{t,h}| \le 4|F|(L_3+1)^{t-2}, \qquad 1 \le j,h \le n;\ 2 \le t \le k, \tag{6}$$

(7) $$|\beta_{t,j} - \beta_{t,h}| \geq 4(4|F|)^{-n(n-1)}$$

hold for all $1 \leq j, h \leq n$; $2 \leq t \leq k$ *such that* $\beta_{t,j} \neq \beta_{t,h}$. *Finally,*

(8) $$|\beta_{t-1,j} - \beta_{t-1,h}| < L_t|\alpha_{t,u} - \alpha_{t,v}|$$

hold for all $1 \leq j, h, u, v \leq n$ *with* $\alpha_{t,u} \neq \alpha_{t,v}$.

PROOF. Let $2 \leq t \leq k$ be fixed, and $F(x, \underline{e}_{t-1}) = f_{n,t}\, x^n + \cdots + f_{0,t}$. Then $f_{n,t} = f_n$ and $|F(x, \underline{e}_{t-1})| \leq |F|$ because $F(1, 0, \ldots, 0) = f_n$ and $f_{s,t}$ is the coefficient of the term $x_1^s x_t^{n-s}$ in $F(x_1, \ldots, x_k)$. By Hilfssatz 1 of SCHNEIDER [10], we have $|f_n \alpha_{t,j}| \leq 2|F|$, hence (4) is true.

Let $A = \{\alpha_{t,1}, \ldots, \alpha_{t,j_t}\}$ be the set of all distinct roots of $F(x, \underline{e}_{t-1})$, and denote by $\mathbf{N}$ the splitting field of $F(x, \underline{e}_{t-1})$. Then we have $A^\sigma = A$ for all elements σ of the Galois group of the field extension $\mathbf{N}/\mathbf{Q}$. Further, $f_n \alpha_{t,j}$, $1 \leq j \leq n$ are algebraic integers, hence $\prod_{i=1}^{j_t} (x - f_n \alpha_{t,i}) \in \mathbf{Z}[x]$, and so its discriminant $\prod_{1 \leq i,j \leq j_t} f_n(\alpha_{t,i} - \alpha_{t,j})$ is a non-zero integer. Combining this with (4) we get (5) at once.

Since F is a decomposable form,

$$F(x_1, \ldots, x_k) = f_n \prod_{j=1}^{n} (x_1 + \alpha_{2,j} x_2 + \cdots + \alpha_{k,j} x_k),$$

which means that $\alpha_{2,j} + L_3 \alpha_{3,j} + \cdots + L_t \alpha_{t,j}$, $j = 1, \ldots, n$ are all the roots of $F(x, 1, L_3, \ldots, L_t, 0, \ldots, 0)$. Therefore

(9) $$\beta_{t,j} = \alpha_{2,j} + L_3 \alpha_{3,j} + \cdots + L_t \alpha_{t,j}, \quad j = 1, \ldots, n$$

holds after possible changes of the subscripts. (9) implies

$$|f_n|\, |\beta_{t,j} - \beta_{t,h}| \leq 4|F|(1 + L_3 + \cdots + L_t).$$

It is easy to derive

$$1 + L_3 + \cdots + L_t = (L_3 + 1)^{t-2}, \quad t = 2, \ldots, k$$

from the definition of the L's, which proves (6).

By (5), inequality (7) is true for $t = 2$. Assume that it is true for a t with $2 \leq t \leq k$. We have $\beta_{t+1,j} = \beta_{t,j} + L_{t+1} \alpha_{t+1,j}$ by (9). Let j and h be chosen so that $\beta_{t+1,j} \neq \beta_{t+1,h}$. If $\alpha_{t+1,j} = \alpha_{t+1,h}$, then we have (7) by the induction hypothesis. In the opposite case we get

$$|\beta_{t+1,j} - \beta_{t+1,h}| \geq L_{t+1} |\alpha_{t+1,j} - \alpha_{t+1,h}| - |\beta_{t,j} - \beta_{t,h}| > 12|F|(L_3 + 1)^{t-2} > 4(4|F|)^{-n(n-1)}$$

by (5) and (6).

Finally (6) and (5) imply

$$|\beta_{t-1,j} - \beta_{t-1,h}| \leq 4|F|(L_3 + 1)^{t-3} < L_t |\alpha_{t,u} - \alpha_{t,v}|.$$

Lemma 2. *Let $F(x_1, \dots, x_k)$, $\alpha_{t,j}$ and $\beta_{t,j}$ be the same as in Lemma 1. Let $\bar{\alpha}_{t,j}, \bar{\beta}_{t,j} \in \mathbf{Q}(i)$ be the approximations to $\alpha_{t,j}$ and $\beta_{t,j}$ respectively, such that*

$$(10) \qquad |\alpha_{t,j} - \bar{\alpha}_{t,j}| \le (2kn|F|)^{-k(n+1)^2}, \quad t = 2, \dots, k;\ j = 1, \dots, n,$$

$$(11) \qquad |\beta_{t,j} - \bar{\beta}_{t,j}| \le (4|F|)^{-n^2}, \quad t = 2, \dots, k;\ j = 1, \dots, n,$$

Then

$$(12) \qquad |\bar{\beta}_{t-1,j} - \bar{\beta}_{t,u} + L_t \bar{\alpha}_{t,v}| < 3(4|F|)^{-n(n-1)}$$

holds iff $\beta_{t,u} = \beta_{t-1,j} + L_t \alpha_{t,v}$.

PROOF. Let $1 \le u, j, v \le n$ be such that $\beta_{t,u} = \beta_{t-1,u} + L_t \alpha_{t,u} \neq \beta_{t-1,j} + L_t \alpha_{t,v}$. Then one can prove

$$(13) \qquad |\beta_{t-1,j} - \beta_{t,u} + L_t \alpha_{t,v}| > 4(4|F|)^{-n(n-1)}$$

with the same argument as (7). Using (10), (11) and (13) we get

$$|\bar{\beta}_{t-1,j} - \bar{\beta}_{t,u} + L_t \bar{\alpha}_{t,v}| \ge |\beta_{t-1,j} - \beta_{t,u} + L_t \alpha_{t,v}| - |\beta_{t,u} - \bar{\beta}_{t,u}| - \\ |\beta_{t-1,j} - \bar{\beta}_{t-1,j}| - L_t |\alpha_{t,v} - \bar{\alpha}_{t,v}| \ge 3(4|F|)^{-n(n-1)}.$$

On the other hand, if $\beta_{t,u} = \beta_{t-1,j} + L_t \alpha_{t,v}$, then

$$|\bar{\beta}_{t-1,j} - \bar{\beta}_{t,u} + L_t \bar{\alpha}_{t,v}| \le |\beta_{t,u} - \bar{\beta}_{t,u}| + |\beta_{t-1,j} - \bar{\beta}_{t-1,j}| + \\ L_t |\alpha_{t,v} - \bar{\alpha}_{t,v}| < (4|F|)^{-n(n-1)}.$$

Lemma 2 is proved.

4. The algorithm

Let $F(x_1, \dots, x_k) \in \mathbf{Z}[x_1, \dots, x_k]$. If $F \neq 0$, then there exist integers $T_2, \dots, T_k$ such that if $G(y_1, \dots, y_k) = F(y_1, T_2 y_1 + y_2, \dots, T_k y_1 + y_k)$ then $G(y_1, \dots, y_k) \in \mathbf{Z}[y_1, \dots, y_k]$ and $G(1, 0, \dots, 0) \neq 0$ (see Borevich and Shafarevich [1, Ch.II.1.]). Hence we may assume without loss of generality that $F(1, 0, \dots, 0) = f_n \neq 0$. We shall describe now an algorithm which establishes n linear forms such that

$$(14) \qquad F(x_1, \dots, x_k) = f_n \prod_{j=1}^{n} (x_1 + \alpha_{2,j} x_2 + \dots + \alpha_{k,j} x_k),$$

if such a factorization exists.

If F satisfies (14) then $\alpha_{t,i}$ $(t = 2, \dots, k;\ i = 1, \dots, n)$ are the roots of $F(x, \underline{e}_{t-1})$. Unfortunately, establishing the α's we do not know yet which are the corresponding coefficients of the linear factors. We find them by using the roots of auxiliary polynomials.

Input. A homogenous form $F(x_1,\dots,x_k)\in \mathbf{Z}[x_1,\dots,x_k]$ of degree n with $F(1,0,\dots,0)=f_n\neq 0$, and $L_3,\dots,L_k$ defined in Lemma 1.

Output. The factorization (14) of F.

Step 1. (Initialization) $\epsilon \leftarrow 3(4|F|)^{-n(n-1)}$, $t\leftarrow 2$. Compute approximations $\bar\alpha_{2,j}\in \mathbf{Q}(i)$ to the roots of $F(x,\underline{e}_1)$ satisfying (10). Take $\bar\beta_{2,j}\leftarrow \bar\alpha_{2,j}$ $j=1,\dots,n$; goto Step 3.

Step 2. Compute approximations $\bar\alpha_{t,j},\bar\beta_{t,j}\in\mathbf{Q}(i)$ $j,h=1,\dots,n$ to the roots of $F(x,\underline{e}_{t-1})$ and $F(x,1,L_3,\dots,L_t,0,\dots,0)$ satisfying (10) and (11) respectively.

```
for s ← 1 to n do begin
    for j ← s to n do begin
      for h ← s to n do begin
         If |β̄_{t−1,s} − β̄_{t,j} + L_t ᾱ_{t,h}| < ε then goto (i)
      end {h loop terminates}
      If j = n then goto Step 4
    end {j loop terminates}
    Exchange β̄_{t,j} with β̄_{t,s} and ᾱ_{t,h} with ᾱ_{t,s}     (i)
end    {s loop terminates}
```

Step 3. If $t=k$ then output: the factorization of F; stop
else $t\leftarrow t+1$; goto Step 2

Step 4. Output: F is not decomposable; stop.

Theorem 2. *Let $F(x_1,\dots,x_k)$ be a decomposable form of degree n with $F(1,0,\dots,0)\neq 0$. Then the above algorithm gives the factorization of F.*

PROOF. First let F be a decomposable form. We show that the indices can be chosen so that

$$\beta_{t,s}=\alpha_{2,s}+L_3\alpha_{3,s}+\cdots+L_t\alpha_{t,s}\tag{15}$$

holds for $s=1,\dots,n$. This is true for $t=2$. Asssume that it holds for t. Let $1\le s\le n$ and assume that (15) with $t+1$ instead of t is proved already for all $u<s$, i.e

$$\beta_{t+1,u}=\alpha_{2,u}+L_3\alpha_{3,u}+\cdots+L_{t+1}\alpha_{t+1,u}=\beta_{t,u}+L_{t+1}\alpha_{t+1,u}\,.$$

If F is decomposable, then there exist $j,h\ge s$ such that

$$\beta_{t,s}+L_{t+1}\alpha_{t+1,h}=\beta_{t+1,j}\tag{16}$$

holds. By Lemma 2 this is true iff

$$|\bar\beta_{t,s}+L_{t+1}\bar\alpha_{t+1,h}-\bar\beta_{t+1,j}|<\epsilon\,.\tag{17}$$

Therefore, if (17) fails in Step 2 for all $j,h\ge s$ then F is not decomposable.

If we have found $j, h \geq s$ with (17), then (16) holds by Lemma 2. There exist $1 \leq j_1, j_2 \leq n$ with $\beta_{t+1,j} = \beta_{t,j_1} + L_{t+1}\alpha_{t+1,j_2}$ because F is decomposable. Using (16) we get

$$\beta_{t,s} - \beta_{t,j_1} = L_{t+1}(\alpha_{t+1,j_2} - \alpha_{t+1,h}).$$

By Lemma 1 this is possible only if $\alpha_{t+1,j_2} = \alpha_{t+1,h}$ and so $\beta_{t,j_1} = \beta_{t,s}$. Hence exchanging $\beta_{t+1,j}$ and $\beta_{t+1,s}$ as well as $\alpha_{t+1,h}$ and $\alpha_{t+1,s}$ we get (15) for s and finally for $t+1$, too. Hence we proved that if F is decomposable then the Algorithm gives its factorization, otherwise it decides that F is not decomposable.

Remark. It is clear from the proof of Theorem 2 that instead of the L's we can take any other integers for which (8) holds.

5. Complexity analysis

Theorem 3. *Let $F(x_1, \dots, x_k) \in \mathbb{Q}[x_1, \dots, x_k]$ be a homogenous form of degree n with $F(1, 0, \dots, 0) \neq 0$. Then the Algorithm stops in at most $O(k^2 n^6 \log^2(2kn|F|) \log\log(2kn|F|))$ additions, subtractions, multiplications and divisions on rational numbers.*

Proof. To compute approximations to the roots of the polynomials $F(x, \underline{e}_{t-1})$ satisfying (10) for fixed $2 \leq t \leq k$ one needs at most $O(kn^3 \log^2 (2kn|F|) \log\log(2kn|F|))$ arithmetical operations using the algorithm of Schönhage [11]. Hence we get all the $\bar{\alpha}_{t,j}$ $t = 2, \dots, k$; $j = 1, \dots, n$ in at most $O(k^2 n^3 \log^2(2kn|F|) \log\log(2kn|F|))$ operations.

A simple calculation gives the upper bound $(4|F|)^{tn^3}$ for the height of the polynomial $F(x, 1, L_3, \dots, L_t, 0, \dots, 0)$, $t = 3, \dots, k$. Using the above mentioned algorithm of Schönhage, approximations to the roots of these polynomials satisfying (11) can be computed in at most $O(tn^6 \log^2(4|F|) \log\log(4|F|))$ operations.

For a fixed $3 \leq t \leq k$ to find the corresponding subscripts j, h, s with (17) one needs at most $O(n^3)$ operations. Combining these estimates we get the statement of Theorem 3.

References

[1] Z. I. Borevich and I. R. Shafarevich, Number Theory, Pure and Appl. Math. Ser., vol. 20, *Academic Press*, 1966.

[2] J. H. Evertse and K. Győry, Finiteness criteria for decomposable form equations, *Acta Arith.* **50** (1988), 357–379.

[3] K. Győry, On the representation of integers by decomposable forms in several variables, *Publ. Math. Debrecen* **28** (1981), 89–98.

[4] K. GYŐRY, On norm form, discriminant form and index form equations, Coll. Math. Soc. J. Bolyai 34. Topics in Classical Number Theory, *Budapest*, 1981, *North-Holland Publ. Comp. 1984*, pp. 617–676.

[5] H–P. van der HULST and A. K. LENSTRA, Factorization of polynomials by transcendental evaluation, *EUROCAL '85*, Lecture Notes in Comp. Science, vol. **204**, *Springer–Verlag*, 1985, pp. 138–145.

[6] M. POHST and H. ZASSENHAUS, Algorithmic Algebraic Number Theory, *Cambridge Univ. Press*, 1989.

[7] W. M. SCHMIDT, Norm form equations, *Annals of Math.* **96** (1972), 526–551.

[8] W. M. SCHMIDT, Inequalities for resultants and for decomposable forms, Proc. Conf. Diophantine Approximation and its Applications, *Washington* 1972. *New York* and *London*, 1973, pp. 235–253.

[9] W. M. SCHMIDT, Diophantine Approximation, Lecture Notes in Math. vol. 785, *Springer Verlag*, 1980.

[10] TH. SCHNEIDER, Einführung in die transzendenten Zahlen, *Springer Verlag*, 1957.

[11] A. SCHÖNHAGE, The fundamental theorem of algebra in terms of computational complexity, Preliminary report, *Math. Inst. Univ. Tübingen*, 1982.

[12] C. L. SIEGEL, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss.* **1** (1929), 1–70.

ATTILA PETHŐ
MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
4010 DEBRECEN P.O. BOX 12
HUNGARY

(Received April 5, 1990)