ACTA ARITHMETICA
101.2 (2002)

On the number of solutions of decomposable polynomial equations

by

A. Bérczes and K. Győry (Debrecen)

1. Introduction. Let $F(\mathbf{X}) = F(X_1, \dots, X_m) \in \mathbb{Q}[X_1, \dots, X_m]$ be a *decomposable polynomial* of degree $n \geq 3$ in $m \geq 2$ variables, that is, a polynomial which can be written in the form

$$F(\mathbf{X}) = \prod_{i=1}^{n} l_i(\mathbf{X}),$$

where $l_1(\mathbf{X}), \dots, l_n(\mathbf{X})$ are linear polynomials with coefficients in an algebraic number field G. This factorization is unique up to proportional factors from G^*. Let $S = \{p_1, \dots, p_s\}$ be a finite set of $s \geq 0$ rational primes, and denote by $\mathbb{Z}_S$ the ring of S-integers in $\mathbb{Q}$. Consider the equation

$$F(\mathbf{x}) = b \quad \text{in } \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m, \tag{1}$$

where b is a given non-zero S-integer. We assume throughout the paper that F has coefficients in $\mathbb{Z}_S$. Then (1) is called a *decomposable polynomial equation* over $\mathbb{Z}_S$. If in particular F is a form, (1) is a decomposable form equation.

We recall (cf. [7]) that if $\mathcal{F}$ is a finite set of linear forms in $G[X_1, \dots, X_k]$, $k \geq 2$, then a non-zero $\mathbb{Q}$-linear subspace V of the vector space $\mathbb{Q}^k$ is called *$\mathcal{F}$-non-degenerate* if $\mathcal{F}$ contains a subset of at least three linear forms whose restrictions to V are linearly dependent, but pairwise linearly independent.

2000 *Mathematics Subject Classification*: 11D57, 11D72.

Key words and phrases: diophantine equations, decomposable polynomial equations, number of solutions.

Research of the first author was supported in part by the Netherlands Organization for Scientific Research (NWO), the Hungarian Academy of Sciences, the Soros Foundation, the Universitas Foundation, Grants 014245 and 034981 from the Hungarian National Foundation for Scientific Research and the FKFP Grant 3272-13/066/2001.

Research of the second author was supported in part by the Netherlands Organization for Scientific Research (NWO), the Hungarian Academy of Sciences, and by Grants 29330 and 25157 from the Hungarian National Foundation for Scientific Research.

Otherwise V is called $\mathcal{F}$-*degenerate*. Further, V is called $\mathcal{F}$-*admissible* if no form in $\mathcal{F}$ vanishes identically on V.

Denote by $\mathcal{L}$ a maximal subset of pairwise linearly independent polynomials among the linear factors $l_1, \dots, l_n$ of F over G. Put

$$\mathcal{L}^* = \{X_{m+1}\} \cup \left\{ X_{m+1} \cdot l\left(\frac{X_1}{X_{m+1}}, \dots, \frac{X_m}{X_{m+1}}\right) : l \in \mathcal{L} \right\}.$$

Then $\mathcal{L}^*$ consists of linear forms in $X_1, \dots, X_{m+1}$ with coefficients in G.

It was shown in [5], Theorem 1, that (1) has only finitely many solutions for every S and b if and only if the following condition holds: (i) the linear forms in $\mathcal{L}^*$ have rank $m+1$ over G, and every $\mathcal{L}^*$-admissible linear subspace of $\mathbb{Q}^{m+1}$ of dimension ≥ 3 is $\mathcal{L}^*$-non-degenerate. Further, under the assumption (i), a non-explicit bound was derived (cf. [5], Theorem 2) for the number of solutions of (1) which does not depend on the coefficients of F. This bound was given explicitly in terms of the numbers of solutions of some unit equations. However, when the paper [5] was written, no explicit upper bound was available on the number of solutions of those equations. On combining the bound of [5] with an explicit upper bound of Evertse [3] on the number of solutions of unit equations, one can easily show that under the assumption (i), our equation (1) has at most

$$n(2^{18}m)^{g(m+2)^4(s+\omega_S(b)+1)/2} \tag{2}$$

solutions. Here $\omega_S(b)$ denotes the number of those distinct primes p, not contained in S, for which $p \mid b$ in $\mathbb{Z}_S$, and g denotes the degree of the field G over $\mathbb{Q}$. If G is chosen to be the splitting field of F over $\mathbb{Q}$ then $g \leq n!$, and this bound for g cannot be diminished in general.

In our paper we give a much better explicit upper bound for the number of solutions of (1) which is already polynomial in n. Further, we extend our result to the more general equation

$$F(\mathbf{x}) \in b\mathbb{Z}_S^* \quad \text{in } \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m, \tag{3}$$

where $\mathbb{Z}_S^*$ denotes the group of S-units in $\mathbb{Z}_S$. We point out that under the assumption (i) this equation may have infinitely many solutions. Then we show that (i) together with the condition: (i′) for at least one polynomial $l^* \in \mathcal{L}^*$ we have $l^*(\mathbf{a}) \neq 0$ for any $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$, already imply the finiteness of the number of solutions. Further, under these assumptions we derive explicit upper bounds for the number of solutions of (3). Moreover, for $b = 1$, we give a similar upper bound, provided only that the number of solutions of (3) is finite.

The significant improvement in our bounds is due to a new approach which is different from that of [5]. As a generalization of Schmidt's famous results [15] on norm form equations, Győry [10] proved that for homogeneous F, the set of solutions of both (1) and (3) is the union of finitely many so-

called families of solutions. Further, he gave an explicit upper bound for the number of these families. This bound was later improved by Evertse and Győry [8]. In the proofs of our main results we first reduce equations (1) and (3) to homogeneous decomposable polynomial equations in $m+1$ unknowns. Then we apply the above-mentioned results of [10] and [8] to derive bounds for the numbers of solutions of (1) and (3).

We give several consequences for inhomogeneous Thue equations, discriminant polynomial equations, norm polynomial equations and resultant polynomial equations. In particular, our results are also valid in the homogeneous case. However, in this case slightly better estimates are known in the literature (cf. [3], [4], [8], [12], [13]), hence we shall not deal here with applications of our results to decomposable form equations.

2. Main results. To state our results we need some further notation. For a prime p not contained in S, denote by $\mathrm{ord}_p(b)$ the greatest integer a such that $p^a \mid b$ in $\mathbb{Z}_S$. Put

$$\psi_S(b,n,m) = \binom{n+1}{m}^{\omega_S(b)} \prod_{\substack{p \text{ prime} \\ p \notin S}} \binom{\mathrm{ord}_p(b)+m}{m}$$

where the product is taken over all primes p not contained in S, and let

$$\delta(m) = \tfrac{2}{3}(m+1)(m+2)(2m+3) - 4.$$

We note that $\delta(m) \le 2(m+1)^3$. We also use the notation introduced in Section 1.

THEOREM 1. *Suppose that*

(i) *the linear forms in $\mathcal{L}^*$ have rank $m+1$ over G, and every $\mathcal{L}^*$-admissible linear subspace of $\mathbb{Q}^{m+1}$ of dimension ≥ 3 is $\mathcal{L}^*$-non-degenerate.*

Then the number of solutions of equation (1) *does not exceed the bounds*

$$n(2^{17}n)^{\delta(m)(s+1)} \cdot \psi_S(b,n,m) \tag{4}$$

and

$$n(2^{17}n)^{\delta(m)(s+\omega_S(b)+1)}. \tag{5}$$

As is easily seen, the bound (5) is in general much better than (2). In the special case when F in (1) is homogeneous, the assumption (i) is equivalent (cf. [5], Corollary 1) to the fact that every $\mathcal{L}$-admissible linear subspace of $\mathbb{Q}^m$ of dimension ≥ 2 is $\mathcal{L}$-non-degenerate. In this case slightly better bounds are given in [3] and [8] for the number of solutions of (1).

Our example given below shows that in contrast with the case of decomposable form equations, Theorem 1 cannot be generalized to decomposable polynomial equations of the form (3). However, if we replace condition (i)

of Theorem 1 with a stronger assumption, we are able to derive a finiteness theorem and explicit bounds for the number of solutions of (3).

THEOREM 2. *Suppose that the condition* (i) *holds, and that*

(i′) *for at least one polynomial* $l^* \in \mathcal{L}^*$ *we have* $l^*(\mathbf{a}) \neq 0$ *for any* $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$.

Then the number of solutions of equation (3) *does not exceed the bound*

$$(2^{17}n)^{\delta(m)(s+\omega_S(b)+1)}. \tag{6}$$

As a consequence of Theorem 2 we now give another finiteness condition for the number of solutions of (3) which is sometimes easier to check. Let $\mathcal{L}_0^* = \mathcal{L}^* \setminus \{X_{m+1}\}$.

COROLLARY 1. *Suppose that*

(ii′) $\mathcal{L}_0^*$ *has rank* $m+1$ *over* G, *and* $l^*(\mathbf{a}) \neq 0$ *for each* $l^* \in \mathcal{L}_0^*$ *and for any* $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$.

Then the number of solutions of (3) *does not exceed the bound* (6).

We note that in the inhomogeneous case our Theorem 2 and Corollary 1 provide bounds also for the number of solutions of the corresponding Mahler type equation.

The following example shows that condition (i′) in Theorem 2 is also necessary.

EXAMPLE. Put $S = \{5, 13\}$ and consider the polynomial $F(X_1, X_2) = (4X_1 + 6X_2 - 5)(X_2 + 4)(X_2 + 12) \in \mathbb{Z}_S[X_1, X_2]$. This polynomial satisfies the condition (i) of Theorem 1, but there is no linear factor l of F for which the corresponding linear form $l^*(X_1, X_2, X_3)$ has the property that $l^*(x_1, x_2, x_3) \neq 0$ for $(0, 0, 0) \neq (x_1, x_2, x_3) \in \mathbb{Q}^3$. It is easy to see that the equation

$$F(x_1, x_2) \in \mathbb{Z}_S^* \quad \text{in } x_1, x_2 \in \mathbb{Z}_S$$

has infinitely many solutions of the form $(x_1, 1)$.

THEOREM 3. *Assume that* $\operatorname{rank}(\mathcal{L}^*) = m+1$ *and* $b = 1$. *If the number of solutions of* (3) *is finite, then this number does not exceed the bound*

$$(2^{17}n)^{\delta(m)(s+1)}. \tag{7}$$

In the next section we formulate some consequences and applications of our Theorems 1 to 3. Following our proofs, our results could be extended to the case when the ground ring is a ring of S-integers of an arbitrary number field. We shall not work this out here.

3. Some consequences and applications. First let $F_0(\mathbf{X}) = F_0(X_1, \dots, X_m) \in \mathbb{Z}_S[X_1, \dots, X_m]$ be a *decomposable form* in $m \geq 2$ variables and assume that

$$F_0(\mathbf{X}) = \prod_{i=1}^{n} h_i(\mathbf{X})$$

with linear forms $h_i(\mathbf{X}) \in G[X_1, \dots, X_m]$ for $i = 1, \dots, n$. Let $\mathcal{L}_0$ denote a maximal subset of pairwise non-proportional linear forms in $\{h_1, \dots, h_n\}$ over G. Let Λ be the set of all n-tuples $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_n) \in G^n$ for which the decomposable polynomial

$$F_{\boldsymbol{\lambda}}(\mathbf{X}) = \prod_{i=1}^{n} (h_i(\mathbf{X}) + \lambda_i)$$

has coefficients in $\mathbb{Z}_S$. Clearly, $F_{\mathbf{0}}(\mathbf{X}) = F_0(\mathbf{X})$, hence $\mathbf{0} \in \Lambda$. Our Theorem 1 implies the following.

COROLLARY 2. *Suppose that*

(ii) *every subspace of $\mathbb{Q}^m$ of dimension ≥ 2 is $\mathcal{L}_0$-non-degenerate.*

Then for any $b \in \mathbb{Z}_S \setminus \{0\}$ and for every fixed $\boldsymbol{\lambda} \in \Lambda$, the number of solutions of the equation

$$F_{\boldsymbol{\lambda}}(\mathbf{x}) = b \quad \text{in } \mathbf{x} \in \mathbb{Z}_S^m \tag{8}$$

does not exceed the bounds occurring in (4) *and* (5).

In what follows, we apply Corollary 2 to inhomogeneous Thue equations, discriminant polynomial equations and norm polynomial equations. In the case of equations considered over $\mathbb{Z}_S$, our Corollary 2 and Corollaries 3, 5 and 7 below give improved, explicit versions of Corollaries 2 to 5 of [5] where non-explicit bounds were given for the numbers of solutions of the corresponding equations.

Let $F(X_1, X_2) \in \mathbb{Z}_S[X_1, X_2]$ be a decomposable polynomial of degree n. Assume that

$$F(X_1, X_2) = \prod_{i=1}^{n} (h_i(X_1, X_2) + \lambda_i) \tag{9}$$

where $h_i(X_1, X_2)$ is a linear form with coefficients in G and $\lambda_i \in G$ for $i = 1, \dots, n$. Let b be a non-zero S-integer.

COROLLARY 3. *Suppose that*

(iii) *there are at least three pairwise linearly independent forms among $h_1(X_1, X_2), \dots, h_n(X_1, X_2)$.*

Then the number of solutions of the inhomogeneous Thue equation

$$F(x_1, x_2) = b \quad \text{in } x_1, x_2 \in \mathbb{Z}_S \tag{10}$$

does not exceed the bounds

$$n(2^{17}n)^{52(s+1)} \cdot \psi_S(b,n,2) \quad \text{and} \quad n(2^{17}n)^{52(s+\omega_S(b)+1)}.$$

From Theorem 2 we shall deduce the following.

COROLLARY 4. *Suppose that*

(iii′) *there are at least three linearly independent polynomials among* $h_1(X_1,X_2)+\lambda_1,\dots,h_n(X_1,X_2)+\lambda_n$, *and for some* i, $h_i(x_1,x_2) \notin \{0,-\lambda_i\}$ *for any* $(0,0) \neq (x_1,x_2) \in \mathbb{Q}^2$.

Then the number of solutions of the equation

$$F(x_1,x_2) \in b\mathbb{Z}_S^* \quad \text{in } x_1,x_2 \in \mathbb{Z}_S \tag{11}$$

does not exceed the bound

$$(2^{17}n)^{52(s+\omega_S(b)+1)}.$$

The bounds in Corollaries 3 and 4 are also valid in the case of Thue and Thue–Mahler equations, when $\lambda_i = 0$ for $i = 1,\dots,n$. However, when in (10) $F(X_1,X_2)$ is an irreducible binary form, Evertse [4] obtained a much better bound for the numbers of solutions of (10) and (11).

Let M be a number field of degree $n \geq 3$, $\alpha_0 = 1, \alpha_1, \dots, \alpha_m$ linearly independent elements of M over $\mathbb{Q}$ such that $M = \mathbb{Q}(\alpha_1,\dots,\alpha_m)$, and λ an arbitrary element of M. Let $\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_n$ be the $\mathbb{Q}$-isomorphisms of M into $\mathbb{C}$. For any $\alpha \in M$, let $\alpha^{(i)} = \sigma_i(\alpha)$. Put

$$L^{(i)}(\mathbf{X}) := X_0 + \alpha_1^{(i)}X_1 + \ldots + \alpha_m^{(i)}X_m + \lambda^{(i)}$$

with the convention that $L(\mathbf{X}) = L^{(1)}(\mathbf{X})$. Then the decomposable polynomial

$$D_{M/\mathbb{Q}}(L(\mathbf{X})) := \prod_{1 \leq i < j \leq n} (L^{(i)}(\mathbf{X}) - L^{(j)}(\mathbf{X}))^2$$

is called a *discriminant polynomial*. We consider the *discriminant polynomial equation*

$$a_0 D_{M/\mathbb{Q}}(\alpha_1 x_1 + \ldots + \alpha_m x_m + \lambda) = b \quad \text{in } x_1,\dots,x_m \in \mathbb{Z}_S, \tag{12}$$

where $a_0 \in \mathbb{Q}^*$, $b \in \mathbb{Z}_S \setminus \{0\}$. Further, suppose that a_0 is chosen such that the discriminant polynomial $a_0 D_{M/\mathbb{Q}}(\alpha_1 X_1 + \ldots + \alpha_m X_m + \lambda)$ has coefficients in $\mathbb{Z}_S$.

COROLLARY 5. *Under the above conditions, the number of solutions of equation* (12) *does not exceed the bounds* (4) *and* (5) *with* n *replaced by* $n(n-1)$.

In the important special case $\lambda = 0$, somewhat better bounds follow for the number of solutions of (12) from the results of [3] and [8] concerning decomposable form equations. Under some conditions on the normal closure of $M/\mathbb{Q}$, even better bounds can be found in [6], [1] and [14] for $\lambda = 0$.

With the above assumptions, consider the following generalization of equation (12):

$$a_0 D_{M/\mathbb{Q}}(\alpha_1 x_1 + \ldots + \alpha_m x_m + \lambda) \in b\mathbb{Z}_S^* \quad \text{in } x_1, \ldots, x_m \in \mathbb{Z}_S. \tag{13}$$

From Corollary 1 we shall deduce

COROLLARY 6. *Suppose that the number field M has no proper subfield, and that $1, \alpha_1, \ldots, \alpha_m, \lambda$ are linearly independent over $\mathbb{Q}$. Then the number of solutions of equation* (13) *does not exceed the bound* (6) *with n replaced by $n(n-1)$.*

In the case $\lambda = 0$, the results of [3] and [8] concerning decomposable form equations provide somewhat better bounds for the number of solutions of (13).

Let again M be a number field of degree $n \geq 3$, $\alpha_1 = 1, \alpha_2, \ldots, \alpha_m$ linearly independent elements of M over $\mathbb{Q}$ such that $M = \mathbb{Q}(\alpha_2, \ldots, \alpha_m)$, and $\lambda \in M$. As above, put

$$L^{(i)}(\mathbf{X}) := \alpha_1^{(i)} X_1 + \ldots + \alpha_m^{(i)} X_m + \lambda^{(i)}.$$

Then the polynomial

$$N_{M/\mathbb{Q}}(\alpha_1 X_1 + \ldots + \alpha_m X_m + \lambda) = \prod_{i=1}^{n} L^{(i)}(\mathbf{X})$$

is called a *norm polynomial*. Consider the *norm polynomial equation*

$$a_0 N_{M/\mathbb{Q}}(\alpha_1 x_1 + \ldots + \alpha_m x_m + \lambda) = b \quad \text{in } x_1, \ldots, x_m \in \mathbb{Z}_S, \tag{14}$$

where $b \in \mathbb{Z}_S \setminus \{0\}$, and $a_0 \in \mathbb{Q}^*$ is chosen so that the norm polynomial $a_0 N_{M/\mathbb{Q}}(\alpha_1 X_1 + \ldots + \alpha_m X_m + \lambda)$ has coefficients in $\mathbb{Z}_S$.

Denote by $\mathcal{M}$ the $\mathbb{Z}$-module generated by $\alpha_1, \ldots, \alpha_m$ in M. Then $\mathcal{M}$ is called *non-degenerate* if the $\mathbb{Q}$-vector space generated by $\mathcal{M}$ does not contain any subspace of the form $\mu M'$ where $\mu \in M^*$ and M' is a subfield of M such that $\mathbb{Q} \subsetneq M' \subseteq M$. Otherwise $\mathcal{M}$ is called *degenerate*.

COROLLARY 7. *Suppose that*

(iv) *$\mathcal{M}$ is non-degenerate.*

Then the number of solutions of equation (14) *does not exceed the bounds occurring in* (4) *and* (5).

We note that for $\lambda = 0$, slightly better bounds are given in [3] and [8] for the number of solutions of (14).

As a generalization of (14), consider now the equation

$$a_0 N_{M/\mathbb{Q}}(\alpha_1 x_1 + \ldots + \alpha_m x_m + \lambda) \in b\mathbb{Z}_S^* \quad \text{in } x_1, \ldots, x_m \in \mathbb{Z}_S. \tag{15}$$

The next corollary is a special case of our Corollary 1. Corollary 8 was proved independently by Evertse, Stewart and Tijdeman (private communication) and by the authors of the present paper.

COROLLARY 8. *Suppose that in* (15) $\alpha_1, \ldots, \alpha_m$ *and* λ *are linearly independent over* $\mathbb{Q}$. *Then the number of solutions of equation* (15) *does not exceed the bound* (6).

The number of solutions of (15) can be finite also in the case when $\alpha_1, \ldots, \alpha_m$ and λ are linearly dependent. The following corollary follows immediately from our Theorem 3.

COROLLARY 9. *Suppose that for* $b = 1$ *equation* (15) *has only finitely many solutions. Then the number of these solutions does not exceed the bound* (7).

Finally, we apply Corollary 2 to resultant equations. Let $P \in \mathbb{Z}_S[X]$ be a polynomial of degree $n \geq 3$ with leading coefficient a_0 and without multiple zeros. Let $\alpha_1, \ldots, \alpha_n$ denote the zeros of P, and put $G = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Fix a positive integer m, and let $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n) \in G^n$ be such that the decomposable polynomial

$$a_0^m \prod_{i=1}^{n} (\alpha_i^m X_0 + \alpha_i^{m-1} X_1 + \ldots + X_m + \lambda_i) \tag{16}$$

has coefficients in $\mathbb{Z}_S$. This is the case e.g. for $\boldsymbol{\lambda} = \mathbf{0}$ when the corresponding decomposable form in (16) is just the resultant $\mathrm{Res}(P, Q)$ of the polynomials $P(X)$ and $Q(X) = X_0 X^m + X_1 X^{m-1} + \ldots + X_m$. Hence in the case $\boldsymbol{\lambda} = \mathbf{0}$ we call (16) a *resultant form*, and in general a *resultant polynomial*. We denote this polynomial by $\mathrm{Res}_{\boldsymbol{\lambda}}(P, Q)$ with the above Q. Consider the *resultant polynomial equation*

$$\mathrm{Res}_{\boldsymbol{\lambda}}(P, Q) = b \quad \text{in } Q \in \mathbb{Z}_S[X], \tag{17}$$

where b is a given non-zero element of $\mathbb{Z}_S$.

It follows from Theorem 5 of [12] that for $\boldsymbol{\lambda} = \mathbf{0}$, $b \in \mathbb{Z}_S^*$ and $m < n/2$, the number of solutions of (17) in $Q \in \mathbb{Z}_S[X]$ with degree m is at most

$$2(2^{34} n^2)^{(m+1)^3 (s+1)}. \tag{18}$$

Further, it was pointed out in [12] that the assumption $m < n/2$ cannot be replaced by $m \leq n/2$ in general.

From our Corollary 2 we shall deduce the following.

COROLLARY 10. *Let* m *be a positive integer with* $m < n/2$, *and suppose that* $P(X)$ *has no non-constant divisor of degree* $< m$ *in* $\mathbb{Q}[X]$. *Then the number of solutions* $Q(X)$ *of* (17) *with degree* m *does not exceed the bounds* (4) *and* (5) *with* m *replaced by* $m + 1$.

For $\boldsymbol{\lambda} = \mathbf{0}$ and $b \in \mathbb{Z}_S^*$, our bound (5) provided by Corollary 10 can be compared with (18). It is likely that Corollary 10 remains valid without the assumption that P has no non-constant factor with rational coefficients and with degree less than m.

We note that similar results can be deduced from Theorem 2 and Corollary 1 for the number of those polynomials $Q \in \mathbb{Z}_S[X]$ for which $\mathrm{Res}_{\boldsymbol{\lambda}}(P, Q) \in b\mathbb{Z}_S^*$.

4. Proofs. To prove our results we shall need some lemmas. First we introduce some further notation.

Let $\widehat{F}(\mathbf{X}) \in \mathbb{Z}_S[X_1, \ldots, X_k]$, $k \geq 2$, be a decomposable form of degree $r \geq 3$, and assume that there are k linearly independent linear forms among the linear factors of $\widehat{F}$ over $\overline{\mathbb{Q}}$. Let b be a non-zero element of $\mathbb{Z}_S$, and consider the decomposable form equation

$$\widehat{F}(\mathbf{x}) \in b\mathbb{Z}_S^* \quad \text{in } \mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{Z}_S^k. \tag{19}$$

We recall that if $\mathbf{x}$ is a solution of (19) then so is $\varepsilon\mathbf{x}$ for each $\varepsilon \in \mathbb{Z}_S^*$. Such a set of solutions is called a $\mathbb{Z}_S^*$-*coset* of solutions of (19). The form $\widehat{F}$ is a product of norm forms. More precisely, it can be written in the form

$$\widehat{F}(\mathbf{X}) = c \prod_{j=1}^{t} N_{M_j/\mathbb{Q}}(l_j(\mathbf{X})),$$

where $c \in \mathbb{Q}^*$, $M_1, \ldots, M_t$ are algebraic number fields, and $l_j(\mathbf{X})$ is a linear form in $\mathbf{X} = (X_1, \ldots, X_k)$ with coefficients in M_j for $j = 1, \ldots, t$ (cf. [2], pp. 77–81). Let

$$A = M_1 \oplus \ldots \oplus M_t$$

denote the direct $\mathbb{Q}$-algebra sum of $M_1, \ldots, M_t$, i.e. the cartesian product $M_1 \times \ldots \times M_t$ endowed with coordinatewise addition and multiplication. Thus A is an algebra over $\mathbb{Q}$ with unit element $1_A = (1, \ldots, 1)$. Denote by A^* the multiplicative group of invertible elements in A, and by $N_{A/\mathbb{Q}}(a)$ the norm of $a = (\alpha_1, \ldots, \alpha_t) \in A$. Then we have

$$N_{A/\mathbb{Q}}(a) = N_{M_1/\mathbb{Q}}(\alpha_1) \ldots N_{M_t/\mathbb{Q}}(\alpha_t).$$

Denote by $\mathcal{M}_S$ the finitely generated $\mathbb{Z}_S$-module

$$\{x = (l_1(\mathbf{x}), \ldots, l_t(\mathbf{x})) : \mathbf{x} \in \mathbb{Z}_S^k\}$$

in the algebra A. Now equation (19) can be written in the form

$$cN_{A/\mathbb{Q}}(x) \in b\mathbb{Z}_S^* \quad \text{in } x \in \mathcal{M}_S. \tag{20}$$

For any algebraic number field M we denote by $\mathcal{O}_{M,S}$ the integral closure of $\mathbb{Z}_S$ in M, and by $\mathcal{O}_{M,S}^*$ the unit group of $\mathcal{O}_{M,S}$. Similarly, for each $\mathbb{Q}$-subalgebra B of A with $1_A \in B$ we denote by $\mathcal{O}_{B,S}$ the integral closure of $\mathbb{Z}_S$ in B, and by $\mathcal{O}_{B,S}^*$ the unit group of $\mathcal{O}_{B,S}$. The dimension of A as a

$\mathbb{Q}$-vector space is r, and the $\mathbb{Q}$-vector space $V := \mathcal{M}_S\mathbb{Q}$ generated by $\mathcal{M}_S$ over $\mathbb{Q}$ has dimension k. Put

$$\widehat{\psi}_S(b) = \binom{r}{k-1}^{\omega_S(b)} \prod_{\substack{p \text{ prime} \\ p \notin S}} \binom{\mathrm{ord}_p(b)+k-1}{k-1}$$

and

$$e(k) = \tfrac{1}{3}k(k+1)(2k+1) - 2.$$

LEMMA 1. *The set of solutions of equation* (20) *is contained in some finite union*

$$x_1\mathcal{O}^*_{B_1,S} \cup \ldots \cup x_w\mathcal{O}^*_{B_w,S} \quad \text{with} \quad w \le (2^{33}r^2)^{e(k)(s+1)}\widehat{\psi}_S(b) \tag{21}$$

such that for $i = 1, \ldots, w$, B_i *is a* $\mathbb{Q}$*-subalgebra of* A *with* $1_A \in B_i$, *and* $x_i \in A^*$ *with* $x_iB_i \subset V$.

Proof. This is a special case of Theorem 1 of [8]. We note that the proof in [8] is based on a combination of some deep results of Győry [10] and Evertse [3]. The proof of the result used from [3] depends on Evertse's improvement (cf. [9]) of Schmidt's quantitative subspace theorem. ∎

Consider the above factorization of $\widehat{F}$ into linear factors, and let $\widehat{\mathcal{L}}$ be a maximal subset of pairwise linearly independent linear factors of $\widehat{F}$. By the assumption made on the linear factors of $\widehat{F}$, $\widehat{\mathcal{L}}$ has rank k over $\overline{\mathbb{Q}}$. Hence the linear mapping

$$\Phi : \mathbb{Q}^k \to V, \qquad \mathbf{x} \mapsto (l_1(\mathbf{x}), \ldots, l_t(\mathbf{x}))$$

gives an isomorphism between $\mathbb{Q}^k$ and V.

LEMMA 2. *Let* H *be a non-zero subspace of the vector space* $\mathbb{Q}^k$. *Then the following statements are equivalent*:

(a) H *is* $\widehat{\mathcal{L}}$*-admissible and* $\widehat{\mathcal{L}}$*-degenerate.*

(b) $\Phi(H) = xB$ *for some* $x \in \Phi(H) \cap A^*$ *and some* $\mathbb{Q}$*-subalgebra* B *of* A *with* $1_A \in B$.

Proof. This is Lemma 8 of [10]. ∎

LEMMA 3. *Suppose that every* $\widehat{\mathcal{L}}$*-admissible linear subspace of* $\mathbb{Q}^k$ *of dimension* ≥ 3 *is* $\widehat{\mathcal{L}}$*-non-degenerate. Then all solutions of* (19) *are contained in a finite union of at most two-dimensional subspaces* $H_1, \ldots, H_w$ *of* $\mathbb{Q}^k$ *such that*

$$w \le (2^{33}r^2)^{e(k)(s+1)}\widehat{\psi}_S(b).$$

Proof. Consider equation (19) in the form (20). By Lemma 1, the set of solutions of equation (20) is contained in some finite union of the form (21) with the properties specified in Lemma 1.

Now fix a coset $x_i\mathcal{O}^*_{B_i,S}$ from (21). We have $x_i\mathcal{O}^*_{B_i,S} \subset x_iB_i$. Since x_iB_i is a $\mathbb{Q}$-linear subspace of V with $1_A \in B_i$, there exists a linear subspace H_i of $\mathbb{Q}^k$ such that $\Phi(H_i) = x_iB_i$ and $x_i \in \Phi(H_i) \cap A^*$. Further, for each solution $\mathbf{x}$ of (20) which is contained in x_iB_i, the corresponding solution $\mathbf{x}$ of (19) is contained in H_i, and vica versa. Moreover, by Lemma 2 we infer that H_i is an $\widehat{\mathcal{L}}$-admissible and $\widehat{\mathcal{L}}$-degenerate subspace of $\mathbb{Q}^k$. However, by assumption, every $\widehat{\mathcal{L}}$-admissible and $\widehat{\mathcal{L}}$-degenerate subspace of $\mathbb{Q}^k$ is of dimension ≤ 2. This completes the proof. ∎

LEMMA 4. *Suppose that equation* (19) *has only finitely many* $\mathbb{Z}^*_S$*-cosets of solutions. Then this number is at most*

$$(2^{33}r^2)^{e(k)(s+1)}\widehat{\psi}_S(b).$$

Proof. This is Corollary 2 in [8]. ∎

To prove Theorems 1 to 3, we first introduce some notation. Consider equations (1) and (3), where

$$F(\mathbf{X}) = F(X_1, \dots, X_m) \in \mathbb{Z}_S[X_1, \dots, X_m]$$

is a decomposable polynomial of degree $n \ge 3$ in $m \ge 2$ variables. Let $l_1, \dots, l_n$ denote the linear factors of F over G. Put

$$F^*(\mathbf{X}^*) = F^*(X_1, \dots, X_m, X_{m+1}) = X_{m+1}^{n+1} \cdot F\left(\frac{X_1}{X_{m+1}}, \dots, \frac{X_m}{X_{m+1}}\right),$$

$$l_i^*(\mathbf{X}^*) = X_{m+1} l_i\left(\frac{X_1}{X_{m+1}}, \dots, \frac{X_m}{X_{m+1}}\right), \quad i = 1, \dots, n,$$

$$l_{n+1}^*(\mathbf{X}^*) = X_{m+1}.$$

Proof of Theorem 1. There is a one-to-one correspondence between the solutions $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m$ of (1) and the corresponding solutions $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ with $x_{m+1} = 1$ of the equation

$$F^*(\mathbf{x}^*) = b \quad \text{in } \mathbf{x}^* \in \mathbb{Z}_S^{m+1}. \tag{22}$$

We give an upper bound for the number of solutions of (22) with $x_{m+1} = 1$. By applying Lemma 3 to this equation we infer that all solutions of (22) are contained in a union $\bigcup_{i=1}^{w} H_i$ of at most two-dimensional subspaces H_i of $\mathbb{Q}^{m+1}$ with

$$w \le (2^{33}(n+1)^2)^{e(m+1)(s+1)}\psi_S(b, n, m). \tag{23}$$

If $\dim_{\mathbb{Q}} H_i = 1$ then (22) can have at most one solution contained in H_i with $x_{m+1} = 1$. Hence it suffices to prove that for each two-dimensional subspace H of $\mathbb{Q}^{m+1}$, there are at most n solutions $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ of (22) in H with $x_{m+1} = 1$. Suppose that (22) has at least two such solutions, say $\mathbf{x}_1^*$ and $\mathbf{x}_2^*$. Then they are $\mathbb{Q}$-linearly independent elements of H. Then for any solution $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ of (22) in H with $x_{m+1} = 1$, we

can write

$$\mathbf{x}^* = \lambda \mathbf{x}_1^* + \mu \mathbf{x}_2^* \tag{24}$$

with suitable rational numbers λ, μ. This implies that

$$l_i^*(\mathbf{x}^*) = \lambda l_i^*(\mathbf{x}_1^*) + \mu l_i^*(\mathbf{x}_2^*), \quad i = 1, \dots, n+1, \tag{25}$$

which gives $\mu = 1 - \lambda$ for $i = n+1$. From (22) we infer that

$$b = F^*(\mathbf{x}^*) = \prod_{i=1}^{n+1} (l_i^*(\mathbf{x}_1^* - \mathbf{x}_2^*)\lambda + l_i^*(\mathbf{x}_2^*)), \tag{26}$$

which is a polynomial of degree at most n in λ. The assumption that $\mathcal{L}^*$ has rank $m+1$ over G implies that this is not a constant polynomial in λ. Hence there are at most n possible values of λ for which (26) and (24) hold. Since $2e(m+1) = \delta(m)$, this proves that the number of solutions of (1) does not exceed the bound occurring in (4).

Next we derive the bound (5). Let $S' = S \cup \{p \mid p \text{ prime with } p \,|\, b \text{ in } \mathbb{Z}_S\}$ and s' the cardinality of S'. Then $s' = s + \omega_S(b)$. Put $F'(\mathbf{X}) = (1/b)F(\mathbf{X})$. Then from $F(\mathbf{X}) \in \mathbb{Z}_S[X_1, \dots, X_m]$, $b \in \mathbb{Z}_{S'}^*$ and $S \subset S'$ we deduce that $F'(\mathbf{X}) \in \mathbb{Z}_{S'}[X_1, \dots, X_m]$. Further, the number of solutions of (1) is not greater than the number of solutions of

$$F'(\mathbf{x}) = 1 \quad \text{in } \mathbf{x} \in \mathbb{Z}_{S'}^m. \tag{27}$$

However, the assumption (i) of Theorem 1 clearly holds also for F'. Hence, by the above, equation (27) cannot have more than

$$n(2^{17}n)^{\delta(m)(s'+1)} \cdot \psi_{S'}(1, n, m)$$

solutions. Since $\psi_{S'}(1, n, m) = 1$ and $s' = s + \omega_S(b)$, the proof is complete. ∎

Proof of Theorem 2. Let $\mathbb{Z}_{S'}$ be as above, and let $\mathbb{Z}_{S'}^*$ denote the unit group of $\mathbb{Z}_{S'}$. For every solution $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m$ of (3), the corresponding vector $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ with $x_{m+1} = 1$ is a solution of the equation

$$F^*(\mathbf{x}^*) \in \mathbb{Z}_{S'}^* \quad \text{in } \mathbf{x}^* \in \mathbb{Z}_{S'}^{m+1}. \tag{28}$$

Further, each $\mathbb{Z}_{S'}^*$-coset of solutions of (28) contains at most one solution of (3). Hence it suffices to derive an upper bound for the number of $\mathbb{Z}_{S'}^*$-cosets of solutions of (28).

We may assume that the number field G is a normal extension of $\mathbb{Q}$. Let $\mathcal{O}_{G,S'}$ denote the integral closure of $\mathbb{Z}_{S'}$ in G. By Lemma 2 of [5] we may assume that the linear factors $l_1, \dots, l_n$ of F are chosen so that

$$l_i^*(\mathbf{x}^*) \in \mathcal{O}_{G,S'}^*, \quad i = 1, \dots, n, \tag{29}$$

for each solution $\mathbf{x}^* \in \mathbb{Z}_{S'}^{m+1}$ of (28). Further, we may also assume that each element σ of $\mathrm{Gal}(G/\mathbb{Q})$ permutes the linear factors $l_1^*, \dots, l_n^*$ of F^*.

We first show that under the assumption of Theorem 2, equation (28) has only finitely many $\mathbb{Z}_{S'}^*$-cosets of solutions. From Lemma 3 we again infer that the solutions of (28) are contained in a finite union of at most two-dimensional subspaces of $\mathbb{Q}^{m+1}$. Each one-dimensional subspace contains at most one $\mathbb{Z}_{S'}^*$-coset of solutions. Hence it remains to show that each fixed subspace H of $\mathbb{Q}^{m+1}$ of dimension 2 contains at most finitely many $\mathbb{Z}_{S'}^*$-cosets of solutions.

The linear factor $l_{n+1}^* = X_{m+1}$ is a divisor of the form $F^*(\mathbf{X}^*)$ over $\mathbb{Z}_{S'}$. Hence (28) implies that each $\mathbb{Z}_{S'}^*$-coset of solutions of (28) contains exactly one $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ with $x_{m+1} = 1$. Such a solution $\mathbf{x}^*$ will be called *normalized*.

Suppose that H contains two distinct $\mathbb{Z}_{S'}^*$-cosets of solutions, say $\mathbf{x}_1^*\mathbb{Z}_{S'}^*$ and $\mathbf{x}_2^*\mathbb{Z}_{S'}^*$, where $\mathbf{x}_1^*$ and $\mathbf{x}_2^*$ are normalized. Then for each $\mathbb{Z}_{S'}^*$-coset of solutions $\mathbf{x}^*\mathbb{Z}_{S'}^* \subset H$ where $\mathbf{x}^*$ is normalized we deduce again (24), (25) and, in place of (26),

$$\prod_{i=1}^{n+1} (l_i^*(\mathbf{x}_1^* - \mathbf{x}_2^*)\lambda + l_i^*(\mathbf{x}_2^*)) = F^*(\mathbf{x}^*) \in \mathbb{Z}_{S'}^*. \tag{30}$$

In (24), $\mathbf{x}^*, \mathbf{x}_1^*$ and $\mathbf{x}_2^*$ are S'-integers and $\mathbf{x}_1^*, \mathbf{x}_2^*$ are fixed. Hence using Cramer's rule one can easily see that there is a finite set S'' of primes with $S'' \supseteq S'$ such that for each $\mathbf{x}^*$ considered above, the corresponding value of λ is contained in $\mathbb{Z}_{S''}$. We show that the polynomial

$$P(\lambda) = \prod_{i=1}^{n+1} (l_i^*(\mathbf{x}_1^* - \mathbf{x}_2^*)\lambda + l_i^*(\mathbf{x}_2^*))$$

in λ has at least two distinct zeros. Then, as is known (see e.g. [16], Ch. 10), equation (30) has finitely many solutions in λ.

Put $\kappa_i = l_i^*(\mathbf{x}_2^*)/l_i^*(\mathbf{x}_1^*)$ for $i = 1, \dots, n$. If $\kappa_i \in \mathbb{Q}$ for some i, then by (29), $\kappa_i \in \mathbb{Q} \cap \mathcal{O}_{G,S'}^* = \mathbb{Z}_{S'}^*$, and so $l_i^*(\mathbf{x}_2^* - \kappa_i \mathbf{x}_1^*) = 0$ where $\mathbf{0} \neq \mathbf{x}_2^* - \kappa_i \mathbf{x}_1^* \in \mathbb{Q}^{m+1}$. However, by our assumption, there is at least one $l^* \in \mathcal{L}^*$ such that $l^*(\mathbf{a}) \neq 0$ for all $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$. Consequently, there exists at least one i such that $\kappa_i \notin \mathbb{Q}$. But $\kappa_i \in G$, hence there is a κ_j which is different from κ_i such that $\kappa_j = \sigma(\kappa_i)$ for some $\sigma \in \mathrm{Gal}(G/\mathbb{Q})$. Then it is easy to check that

$$-l_i^*(\mathbf{x}_2^*)/l_i^*(\mathbf{x}_1^* - \mathbf{x}_2^*) \quad \text{and} \quad -l_j^*(\mathbf{x}_2^*)/l_j^*(\mathbf{x}_1^* - \mathbf{x}_2^*)$$

are distinct zeros of $P(\lambda)$. As mentioned above, this implies that (30) has only finitely many solutions $\lambda \in \mathbb{Z}_{S''}$. Then also (28) has only finitely many $\mathbb{Z}_{S'}^*$-cosets of solutions. We can now apply Lemma 4 to (28) with $r = n+1$, $k = m+1$, $b = 1$, $S = S'$, to infer that the number of $\mathbb{Z}_{S'}^*$-cosets of solutions of (28) does not exceed

$$(2^{33}(n+1)^2)^{e(m+1)(s+\omega_S(b)+1)}.$$

This implies the bound (6) for the number of solutions of (3). ∎

Proof of Corollary 1. In view of Theorem 2 we only have to prove that condition (ii′) implies (i) and (i′). This means that we have to prove that under the assumption of Corollary 1 every $\mathcal{L}^*$-admissible subspace H of $\mathbb{Q}^{m+1}$ of dimension ≥ 3 is $\mathcal{L}^*$-non-degenerate.

Suppose that H is $\mathcal{L}^*$-admissible and $\dim_{\mathbb{Q}} H = t \geq 3$. By our assumption we have $\operatorname{rank}(\mathcal{L}_0^*) = m+1$, and thus we get

$$X_{m+1} = \sum_{i=1}^{n} c_i l_i^*(\mathbf{X}^*) \tag{31}$$

with suitable constants c_i. Since H is $\mathcal{L}^*$-admissible, X_{m+1} does not vanish on H. Thus there exists a basis $\mathbf{a}_1^*, \ldots, \mathbf{a}_t^*$ of H such that the $(m+1)$th coordinate of $\mathbf{a}_1^*$ is 1 and the $(m+1)$th coordinates of $\mathbf{a}_2^*, \ldots, \mathbf{a}_t^*$ are 0. Put

$$\mathbf{X}^* = Y_1 \mathbf{a}_1^* + \ldots + Y_t \mathbf{a}_t^*.$$

Now X_{m+1} takes the form Y_1 on H, and we also have

$$l_i^*(\mathbf{X}^*) = Y_1 l_i^*(\mathbf{a}_1^*) + \ldots + Y_t l_i^*(\mathbf{a}_t^*), \qquad i = 1, \ldots, n,$$

on H. Further, by (ii′) the coefficients of the forms $Y_1 l_i^*(\mathbf{a}_1^*) + \ldots + Y_t l_i^*(\mathbf{a}_t^*)$ are non-zero. Thus among the restrictions of the forms X_{m+1}, $l_1^*(\mathbf{X}^*), \ldots, l_n^*(\mathbf{X}^*)$ to the subspace H there are at least two which are linearly independent. Further, by (31) there are at least three forms among these restrictions which are pairwise linearly independent. However, (31) implies that the restrictions of $X_{m+1}, l_1^*, \ldots, l_n^*$ to H are linearly dependent. Hence H is $\mathcal{L}^*$-non-degenerate and Corollary 1 follows from Theorem 2. ∎

Proof of Theorem 3. Consider equation (3) and the corresponding equation (28) with $b = 1$. Then in (28) we have $S' = S$. Further, for every solution $\mathbf{x} = (x_1, \ldots, x_m)$ of (3), $\mathbf{x}^* = (x_1, \ldots, x_m, x_{m+1})$ with $x_{m+1} = 1$ is a solution of (28). Conversely, in view of $b = 1$ any $\mathbb{Z}_S^*$-coset of solutions of (28) contains exactly one solution $\mathbf{x}^* = (x_1, \ldots, x_m, x_{m+1})$ with $x_{m+1} = 1$ and then $\mathbf{x} = (x_1, \ldots, x_m)$ is clearly a solution of (3). Hence the number of solutions of (3) coincides with the number of $\mathbb{Z}_S^*$-cosets of solutions of (28). By applying now Lemma 4 to equation (28) with $r = n+1$, $k = m+1$, $b = 1$ the assertion immediately follows. ∎

Proof of Corollary 2. It was proved in [5] that under condition (ii) and the other assumptions concerning equation (8), condition (i) of our Theorem 1 holds. Hence Corollary 2 follows at once from Theorem 1. ∎

Proof of Corollary 3. We prove that under condition (iii), equation (10) satisfies condition (ii) of Corollary 2. By (iii) there are at least three pairwise linearly independent linear forms in the set

$$\mathcal{L}_0 = \{h_1(X_1, X_2), \ldots, h_n(X_1, X_2)\}.$$

We may suppose that these forms are $h_i(X_1, X_2) = a_iX_1 + b_iX_2$ for $i = 1, 2, 3$. They are obviously linearly dependent. Hence $\mathbb{Q}^2$ is $\mathcal{L}_0$-non-degenerate, and so Corollary 3 follows at once from Corollary 2. ∎

Proof of Corollary 4. It is easy to check that condition (iii′) of Corollary 4 implies conditions (i) and (i′) of Theorem 2 with $m = 2$. Hence Corollary 4 follows from Theorem 2. ∎

Proof of Corollary 5. We keep the notation of Corollary 5. Using some ideas from the proof of Theorem 2 in [6] we prove that equation (12) satisfies condition (ii) of Corollary 2. Put

$$L_0^{(i)}(\mathbf{X}) := \alpha_1^{(i)}X_1 + \ldots + \alpha_m^{(i)}X_m.$$

Denote by $\mathcal{L}_0$ a maximal subset of pairwise linearly independent forms among $L_0^{(i)} - L_0^{(j)}$, $1 \le i \ne j \le n$. Since $1, \alpha_1, \ldots, \alpha_m$ are linearly independent over $\mathbb{Q}$, it is easy to see that $\mathcal{L}_0$ has rank m. The set $\mathcal{L}_0$ is spanned by the linear forms $L_0^{(1)} - L_0^{(j)}$, $2 \le j \le n$. Then one can easily show that for every subspace V of $\mathbb{Q}^m$ of dimension ≥ 2 there are at least two forms among $L_0^{(1)} - L_0^{(j)}$, $2 \le j \le n$, which are linearly independent on V, say $L_0^{(1)} - L_0^{(2)}$ and $L_0^{(1)} - L_0^{(3)}$. Then clearly $L_0^{(1)} - L_0^{(2)}$, $L_0^{(1)} - L_0^{(3)}$ and $L_0^{(2)} - L_0^{(3)}$ are pairwise linearly independent on V and

$$(L_0^{(1)} - L_0^{(2)}) - (L_0^{(1)} - L_0^{(3)}) + (L_0^{(2)} - L_0^{(3)}) = 0,$$

which implies that condition (ii) of Corollary 2 holds. Now Corollary 5 is a simple consequence of Corollary 2. ∎

Proof of Corollary 6. Keeping the above notation, put

$$l^{*(i)}(\mathbf{X}) := \alpha_1^{(i)}X_1 + \ldots + \alpha_m^{(i)}X_m + \lambda^{(i)}X_{m+1}.$$

Denote by $\mathcal{L}_0^*$ a maximal subset of pairwise linearly independent forms among $l^{*(i)} - l^{*(j)}$, $1 \le i < j \le n$. We can see as above that $\operatorname{rank}(\mathcal{L}_0^*) = m+1$. Further, if $l^{*(i)}(\mathbf{a}) - l^{*(j)}(\mathbf{a}) = 0$ for some distinct i, j and some $\mathbf{0} \ne \mathbf{a} \in \mathbb{Q}^{m+1}$, then $l^{*(i)}(\mathbf{a})$ cannot be a primitive element of M. However, by our assumptions the field M is primitive, hence it follows that $l^{*(i)}(\mathbf{a}) \in \mathbb{Q}$, which contradicts the fact that $1, \alpha_1, \ldots, \alpha_m$ and λ are linearly independent over $\mathbb{Q}$. Thus condition (ii′) of Corollary 1 holds, and Corollary 6 follows from Corollary 1. ∎

Proof of Corollary 7. As shown in [5], under the assumptions of Corollary 7, equation (14) satisfies condition (ii) of Corollary 2. Hence Corollary 7 follows immediately from Corollary 2. ∎

Proof of Corollary 8. It is easy to see that under the assumptions of Corollary 8, equation (15) satisfies the conditions of Corollary 1. Hence the assertion follows. ∎

For any system $\mathcal{F}$ of linear forms with coefficients in a number field G, denote by $\mathcal{V}_G(\mathcal{F})$ the G-vector space generated by the forms in $\mathcal{F}$.

LEMMA 5. *Let $\widehat{F}(X_0, X_1, \ldots, X_k)$ $(k \geq 1)$ be a decomposable form of degree n with coefficients in $\mathbb{Q}$ which factorizes into linear factors over a number field G. Suppose that any $k+1$ linear factors in the factorization of $\widehat{F}$ are linearly independent. Denote by $\widehat{\mathcal{L}}$ a maximal subset of pairwise linearly independent forms among the linear factors of $\widehat{F}$. Then for each proper non-empty subset $\widehat{\mathcal{L}}_1$ of $\widehat{\mathcal{L}}$ we have*

$$(\mathcal{V}_G(\widehat{\mathcal{L}}_1) \cap \mathcal{V}_G(\widehat{\mathcal{L}} \setminus \widehat{\mathcal{L}}_1)) \cap \widehat{\mathcal{L}} \neq \emptyset.$$

Proof. This is proved in the proof of Theorem 3 in [11]. ∎

LEMMA 6. *Under the assumptions of Lemma 5 the following two statements are equivalent*:

(a) *Every $\widehat{\mathcal{L}}$-admissible subspace of G^{k+1} of dimension ≥ 2 is $\widehat{\mathcal{L}}$-non-degenerate.*

(b) *The forms in $\widehat{\mathcal{L}}$ have rank $k+1$ over G and for each proper non-empty subset $\widehat{\mathcal{L}}_1$ of $\widehat{\mathcal{L}}$ we have*

$$(\mathcal{V}_G(\widehat{\mathcal{L}}_1) \cap \mathcal{V}_G(\widehat{\mathcal{L}} \setminus \widehat{\mathcal{L}}_1)) \cap \widehat{\mathcal{L}} \neq \emptyset.$$

Proof. This is the Proposition in [7]. ∎

Proof of Corollary 10. For convenience, we denote by $F_{\boldsymbol{\lambda}}(X_0, \ldots, X_m)$ the resultant polynomial occurring in (16). Then for each solution $Q(X) = x_0X^m + \ldots + x_m$ of (17), $x_0, \ldots, x_m$ is a solution of the equation

$$F_{\boldsymbol{\lambda}}(x_0, \ldots, x_m) = b \quad \text{in } x_0, \ldots, x_m \in \mathbb{Z}_S. \tag{32}$$

Let $\mathcal{L}_0$ denote the set of linear forms

$$h_i(\mathbf{X}) = \alpha_i^m X_0 + \alpha_i^{m-1} X_1 + \ldots + X_m, \quad i = 1, \ldots, n.$$

It is clear that any $m+1$ forms in $\mathcal{L}_0$ are linearly independent over G, the splitting field of $F_{\boldsymbol{\lambda}}$ over $\mathbb{Q}$.

By our assumptions, $P(X)$ has no non-constant factor of degree $< m$ in $\mathbb{Q}[X]$. This implies that for given i with $1 \leq i \leq n$, there are no linearly independent vectors $\mathbf{a}_1, \mathbf{a}_2$ in $\mathbb{Q}^{m+1}$ such that $h_i(\mathbf{a}_1) = h_i(\mathbf{a}_2) = 0$. This means that every linear subspace of $\mathbb{Q}^{m+1}$ of dimension ≥ 2 is $\mathcal{L}_0$-admissible.

We now show that every linear subspace V of $\mathbb{Q}^{m+1}$ of dimension ≥ 2 is $\mathcal{L}_0$-non-degenerate. Our equation (32) satisfies the conditions of Lemma 5. Hence

$$(\mathcal{V}_G(\mathcal{L}_1) \cap \mathcal{V}_G(\mathcal{L}_0 \setminus \mathcal{L}_1)) \cap \mathcal{L}_0 \neq \emptyset$$

for each proper non-empty subset $\mathcal{L}_1$ of $\mathcal{L}_0$. By Lemma 6, this is equivalent to the fact that every $\mathcal{L}_0$-admissible G-linear subspace of G^{m+1} of dimension ≥ 2 is $\mathcal{L}_0$-non-degenerate. However, this implies that every $\mathcal{L}_0$-admissible

linear subspace V of $\mathbb{Q}^{m+1}$ of dimension ≥ 2 is also $\mathcal{L}_0$-non-degenerate. This proves our claim above. Therefore condition (ii) of Corollary 2 holds for equation (32), and Corollary 10 follows from Corollary 2 with the choice $m+1$ in place of m. ∎

References

[1] A. Bérczes, *On the number of solutions of index form equations*, Publ. Math. Debrecen 56 (2000), 251–262.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, 2nd ed., Academic Press, New York, 1967.

[3] J.-H. Evertse, *The number of solutions of decomposable form equations*, Invent. Math. 122 (1995), 559–601.

[4] —, *The number of solutions of the Thue–Mahler equation*, J. Reine Angew. Math. 482 (1997), 121–149.

[5] J.-H. Evertse, I. Gaál and K. Győry, *On the numbers of solutions of decomposable polynomial equations*, Arch. Math. (Basel) 52 (1989), 337–353.

[6] J.-H. Evertse and K. Győry, *On unit equations and decomposable form equations*, J. Reine Angew. Math. 358 (1985), 6–19.

[7] —, —, *Finiteness criteria for decomposable form equations*, Acta Arith. 50 (1988), 357–379.

[8] —, —, *The number of families of solutions of decomposable form equations*, ibid. 80 (1997), 367–394.

[9] J.-H. Evertse and H. P. Schlickewei, *The Absolute Subspace Theorem and linear equations with unknowns from a multiplicative group*, in: Number Theory in Progress, K. Győry, H. Iwaniec and J. Urbanowicz (eds.), de Gruyter, Berlin, 1999, 121–142.

[10] K. Győry, *On the numbers of families of solutions of systems of decomposable form equations*, Publ. Math. Debrecen 42 (1993), 65–101.

[11] —, *Some applications of decomposable form equations to resultant equations*, Colloq. Math. 65 (1993), 267–275.

[12] —, *On the irreducibility of neighbouring polynomials*, Acta Arith. 67 (1994), 283–294.

[13] —, *On the distribution of solutions of decomposable form equations*, in: Number Theory in Progress, K. Győry, H. Iwaniec and J. Urbanowicz (eds.), de Gruyter, Berlin, 1999, 237–265.

[14] —, *Discriminant form and index form equations*, in: Algebraic Number Theory and Diophantine Analysis, de Gruyter, Berlin, 2000, 191–214.

[15] W. M. Schmidt, *Norm form equations*, Ann. of Math. 96 (1972), 525–551.

[16] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, 1986.

Institute of Mathematics and Informatics
University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail: berczesa@math.klte.hu
gyory@math.klte.hu

Received on 29.1.2001 (3960)