Astérisque

KÁLMÁN GYÖRY

Some recent applications of S-unit equations

Astérisque, tome 209 (1992), p. 17-38

<http://www.numdam.org/item?id=AST_1992__209__17_0>

SOME RECENT APPLICATIONS OF S-UNIT EQUATIONS

Kálmán GYŐRY *

§ 1. Introduction

In 1988, we published with Evertse, Stewart and Tijdeman [11] a long survey article on S-unit equations and their applications. Since then much progress has been made in this fertile field. The purpose of this paper is to give a survey of some recent developments. In § 2, known finiteness theorems (cf. Theorems A, B) and some recent quantitative results (cf. Theorems 1, 2 and 3) are presented for S-unit equations. The proofs of Theorems A and 1 to 3 depend on the Thue-Siegel-Roth-Schmidt method and its p-adic generalization. §§ 3 to 6 are devoted to recent applications of the mentioned results. In § 3, finiteness theorems are established for certain arithmetic graphs (cf. Theorem 4) and irreducible polynomials of the form $g(f(X))$ (cf. Theorem 5). These are considerable improvements of earlier theorems obtained in this direction, and furnish definitive results in a sense. The results of Schinzel and the author in § 4 (cf. Theorem 6) resolve a conjecture of Posner and Rumsey [28] on common polynomial divisors of trinomials. § 5 is concerned with generalizations for decomposable form equations (cf. Theorem 7, 8) of finiteness theorems of Schmidt [34], Schlickewei [30] and Laurent [25] on families of solutions of norm form equations. Uniform upper bounds are given for the number of families of solutions. As a consequence, bounds are derived for the number of solutions, provided that this number is finite (cf. Corollary 1).

* Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research.

A further consequence is deduced in § 6 for some generalized systems of S-unit equations (cf. Theorem 9). It provides, over number fields, a quantitative version of a more general result of Laurent [25].

The results treated in §§ 2 to 6 are all ineffective. Baker's effective method and its p-adic analogue made it possible to establish an effective finiteness theorem (cf. Theorem C in § 7) for S-unit equations in two unknowns. As a recent application of Theorem C, in § 8 an effective finiteness theorem (cf. Theorem 10) of Evertse and the author is presented for decomposable forms of given discriminant. It makes effective in a more general form an ineffective theorem of Birch and Merriman [2] on binary forms. Apart from certain particular cases, no effective results are known for S-unit equations in more than two unknowns. In § 7 we state a generalization of Baker's type inequalities (cf. Proposition) whose effective resolution would imply effective versions of all results of this paper.

Theorems A, B and C were already treated in [11], while Theorems 1 to 10 have been obtained since 1988. The complete proofs of Theorems 4 to 8 and 10 will be published in Győry [18, Part II], [14, Part IV], [20], Győry and Schinzel [21] and Evertse and Győry [9], [10].

It is impossible to deal with all recent applications of unit equations within the frame of the present paper. Further applications have recently been obtained for instance to diophantine equations and irreducible polynomials of other type, modular forms, pairs of polynomials and binary forms of given resultant, recurrence sequences, group theory, algebraic number theory and transcendental number theory. Some generalizations and analogues have also been established over finitely generated domains and function fields, respectively.

§ 2. S-unit equations; ineffective results

We introduce some notation which will be used throughout this paper. Let K be an algebraic number field, O_K the ring of integers of K, and O_K^* the unit group[1] of O_K. Further, let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a finite set of prime ideals in O_K, and put

$$O_S = \{\alpha \in K : \ \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \ \text{ for all prime ideals } \mathfrak{p} \text{ of } O_K \text{ with } \mathfrak{p} \notin S\}.$$

Then O_S is a subring of K which is called the ring of S-integers. It contains O_K as a subring. The units of O_S, i.e. the invertible elements are called S-units.

[1] In general, if R is an integral domain then R^* will denote its group of units; thus if R is a field then $R^* = R \setminus \{0\}$.

They form a multiplicative group which is denoted by O_S^*. Put $d = [K : \mathbb{Q}]$ and $s = r + t + 1$ where r denotes the unit rank of O_K^*. Thus $r \leq d - 1$.

Many problems of number theory can be reduced to equations of the form

$$\alpha_1 x_1 + \alpha_2 x_2 = 1 \text{ in } x_1, x_2 \in O_S^* \tag{1}$$

or, more generally,

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 1 \text{ in } x_1, \ldots, x_n \in O_S^* \tag{2}$$

where $\alpha_1, \ldots, \alpha_n$ are elements of K^*. Equation (2) is called an *S-unit equation in n unknowns*. For $n > 2$, it can happen that for a solution $x_1, \ldots, x_n$, the left hand side of (2) has a vanishing subsum. In this case the solution is called *degenerate*, otherwise *non-degenerate*. If (2) has a degenerate solution and if O_S^* is infinite then (2) has infinitely many solutions. Denote by $\mu_n(\alpha_1, \ldots, \alpha_n)$ the number of non-degenerate solutions of (2). Several results have been obtained on $\mu_n(\alpha_1, \ldots, \alpha_n)$; for references see [37] and [11]. Using the Thue-Siegel-Roth-Schmidt method, van der Poorten and Schlickewei [26] (see also [27]) and Evertse [3] proved independently of each other the following

THEOREM A. *For $n \geq 2$ we have $\mu_n(\alpha_1, \ldots, \alpha_n) < \infty$.*

The next quantitative result was established by Evertse [4].

THEOREM B. *We have*

$$\mu_2(\alpha_1, \alpha_2) \leq 3 \times 7^{d+2s}. \tag{3}$$

In 1988, we derived with Evertse [7] an upper bound for $\mu_n(\alpha_1, \ldots, \alpha_n)$ which is independent of $\alpha_1, \ldots, \alpha_n$. Recently this has been made explicit by Schlickewei [31] who proved

THEOREM 1. *For $n \geq 2$, we have*

$$\mu_n(\alpha_1, \ldots, \alpha_n) \leq \exp\{2^{36nd!} \cdot s^6 \log(4sd!)\}. \tag{4}$$

Further, if K is a normal extension of $\mathbb{Q}$ then $d!$ can be replaced by d.

The proof is based on Schlickewei's p-adic generalization [32] of the quantitative Subspace Theorem of Schmidt [35]. Very recently Evertse (private communication) has improved (4) in terms of d to

$$\mu_n(\alpha_1,\dots,\alpha_n) \le \exp\{2^{37nd}\cdot s^6\log(8sd!)\}. \tag{5}$$

The dependence on d is much weaker in (4) and (5) than in (3). Probably s^6 can be improved to s.

We call two n-tuples $(\alpha_1,\dots,\alpha_n)$ and $(\alpha_1',\dots,\alpha_n')$ in $(K^*)^n$ (and the corresponding S-unit equations) *S-equivalent* if $\alpha_i'/\alpha_i \in O_S^*$ for $i=1,\dots,n$. If $(\alpha_1,\dots,\alpha_n)$ and $(\alpha_1',\dots,\alpha_n')$ are S-equivalent then $\mu_n(\alpha_1,\dots,\alpha_n) = \mu_n(\alpha_1',\dots,\alpha_n')$. We showed with Evertse, Stewart and Tijdeman [12] (see also [11]) that $\mu_2(\alpha_1,\alpha_2)\le 2$ for all but finitely many S-equivalence classes of pairs $(\alpha_1,\alpha_2)\in(K^*)^2$. Further, we pointed out that if O_S^* is infinite then there are infinitely many S-equivalence classes of pairs (α_1,α_2) for which (1) has two solutions. The proof of the above estimate depends among other things on the fact that $\mu_n := \mu_n(1,1,\dots,1)$ is finite for all $n\le 5$. Following the proof of [12] it is easy to show that apart from at most $\mu_5+12\mu_3+30\mu_2^2$ S-equivalence classes of pairs (α_1,α_2), we have $\mu_2(\alpha_1,\alpha_2)\le 2$ (see e.g. [19] or [21]). Hence, in view of Theorem 1, the above-mentioned result of [12] can be stated in the following quantitative form.

THEOREM 2. *Apart from at most*

$$\exp\{2^{180d!}\cdot s^6\log(2(4sd!))\}$$

S-equivalence classes of pairs $(\alpha_1,\alpha_2)\in(K^*)^2$, we have $\mu_2(\alpha_1,\alpha_2)\le 2$. Further, if K is a normal extension of $\mathbb{Q}$ then $d!$ can be replaced by d.

It was shown in [12] that for $n>2$, there can exist infinitely many S-equivalence classes of equations (2) with "many" non-degenerate solutions. Hence Theorem 2 cannot be generalized in this sense to solutions of (2). There is, however, another possibility for generalization. Denote by $\nu_n(\alpha_1,\dots,\alpha_n)$ the minimal number of $(n-1)$-dimensional linear subspaces of K^n whose union contains all solutions of (2). Theorem 1 implies an upper bound for $\nu_n(\alpha_1,\dots,\alpha_n)$. In 1988, we proved with Evertse [7] that apart from finitely many S-equivalence classes of equations (2), $\nu_n(\alpha_1,\dots,\alpha_n) < 2^{(n+1)!}$ holds. Recently, Evertse [5] improved this bound to $(n!)^{2n+2}$, and applied his estimate to decomposable form equations.

Following the proof of [7], one can derive $\mu_{(n+1)!-1}^{n-1}$ as an upper bound for the number of exceptional S-equivalence classes in question. Together with Theorem 1 this implies that the result of [7] under consideration can now be enunciated in the following quantitative form.

THEOREM 3. *Apart from at most*

$$\exp\{n2^{36(n+1)!d!} \cdot s^6 \log(4sd!)\}$$

S-equivalence classes of n-tuples $(\alpha_1, \ldots, \alpha_n) \in (K^*)^n$, *we have* $\nu_n(\alpha_1, \ldots, \alpha_n) < 2^{(n+1)!}$. *Further, if* K *is a normal extension of* $\mathbb{Q}$ *then* $d!$ *can be replaced by* d.

For $n = 2$, $\nu_2(\alpha_1, \alpha_2) = \mu_2(\alpha_1, \alpha_2)$ holds. Thus, for $n = 2$, Theorem 3 gives a weaker version of Theorem 2. The proof of Theorem 3 will be published in a joint paper with Tijdeman, together with some generalizations and further related results.

It is likely that combining the proof of [5] with Theorem 1, the bound $2^{(n+1)!}$ in Theorem 3 can be improved to $(n!)^{2n+2}$. However, this bound $(n!)^{2n+2}$ is still probably far from being best possible. Theorem 3 and its possible improvements would have applications, e.g. to decomposable form equations (cf. [5]).

§ 3. Applications to irreducible polynomials and arithmetic graphs

Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be a finite subset of O_K. For given $N \geq 1$, we denote by $\mathcal{G} = \mathcal{G}_K(\mathcal{A}, N)$ the simple graph whose vertex set is $\mathcal{A}$ and whose edges are the unordered pairs $[\alpha_i, \alpha_j]$ such that $\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha_i - \alpha_j)\right| > N$. The ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ and $\mathcal{A}' = \{\alpha_1', \ldots, \alpha_m'\}$ of O_K are called *equivalent* if $\alpha_i' = \varepsilon\alpha_i + \beta$ for some $\varepsilon \in O_K^*$ and $\beta \in O_K$, $i = 1, \ldots, m$. Then the graphs $\mathcal{G}_K(\mathcal{A}, N)$ and $\mathcal{G}_K(\mathcal{A}', N)$ are isomorphic.

Many diophantine problems, for example related to reducibility of polynomials, pairs of polynomials of given resultant, decomposable form equations or algebraic number theory lead to the study of connectedness properties of graphs $\mathcal{G}_K(\mathcal{A}, N)$ (see [17], [11], [18] and the references given there). Let $m \geq 3$. Using Theorem C of the present paper on S-unit equations in two unknowns, we proved in [17] (see also [11]) in a more precise and effective form that for all but at most finitely many equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A}, N)$ has either

(i) a connected component of order at least $m - 1$,

or

(ii) two connected components of order ≥ 2 which are complete.

This result and its various other variants have been used to solve the diophantine problems mentioned.

For certain applications, for instance to irreducible polynomials (see Theorem 5 below) it is crucial to eliminate the possibility (ii) from the above

statement. Recently, we have proved in [18, Part II] (see also [18, Part I]) a more precise and quantitative version of the following theorem.

THEOREM 4. *Let m be a positive integer different from 4. Then for all but at most finitely many equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A}, N)$ has a connected component of order at least $m-1$.*

In the case $m = 4$, we described in [18] the exceptions having property (ii). In the proof, we used the above-mentioned result of Evertse and myself [7] on S-unit equations. Further, to prove the quantitative version, we needed Theorem 1.

For given $m > 4$, we shall now sketch the proof that apart from finitely many equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A}, N)$ cannot have property (ii). In contrast with [18, Part II], here Theorem 2 will be used in a qualitative form. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be an arbitrary ordered subset of O_K for which $\mathcal{G} = \mathcal{G}_K(\mathcal{A}, N)$ has two connected components, say $\mathcal{G}_1$ and $\mathcal{G}_2$, with orders ≥ 2 such that both $\mathcal{G}_1$ and $\mathcal{G}_2$ are complete. We may assume without loss of generality that $\{\alpha_1, \ldots, \alpha_k\}$ and $\{\alpha_{k+1}, \ldots, \alpha_{k+l}\}$ are the vertex sets of $\mathcal{G}_1$ and $\mathcal{G}_2$, respectively. Then we have

$$\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha_i - \alpha_j)\right| \leq N \tag{6}$$

for each i, j with $1 \leq i \leq k$, $k+1 \leq j \leq k+l$. Denote by S the set of all prime ideals in O_K with norm at most N. Then all $\alpha_i - \alpha_j$ satisfying (6) are S-units. For distinct i, i' with $1 \leq i, i' \leq k$, we have

$$\alpha_i - \alpha_{i'} = (\alpha_i - \alpha_j) + (\alpha_j - \alpha_{i'}) \text{ for } j = k+1, \ldots, k+l.$$

Now Theorem 2 implies that apart from an S-unit factor ε, $\alpha_i - \alpha_{i'}$ can assume only finitely many values, say β. But using Theorem B for fixed β, it follows from

$$\beta = (\alpha_i - \alpha_j)/\varepsilon + (\alpha_j - \alpha_{i'})/\varepsilon, \quad j = k+1, \ldots, k+l$$

that $(\alpha_i - \alpha_j)/\varepsilon$ and $(\alpha_j - \alpha_{i'})/\varepsilon$ can assume only finitely many values. Hence the same holds for $(\alpha_p - \alpha_q)/\varepsilon$ for all distinct p, q with $1 \leq p, q \leq m$. Thus $\mathcal{A} = \varepsilon\mathcal{A}' + \alpha_1$ for some ordered subset $\mathcal{A}'$ of O_K whose elements can assume only finitely many values. This proves our claim.

We present now an application of Theorem 4 to irreducible polynomials. I. Schur, A. Brauer, R. Brauer, H. Hopf, I. Seres and others investigated the reducibility of polynomials of the form $f(g(X))$, where f, g are monic polynomials with coefficients in $\mathbb{Z}$, g is irreducible over $\mathbb{Q}$ and the roots of f are

distinct rational integers. For a survey of results obtained in this direction, see [14]. In [14] I extended these investigations to the case when the roots of f are distinct elements of an arbitrary but fixed totally real algebraic number field K of degree d. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be the set of roots of such a monic polynomial $f \in \mathbb{Z}[X]$. Further, suppose that $g \in \mathbb{Z}[X]$ is an irreducible monic polynomial whose splitting field over $\mathbb{Q}$ is a CM-field, i.e. a totally imaginary quadratic extension of a totally real algebraic number field. In this case we say that $g(X)$ is of *CM-type*. If $g(f(X))$ is reducible then so are $g(f(X+a))$ for all $a \in \mathbb{Z}$. Such polynomials $f(X), f(X+a)$ are called *equivalent*. I showed that if the graph $\mathcal{G}_K(\mathcal{A}, N)$ for $N = 2^d|g(0)|^{d/\deg(g)}$ has a connected component with v vertices, then the number of irreducible factors of $g(f(X))$ over $\mathbb{Q}$ is at most $\deg(f)/v$. Further, this estimate is in general best possible (cf. [14, Part II]). Hence it is easy to deduce from Theorem 4 the following

THEOREM 5. *Let $g \in \mathbb{Z}[X]$ be an irreducible monic polynomial of CM-type. There are only finitely many pairwise inequivalent monic polynomials $f \in \mathbb{Z}[X]$ with degree greater than 4 and with distinct roots in K such that $g(f(X))$ is reducible over $\mathbb{Q}$.*

This theorem is in a certain sense a considerable refinement of Theorem 1 of [14, Part III]. We should, however, remark that this theorem of [14] was established in an effective way and over an arbitrary totally real ground field instead of $\mathbb{Q}$.

Recently, we have obtained in [14, Part IV] a more precise version of Theorem 5. There can exist infinitely many pairwise inequivalent exceptions $f(X)$ of degree 4 for which $g(f(X))$ is reducible for a suitable $g(X)$. We give in [14, Part IV] a precise description of these exceptions. Further, we show that Theorem 5 does not remain valid for any irreducible monic polynomial $g \in \mathbb{Z}[X]$ and for any number field K.

§ 4. Applications to common polynomial divisors of trinomials

Using the terminology of [28], for $i \geq 2$ we shall mean by a monic i-nomial over $\mathbb{Q}$ a polynomial of the form $X^{m_1} + a_2X^{m_2} + \cdots + a_{i-1}X^{m_{i-1}} + a_i$ over $\mathbb{Q}$ with $m_1 > m_2 > \cdots > m_{i-1} > 0$. If $p(X)$ and $s(X)$ are polynomials over $\mathbb{Q}$ with $\deg(s) \leq i-1$ such that $p(X) \mid s(X^r)$ over $\mathbb{Q}$ for some integer $r \geq 1$ then $p(X)$ divides infinitely many i-nomials over $\mathbb{Q}$. Indeed, the vector space of polynomials in $\mathbb{Q}[X]$ modulo $s(X)$ is at most $(i-1)$-dimensional, and hence $s(X)$ divides infinitely many i-nomials $T(X)$ over $\mathbb{Q}$. But then $s(X^r) \mid T(X^r)$ and so $p(X) \mid T(X^r)$ over $\mathbb{Q}$. Conversely, Posner and Rumsey [28] made in 1965 the following conjecture: *If a polynomial with rational coefficients divides*

infinitely many monic i-nomials over $\mathbb{Q}$, then it divides a non-zero polynomial in $\mathbb{Q}[X]$ with degree less than i in X^r for some $r \geq 1$.

For $i = 2$ the conjecture is obvious. For $i = 3$, Posner and Rumsey [28] proved a weaker version of their conjecture. Recently, we have proved with Schinzel [21] that the conjecture is true for $i = 3$ and false for every $i \geq 4$. The disproof for the case $i \geq 4$ is elementary. For $i = 3$, we obtained with Schinzel the following stronger assertion.

THEOREM 6. *Let $p \in \mathbb{Q}[X] \setminus \mathbb{Q}$, k the number of distinct roots of $p(X)$, K the splitting field of $p(X)$ over $\mathbb{Q}$, $d = [K : \mathbb{Q}]$, S the set of places of K consisting of all infinite places and all valuations induced by the prime ideal divisors of the non-zero roots of $p(X)$, and $s = \mathrm{Card}(S)$. If $p(X)$ divides more than*

$$\exp\{(s^6 \cdot 2^{180d} + 8sk)\log(4sd)\}$$

monic trinomials over $\mathbb{Q}$, then it divides a linear or quadratic polynomial in X^r over $\mathbb{Q}$ for some integer $r \geq 1$.

The proof depends on Theorems B and 2 on S-unit equations. We sketch the basic idea of the proof. The details will be published in [21].

Let $T(X) = X^m + aX^n + b$ be a trinomial over $\mathbb{Q}$ which is divisible by $p(X)$. If $p(X)$ is divisible by X or if $ab = 0$, the assertion easily follows. Hence it suffices to deal with the case when $X \nmid p(X)$ and $ab \neq 0$. It is easy to show that $p(X)$ can be written in the form $p(X) = p_1(X) \cdot p_2^2(X)$ where p_1, p_2 are relatively prime squarefree polynomials in $\mathbb{Q}[X]$. Denote by $\xi_1, \ldots, \xi_k$ the distinct roots of $p_1(x) \cdot p_2(x)$, and by S the set of all prime ideal divisors of $\xi_1 \cdots \xi_k$ in O_K. Then, for $j = 1, \ldots, k$, (ξ_j^m, ξ_j^n) is a solution of the S-unit equation

$$(-1/b)x_1 + (-a/b)x_2 = 1 \text{ in } x_1, x_2 \in O_S^*. \tag{7}$$

If (7) has at most 2 solutions, then the assertion can be proved by means of some elementary arguments from algebraic number theory. On the other hand, if $p(X)$ divides trinomials $T(X)$ over $\mathbb{Q}$ for which the corresponding equation (7) has more than 2 solutions, then one can use Theorem 2 to derive an upper bound for the number of S-equivalence classes of these equations (7). If now there are sufficiently many trinomials $T(X)$ over $\mathbb{Q}$ for which the corresponding equations (7) are S-equivalent, then one can show by means of Theorem B that there is an integer $r \geq 1$ such that ξ_j^r assumes the same value, say c, for $j = 1, \ldots, k$. Here $c \in \mathbb{Q}^*$ and $p(X) \mid (X^r - c)^2$ over $\mathbb{Q}$, which proves the assertion of Theorem 6.

§ 5. Applications to decomposable form equations

In this section, we present some generalizations to decomposable form equations of well-known finiteness theorems of Schmidt, Schlickewei and Laurent concerning families of solutions of norm form equations.

Let $\mathfrak{M}$ be an O_S-lattice, i.e. a finitely generated O_S-submodule of some K-vector space. Consider a *decomposable form* $F(\mathbf{x})$ on

$$K\mathfrak{M} := \{\lambda \mathbf{x} : \lambda \in K,\ \mathbf{x} \in \mathfrak{M}\}$$

over K, i.e. a function $F\colon K\mathfrak{M} \to K$ for which there are an $\alpha \in K^*$, a finite and normal field extension G/K and K-linear functions $l_1, \ldots, l_f\colon K\mathfrak{M} \to G$ such that $F(\mathbf{x}) = \alpha \prod_{i=1}^{f} l_i(\mathbf{x})$ for all $\mathbf{x} \in K\mathfrak{M}$ (for this general definition, see e.g. [9]). We may assume that G is the splitting field of F, i.e the smallest extension of K over which F factorizes into linear functions. Suppose that $n := \dim_K K\mathfrak{M} \geq 2$ and that $\{l_1, \ldots, l_f\}$ contains n linearly independent functions over G. If in particular $K\mathfrak{M} = K^n$ and $\mathbf{e}_1 = (1, 0, \ldots, 0)^T, \ldots, \mathbf{e}_n = (0, \ldots, 0, 1)^T$ is the standard basis of K^n, we identify $F(\mathbf{x})$ on K^n with the homogeneous polynomial $F(\mathbf{X}) = F(X_1\mathbf{e}_1 + \cdots + X_n\mathbf{e}_n) \in K[X_1, \ldots, X_n]$. This homogeneous polynomial is also called a decomposable form.

Let $\beta \in O_S \setminus \{0\}$ and consider the *decomposable form equation*

$$F(\mathbf{x}) \in \beta O_S^* \ \text{ in } \ \mathbf{x} \in \mathfrak{M}. \tag{8}$$

Put $\mathcal{J} = \{1, \ldots, f\}$. We may assume that $l_i = l_j$ if l_i and l_j are linearly dependent over G and that $\sigma(l_j) = l_{\sigma(j)}$ for all $j \in \mathcal{J}$ and $\sigma \in \mathrm{Gal}(G/K)$, where $(\sigma(1), \ldots, \sigma(f))$ is a permutation of $(1, \ldots, f)$. In the special case when $F(\mathbf{x}) = \alpha \prod_{\sigma \in \mathrm{Gal}(G/K)} \sigma(l_1(\mathbf{x}))$, $F(\mathbf{x})$ is in fact a *norm form* over K, and (8) is a *norm form equation*. Denote by $\mathbf{M}$ the set of tuples $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_f) \in G^f$ for which $\lambda_i = \lambda_j$ if $l_i = l_j$, $i, j \in \mathcal{J}$ and $\sigma(\lambda_i) = \lambda_{\sigma(i)}$ for all $i \in \mathcal{J}$ and $\sigma \in \mathrm{Gal}(G/K)$. Defining the product of $\boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbf{M}$ componentwise, $\mathbf{M}$ becomes a K-subalgebra of G^f with unit element $\mathbf{1} = (1, \ldots, 1)$. We denote by $\mathbf{M}^*$ the multiplicative group of invertible elements of $\mathbf{M}$, and by $N(\boldsymbol{\lambda})$ the product of components of $\boldsymbol{\lambda} \in \mathbf{M}$. This function $N\colon \mathbf{M} \to K$ is clearly multiplicative. The linear mapping $\Psi\colon K\mathfrak{M} \to G^f\colon \mathbf{x} \mapsto (l_1(\mathbf{x}), \ldots, l_f(\mathbf{x}))$ is injective. Further, $\Psi(K\mathfrak{M})$ is contained in $\mathbf{M}$. Put $\mathcal{M} = \Psi(\mathfrak{M})$. Then $\mathcal{M}$ is an O_S-lattice in $\mathbf{M}$ and Ψ induces an isomorphism betweer $\mathfrak{M}$ and $\mathcal{M}$ (as well as between $K\mathfrak{M}$ and $K\mathcal{M}$). We say that $\mathcal{M}$ is *full* (in [illegible] $K\mathcal{M} = \mathbf{M}$. It will be more convenient to consider (8) in the form

$$\alpha \mathrm{N}(\boldsymbol{\mu}) \in \beta O_S^* \ \text{ in } \ \boldsymbol{\mu} \in \mathcal{M}. \tag{9}$$

If in particular $F(\mathbf{x})$ is a norm form then (9) becomes the norm form equation

$$\alpha \mathrm{N}_{M/K}(\boldsymbol{\mu}) \in \beta O_S^* \text{ in } \boldsymbol{\mu} \in \mathcal{M}, \tag{10}$$

where $\mathcal{M}$ denotes now the O_S-module $\{l_1(\mathbf{x}) : \mathbf{x} \in \mathfrak{M}\}$ and M is a suitable subfield of G containing K and $K\mathcal{M}$.

A partition $\mathrm{I} = \{A_1, \dots, A_h\}$ of $\mathcal{J}$ is called symmetric if $i, j \in \mathcal{J}$ belong to the same subset if $l_i = l_j$, and if $\sigma(A_1), \dots, \sigma(A_h)$ is a permutation of $A_1, \dots, A_h$ for every $\sigma \in \mathrm{Gal}(G/K)$. For a symmetric partition $\mathrm{I} = \{A_1, \dots, A_h\}$ of $\mathcal{J}$, we denote by $\mathbf{L} = \mathbf{L}(\mathrm{I})$ the subset of $\mathbf{M}$ consisting of those elements $\boldsymbol{\lambda} = (\lambda_i)_{i \in \mathcal{J}}$ of $\mathbf{M}$ for which $\lambda_i = \lambda_j$ whenever i and j belong to the same subset in the partition I. Then $\mathbf{L}$ is a K-subalgebra of $\mathbf{M}$ with $\mathbf{1}$. If in particular $\mathrm{I} = \{\mathcal{J}\}$ then we write $\mathbf{K}$ for $\mathbf{L}(\mathcal{J})$. Further, $\mathbf{M} = \mathbf{L}(\mathrm{I}_0)$ for the partition I_0 for which $i, j \in \mathcal{J}$ belong to the same subset if and only if $l_i = l_j$. The subrings of $\mathbf{M}$ with $\mathbf{1}$ are precisely the subalgebras $\mathbf{L}(\mathrm{I})$ where I is a symmetric partition of $\mathcal{J}$.

Let $\mathbf{L} = \mathbf{L}(\mathrm{I})$ with a symmetric partition I of $\mathcal{J}$, and denote by $\mathbf{O}_{S,\mathbf{L}}$ the set of those elements $\boldsymbol{\lambda} = (\lambda_i)_{i \in \mathcal{J}}$ of $\mathbf{L}$ for which all components λ_i are integral over O_S. Then $\mathbf{O}_{S,\mathbf{L}}$ is a subring of $\mathbf{L}$ with unit element $\mathbf{1}$. Its unit group is denoted by $\mathbf{O}_{S,\mathbf{L}}^*$. Let $\mathcal{M}^{\mathbf{L}}$ denote the set of all elements $\boldsymbol{\mu} \in \mathcal{M}$ for which $\boldsymbol{\lambda} \cdot \boldsymbol{\mu} \in K\mathcal{M}$ for every $\boldsymbol{\lambda} \in \mathbf{L}$. One can show that in this case $\boldsymbol{\lambda} \cdot \boldsymbol{\mu} \in K\mathcal{M}^{\mathbf{L}}$, that $\mathcal{M}^{\mathbf{L}}$ is an O_S-sublattice of $\mathcal{M}$, that $\mathcal{M}^{\mathbf{K}} = \mathcal{M}$, and that $\mathcal{M}^{\mathbf{M}} = \mathcal{M}$ if $\mathcal{M}$ is full. We say that $\mathbf{L}$ is *admissible* with respect to $\mathcal{M}$ or simply admissible if $\mathcal{M}^{\mathbf{L}} \cap \mathbf{M}^* \neq \varnothing$ and if there is no subalgebra $\mathbf{L}'$ with $\mathbf{1}$ in $\mathbf{M}$ such that $\mathbf{L}' \supsetneq \mathbf{L}$ and $K\mathcal{M}^{\mathbf{L}'} = K\mathcal{M}^{\mathbf{L}}$. We note that if $\mathcal{M}$ is full then $\mathbf{M}$ is admissible. For an admissible subalgebra $\mathbf{L}$ of $\mathbf{M}$, denote by $\mathcal{D}_{\mathcal{M}}^{\mathbf{L}}$ the set of those $\boldsymbol{\lambda} \in \mathbf{L}$ for which $\boldsymbol{\lambda} \cdot \boldsymbol{\mu} \in \mathcal{M}^{\mathbf{L}}$ for all $\boldsymbol{\mu} \in \mathcal{M}^{\mathbf{L}}$. Then $\mathcal{D}_{\mathcal{M}}^{\mathbf{L}}$ is a subring of $\mathbf{O}_{S,\mathbf{L}}$ with $\mathbf{1}$ which contains O_S as a subring (identifying the elements λ of O_S with $\boldsymbol{\lambda} = (\lambda, \dots, \lambda)$). Further, $K\mathcal{D}_{\mathcal{M}}^{\mathbf{L}} = \mathbf{L}$. Denote by $\mathcal{D}_{\mathcal{M}}^{\mathbf{L}\,*}$ the unit group of $\mathcal{D}_{\mathcal{M}}^{\mathbf{L}}$. One can show that $\mathfrak{I}_{\mathbf{L}} := [\mathbf{O}_{S,\mathbf{L}}^* : \mathcal{D}_{\mathcal{M}}^{\mathbf{L}\,*}]$ is finite. If $\boldsymbol{\mu} \in \mathcal{M}^{\mathbf{L}}$ is a solution of (9) then so is every element of $\boldsymbol{\mu}\mathcal{D}_{\mathcal{M}}^{\mathbf{L}\,*}$. Then the set $\boldsymbol{\mu}\mathcal{D}_{\mathcal{M}}^{\mathbf{L}\,*}$ is called a *family of solutions* or more precisely an $(\mathcal{M}, \mathbf{L})$-*family of solutions* of (9). Further, a family of solutions is called *maximal* if it is not properly contained in another family of solutions. Every solution is contained in a maximal family of solutions.

We shall state our results in a quantitative form. Hence we need some further notation. Denote by D the degree of the normal closure of G over $\mathbb{Q}$. Let $m = n$ or $m = n + 1$ according as $\mathfrak{M}$ is free or not. One can show that m is the minimum of the cardinalities of the sets of generators of $\mathfrak{M}$. Assume that F is integral on $\mathfrak{M}$, i.e. that for some set of generators $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$ of $\mathfrak{M}$, the polynomial $F(\sum_{j=1}^m X_j \mathbf{a}_j)$ has their coefficients in O_S. This notion of integrality is independent of the choice of $\mathbf{a}_1, \dots, \mathbf{a}_m$. For $\beta \in O_S \setminus \{0\}$, (β) denotes the O_S-ideal generated by β, $\tau_m(\beta)$ is the number of factorizations

of (β) into m integral ideals in O_S, and $\omega(\beta)$ is the number of distinct prime ideal divisors of (β) in O_S. Further, r denotes the maximal number of pairwise linearly independent linear functions in $\{l_i\}_{i\in\mathcal{J}}$ over G, and u is the maximum of the degrees of the irreducible factors of F over K. Throughout this section, let

$$C = \binom{r}{m-1}^{\omega(\beta)} \tau_m(\beta^u).$$

In the non full case, the proof of the next theorem involves among other things Theorem 1 on S-unit equations.

THEOREM 7. *The set of solutions of* (9) *is the union of at most* $\sum_{\mathbf{L}} \mathfrak{I}_{\mathbf{L}}$ *families of solutions, where the sum is taken over at most*

$$C \cdot \exp\{2^{37nD} \cdot s^6 \log(4sD)\} \tag{11}$$

admissible subalgebras $\mathbf{L}$ *of* $\mathbf{M}$ *(for which* (9) *has an* $(\mathcal{M}, \mathbf{L})$*-family of solutions, and among which there can be identical subalgebras* $\mathbf{L}$*). Further, if* $\mathcal{M}$ *is full in* $\mathbf{M}$ *then* $C \cdot \mathfrak{I}_{\mathbf{M}}$ *is an upper bound for the number of families of solutions in question.*

The following theorem can be deduced from Theorem 7.

THEOREM 8. *Equation* (9) *has at most* $\sum_{\mathbf{L}} \mathfrak{I}_{\mathbf{L}}$ *maximal families of solutions, where the sum is taken over at most*

$$Cn^r \exp\{2^{37nD} \cdot s^6 \log(4sD)\} \tag{12}$$

admissible subalgebras $\mathbf{L}$ *of* $\mathbf{M}$ *(for which* (9) *has a maximal* $(\mathcal{M}, \mathbf{L})$*-family of solutions, and among which there can be identical subalgebras* $\mathbf{L}$*). Further, if* $\mathcal{M}$ *is full in* $\mathbf{M}$ *then* (9) *has at most* $C \cdot \mathfrak{I}_{\mathbf{M}}$ *maximal families of solutions and all these are* $(\mathcal{M}, \mathbf{M})$*-families of solutions.*

We remark that in our bounds, the factor $\mathfrak{I}_{\mathbf{L}}$ cannot be omitted. Further, $D \leq (dr)!$

For norm form equations, i.e. for equation (10), the above finiteness theorems were proved in qualitative forms by Schmidt [34] for $K = \mathbb{Q}, S = \varnothing$, by Schlickewei [30] for $K = \mathbb{Q}$, and by Laurent [25] in general. Some qualitative versions of Theorems 7 and 8 have been established independently by Evertse (private communication). He uses different terminology which is however equivalent to ours.

If $\boldsymbol{\mu}$ is a solution of (9) then so is $\boldsymbol{\mu}\,\varepsilon$ for every $\varepsilon \in O_S^*$. A set of solutions of the form $\boldsymbol{\mu}\, O_S^*$ is called an O_S^**-coset of solutions*. For equation (8), O_S^*-cosets of solutions can be defined in a similar way. From Theorem 7 one can deduce

COROLLARY 1. *Suppose that equation* (9) *(or equivalently equation* (8)*) has only finitely many O_S^*-cosets of solutions. Then the number of its O_S^*-cosets of solutions is at most*

$$C \exp\{2^{37nD} \cdot s^6 \log(5sD)\}.$$

We say that $\mathcal{M}$ is *degenerate* if there is a subalgebra $\mathbf{L}$ of $\mathbf{M}$ with $\mathbf{1}$ which is different from $\mathbf{K}$ and is admissible with respect to $\mathcal{M}$, and *non-degenerate* otherwise. Since the O_S^*-cosets of solutions of (9) are precisely the $(\mathcal{M}, \mathbf{K})$-families of solutions, our next corollary is an immediate consequence of Theorem 7.

COROLLARY 2. *If $\mathcal{M}$ is non-degenerate, then the number of O_S^*-cosets of solutions of* (9) *(or, equivalently, of* (8)*) is bounded above by the number occurring in* (11).

Qualitative versions of Corollary 2 were earlier established by Schmidt [33] (in case $K = \mathbb{Q}, S = \varnothing$), Schlickewei [30] (in case $K = \mathbb{Q}$) and Laurent [25] (in the general case) for the norm form equation (10), and by Evertse and Győry [6] for equation (8). In the case $K = \mathbb{Q}$, $S = \varnothing$, Schmidt [36] has recently derived the bound $C \cdot r^{c_1}$ with $c_1 = \min(2^{29n} \cdot r^2, (2n)^{n \cdot 2^{n+4}})$ for the number of solutions of the norm form equation (10) in the non-degenerate case. In terms of r, this bound is better than (11) in the special case under consideration. Very recently Evertse (private communication) has obtained another version of Corollary 2 with a bound which is better than (11) in terms of D but is in general weaker in terms of β. On combining our method of proof with that of Evertse, both Evertse's bound and our bound can be improved. Namely, the factor $\exp\{2^{37nD} \cdot s^6 \log(4sD)\}$ in our bounds (11), (12) can be replaced by

$$\exp\{2^{38nd} \cdot s^6 \log(8sD)\}. \tag{13}$$

The above-presented results will be published with detailed proofs in [20]. The proofs of Theorems 7 and 8 are rather long. The main steps in the proof of Theorem 7 are as follows. *Step* 1. Partition the set of solutions $\boldsymbol{\mu} \in \mathcal{M}$ of (9) into classes $\mathcal{C}$ such that two solutions $\boldsymbol{\mu}_1 = (\mu_{1i})_{i \in \mathcal{J}}$ and $\boldsymbol{\mu}_2 = (\mu_{2i})_{i \in \mathcal{J}}$ belong to the same class if both μ_{1i}/μ_{2i} and μ_{2i}/μ_{1i} are integral over O_S for each $i \in \mathcal{J}$. Generalizing a method of Schmidt [36], one can show that the number of classes $\mathcal{C}$ of solutions of (9) is at most C. *Step* 2. In the non-full case one can prove that the solutions of (9) belonging to a fixed class $\mathcal{C}$ are contained in

the union of at most $\exp\{2^{37nD} \cdot s^6 \log(4sD)\}$ sets of the form $\boldsymbol{\mu}\,\mathbf{L}$, where $\boldsymbol{\mu}$ is a solution and $\mathbf{L}$ is an admissible subalgebra of $\mathbf{M}$. The proof depends among other things on Theorem 1 and some arguments from [6]. *Step* 3. Finally, it is shown that the solutions under consideration which belong to a fixed set $\boldsymbol{\mu} \cdot \mathbf{L}$ are contained in the union of at most $\mathfrak{I}_{\mathbf{L}}$ $(\mathcal{M}, \mathbf{L})$-families of solutions.

§ 6. Applications to generalized systems of S-unit equations

Let $m \geq 2$ be an integer and $\Gamma = (O_S^*)^m$. For any m-tuple $\lambda = (\lambda_1, \ldots, \lambda_m)$ of non-negative integers, put $x^\lambda = x_1^{\lambda_1} \cdots x_m^{\lambda_m}$. Consider the following generalization of equation (2)

$$P_i(x) = \sum_{\lambda \in \mathcal{L}_i} p_i(\lambda) x^\lambda = 0 \text{ in } x \in \Gamma \text{ for } i \in \mathrm{I}, \tag{14}$$

where I is a finite index set, $p_i(\lambda) \in K$, and $\mathcal{L}_i$ is the support of P_i (i.e. the set of exponents λ for which the coefficient $p_i(\lambda)$ of x^λ in P_i is non-zero). Denote by $\mathcal{L}$ the disjoint union $\mathcal{L} = \coprod_{i \in \mathrm{I}} \mathcal{L}_i$ of the sets $\mathcal{L}_i$. Let $\mathcal{P}$ be a partition of $\mathcal{L}$; it induces partitions $\mathcal{L}_i = \coprod_{j \in \mathrm{J}_i} \mathcal{L}_{i,j}$ on each $\mathcal{L}_i$. Then $\mathcal{P}$ is said to be *compatible* with a $\gamma \in \Gamma$ if

$$\sum_{\lambda \in \mathcal{L}_{i,j}} p_i(\lambda) \gamma^\lambda = 0 \text{ for each } i \in \mathrm{I} \text{ and } j \in \mathrm{J}_i.$$

Further, we say that $\mathcal{P}$ is *maximal compatible* with γ if $\mathcal{P}'$ is not compatible with γ for any refinement $\mathcal{P}'$ of $\mathcal{P}$. Denote by $H_{\mathcal{P}}$ that subgroup of Γ whose elements γ have the property that for each $\mathcal{L}_{i,j}$, $\gamma^\lambda = \gamma^{\lambda'}$ if $\lambda, \lambda' \in \mathcal{L}_{i,j}$. If γ is a solution of (14), then so is every element of $\gamma H_{\mathcal{P}}$, where $\mathcal{P}$ is a partition of $\mathcal{L}$, compatible with γ. Laurent [25] proved that the set of solutions of (14) is the union of finitely many sets of the form $\gamma H_{\mathcal{P}}$ where γ is a solution and $\mathcal{P}$ is a partition of $\mathcal{L}$ which is maximal compatible with γ. In fact Laurent proved this result in a more general situation, for subgroups Γ of finite rank of $\mathbb{C}^*$. In his proof, he used his more general version of Theorem A (in which the solutions of (2) are taken from an arbitrary but fixed subgroup of finite rank of $\mathbb{C}^*$).

As a consequence of Theorem 8, we get the following quantitative version. Denote by r the cardinality of $\mathcal{L}$, and by k the rank of the matrix $(p_i(\lambda))_{i \in \mathrm{I}, \lambda \in \mathcal{L}}$ formed from the coefficients $p_i(\lambda)$ in (14). Put $n = r - k$.

THEOREM 9. *The set of solutions of* (14) *is the union of at most*

$$n^r \cdot \exp\{2^{37nd!} \cdot s^6 \log(4sd!)\} \tag{15}$$

sets of the form $\gamma H_{\mathcal{P}}$, *where* γ *is a solution of* (14) *and* $\mathcal{P}$ *is a partition of* $\mathcal{L}$ *which is maximal compatible with* γ. *Further, if* $K/\mathbb{Q}$ *is normal then* $d!$ *can be replaced by* d.

In the special case when (14) consists of a single inhomogeneous linear equation, Theorem 9 implies Theorem 1 with a slightly weaker bound. Indeed, in this special case Theorem 9 gives the bound (15) for the number of sets of solutions of the form $\gamma H_{\mathcal{P}_0}$ where $\mathcal{P}_0 = \{\mathcal{L}\}$, and $\mathcal{P}_0$ is maximal compatible with γ. But these solutions γ are just the non-degenerate solutions and $H_{\mathcal{P}_0} = (1, \dots, 1)$, hence our claim follows.

We remark that Theorem 9 can also be proven by combining the proof of Laurent with Theorem 1. Hence, apart from the forms of the bounds, Theorems 9 and 1 are equivalent. Finally, we note that using Theorem 8 with the improved bound (13), the second factor in (15) can be replaced by (13) with the choice $D = d!$

Proof of Theorem 9. If $n \leq 1$ and if (14) has a solution γ then all solutions are contained in $\gamma H_{\mathcal{P}_0}$ with the above $\mathcal{P}_0$, and $\mathcal{P}_0$ is maximal compatible with γ. Next suppose that $n \geq 2$. Put $\widetilde{\Gamma} = (O_S^*)^r$. To each solution $\gamma \in \Gamma$ of (14) we associate the solution $y = (y_\lambda) = (\gamma^\lambda)$ of the system of S-unit equations

$$\widetilde{P}_i(y) = \sum_{\lambda \in \mathcal{L}_i} p_i(\lambda) y_\lambda = 0 \text{ in } y = (y_\lambda) \in \widetilde{\Gamma} \text{ for } i \in \mathrm{I}. \tag{16}$$

This is in fact a special equation of the form (14). If $\mathcal{P}$ is a partition of $\mathcal{L}$ which is maximal compatible with γ, then it is at the same time maximal compatible with (γ^λ) in (16), and conversely. We define the subgroup $\widetilde{H}_{\mathcal{P}}$ of $\widetilde{\Gamma}$ in a similar way as $H_{\mathcal{P}}$ above. The solutions of (16) associated to the solutions in $\gamma H_{\mathcal{P}}$ of (14) are contained in $(\gamma^\lambda)\widetilde{H}_{\mathcal{P}}$. Conversely, it is easy to see that those solutions γ' of (14) for which the associated solutions (γ'^λ) of (16) belong to $(\gamma^\lambda)\widetilde{H}_{\mathcal{P}}$ are all contained in $\gamma H_{\mathcal{P}}$. Hence it suffices to give an upper bound for the number of sets of solutions of the form $(\gamma^\lambda)\widetilde{H}_{\mathcal{P}}$ of (16).

Let $V = \{\mathbf{y} = (y_\lambda) \in K^r : \sum_{\lambda \in \mathcal{L}_i} p_i(\lambda) y_\lambda = 0 \text{ for each } i \in \mathrm{I}\}$, $\mathfrak{M} = V \cap O_S^r$ and $F(\mathbf{y}) = \prod_{\lambda \in \mathcal{L}} y_\lambda$. Then $\dim_K K\mathfrak{M} = n$. It is easy to show that $\mathbf{y}$ is a solution of (16) if and only if it is a solution of

$$F(\mathbf{y}) \in O_S^* \text{ in } \mathbf{y} \in \mathfrak{M}.$$

This is an equation of type (8), hence it has an equivalent formulation of the form (9), say

$$\mathrm{N}(\boldsymbol{\mu}) \in O_S^* \text{ in } \boldsymbol{\mu} \in \mathcal{M}, \tag{17}$$

where now $\mathbf{M} = K^r$, $\mathcal{M} = \mathfrak{M}$ and $\boldsymbol{\mu} = \mathbf{y}$. It is easily seen that the sets of solutions $(\gamma^\lambda)\widetilde{H}_\mathcal{P}$ of (16) considered above are all maximal families of solutions of (17). By applying now Theorem 8 to (17) with $\beta = 1$, Theorem 9 follows.

§ 7. S-unit equations; effective results

The results presented above are all ineffective. Baker's method for estimating linear forms in logarithms of algebraic numbers and its p-adic analogue enabled one to give explicit bounds for the sizes of the solutions of (1). For a survey of effective results concerning (1), we refer to [37] or [11]. Let h_K and R_K denote the class number and regulator of K, respectively, and let P be the maximum of the rational primes divisible by $\mathfrak{p}_1, \ldots, \mathfrak{p}_{t-1}$ or $\mathfrak{p}_t$ (with the convention that $P = 1$ if $t = 0$). Further, denote by $H(\alpha)$ the height of an algebraic number α, i.e. the maximum absolute value of the coefficients of the minimal defining polynomial of α over $\mathbb{Z}$. By using Baker's method and its p-adic analogue I proved [16] in 1979 the following theorem in a slightly different form.

THEOREM C. *All solutions x_1, x_2 of (1) satisfy*

$$\max_{i=1,2} H(x_i) < \exp\{(c_1 s)^{c_2 s} \cdot P^{d+1} \cdot \log A\}$$

where $A = \max(H(\alpha_1), H(\alpha_2), 2)$ and $c_1 = c_1(d, h_K, R_K)$, $c_2 = c_2(d)$ are effectively computable numbers.

In [16], c_1 and c_2 were given explicitly.

Apart from certain special results concerning the case $n = 3$ (for references see [37] or [11]), for $n > 2$ there are no effective results which would make it possible to determine all non-degenerate solutions of (2). An effective version of Schmidt's Subspace Theorem and its p-adic generalization would yield an effective version of Theorem A. It seems however hopeless to make effective the Subspace Theorem by the present methods. We formulate now a weaker diophantine inequality whose effective resolution would also imply an effective version of Theorem A. Such an effective variant of Theorem A would be of great importance for applications. For instance, it would enable one to make effective all the results presented in §§ 2 to 6 of this paper.

Let $k, l \geq 1$ be integers, $\alpha_0, \ldots, \alpha_k, \beta_1, \ldots, \beta_l$ non-zero elements of K, and $b_{i1}, \ldots, b_{il}$ $(i = 1, \ldots, k)$ rational integers with absolute values at most B such that

(18) $\Lambda = \alpha_0 - \sum_{i=1}^{k} \alpha_i \beta_1^{b_{i1}} \dots \beta_l^{b_{il}}$ has no vanishing subsum containing α_0.

Consider a normalized multiplicative valuation $|\ .\ |_v$ of K, where v is one of the infinite places or the finite places corresponding to the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$.

PROPOSITION. *If*

$$0 < |\Lambda|_v < e^{-\delta B}$$

for some $\delta > 0$, *then* $B < C$, *where* C *is a number depending only on* $\alpha_0, \dots, \alpha_k, \beta_1, \dots, \beta_l, k, l, K, v$ *and* δ.

For $k = 1$, this is a non-effective version of Baker's famous theorem and its p-adic analogue; for a historical survey of Baker's theory, we refer to [1]. For $k \geq 1$, the above Proposition is a straightforward consequence of Theorem 2 of Evertse [3]. Since this result of [3] was derived from Schlickewei's p-adic Subspace Theorem [29], our Proposition is ineffective, i.e. C is not effectively computable for $k > 1$ by the method of proof.

It is easy to see that the assumption (18) is necessary in the above Proposition.

We now show that *an effective version of our Proposition would imply an effective variant of Theorem A.*

In what follows, we use the notation of § 2. c_1 to c_7 will denote numbers depending only on $\alpha_1, \dots, \alpha_n, n, K$ and S. Furthermore, the numbers c_1 to c_5 will be effectively computable.

Suppose that (2) has a non-degenerate solution, and let $x_1, \dots, x_n$ be such a solution. Let $\{v_1, \dots, v_s\}$ be the set of the infinite places of K and of the finite places of K corresponding to the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$. It is known (see e.g. [22]) that there are multiplicatively independent S-units $\eta_1, \dots, \eta_{s-1}$ in O_S with $H(\eta_j) \leq c_1$ for $j = 1, \dots, s-1$, such that

$$(19) \qquad \begin{cases} x_i = \gamma_i \eta_1^{b_{i1}} \dots \eta_{s-1}^{b_{i,s-1}} \text{ with some } b_{i1}, \dots, b_{i,s-1} \in \mathbb{Z} \text{ and some} \\ \gamma_i \in O_S^* \text{ for which } H(\gamma_i) \leq c_2 \text{ for } i = 1, \dots, n. \end{cases}$$

Further, the absolute values of the elements of the inverse of the matrix

$$(\log |\eta_j|_{v_p})_{p,j=1,\dots,s-1}$$

is less than c_3. Put $B_i = \max_{1 \leq j \leq s-1} |b_{ij}|$ for $i = 1, \dots, n$. We may suppose that $B = B_1 \geq B_2 \geq \dots \geq B_n$ and that $B > 0$. Fix a q with $1 \leq q \leq s$ for which $|x_1|_{v_q}$ is minimal. Then putting $|\bar{x}_1|_S = \max_{1 \leq p \leq s} |x_1|_{v_p}$, we get by the product formula that

$$|x_1|_{v_q}^{s-1} \leq \frac{1}{|\bar{x}_1|_S}. \tag{20}$$

Further, we have

$$\log |x_1/\gamma_1|_{v_p} = \sum_{j=1}^{s-1} b_{1j} \log |\eta_j|_{v_p} \quad \text{for } p = 1, \ldots, s,$$

whence

$$B < c_4 \max_{1 \leq p \leq s} \left| \log |x_1/\gamma_1|_{v_p} \right| < c_5 \log |\bar{x}_1|_S.$$

Together with (20) this gives

$$|x_1|_{v_q} < e^{-\delta B} \tag{21}$$

with the choice $\delta = ((s-1)c_5)^{-1}$. It follows from (2), (19) and (21) that

$$e^{-\delta B} > |x_1|_{v_q} = \left| (1/\alpha_1) - \sum_{i=2}^{n} (\alpha_i \gamma_i / \alpha_1)\, \eta_1^{b_{i1}} \ldots \eta_{s-1}^{b_{i,s-1}} \right|_{v_q} > 0. \tag{22}$$

Since the solution $x_1, \ldots, x_n$ is non-degenerate, the conditions of the Proposition are fulfilled. By applying now the above Proposition to (22) we obtain $B \leq c_6$ whence $\max_{1 \leq i \leq n} H(x_i) \leq c_7$, where c_6 and c_7 are effectively computable, provided that the corresponding constant C in the Proposition is also effectively computable.

REMARK. For $k = 1$ effective versions of the Proposition are available, hence we gave at the same time a proof for a non-explicit variant of Theorem C.

§ 8. Applications to binary forms and decomposable forms of given discriminant

In this section, we present a recent application of our effective Theorem C on S-unit equations.

Every binary form $F \in \mathbb{Z}[X, Y]$ of degree r can be factorized as $\prod_{i=1}^{r} (\alpha_i X - \beta_i Y)$ over some algebraic number field. The discriminant of F, denoted by $D(F)$, is defined by

$$D(F) = \prod_{1 \leq i < j \leq r} (\alpha_i \beta_j - \alpha_j \beta_i)^2.$$

$D(F)$ is a rational integer, and is independent of the factorization of F. Further, if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ (i.e. A has entries in $\mathbb{Z}$ and determinant 1) and $F_A(X,Y) = F(aX + bY, cX + dY)$ then $D(F_A) = D(F)$. Such binary forms F, F_A are called *equivalent*. It was proved by Lagrange [24] for $r = 2$ and by Hermite [23] for $r = 3$ that for every binary form $F \in \mathbb{Z}[X,Y]$ with degree r and non-zero discriminant, there is an $A \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$H(F_A) \leq c_1 |D(F)|$$

with some effectively computable absolute constant c_1. As usual, $H(P)$ denotes the height of a polynomial P with coefficients in $\mathbb{Z}$. In 1972 Birch and Merriman [2] showed that for every $r \geq 4$ and $D \neq 0$, there exist only finitely many equivalence classes of binary forms $F \in \mathbb{Z}[X,Y]$ of degree r and discriminant D. Here the dependence on r is not necessary because it was shown in 1974 (cf. [15, Part II]) that

$$r \leq 3 + 2 \log |D(F)| / (\log 3) \tag{23}$$

which is already sharp.

The proof of Birch and Merriman is ineffective. Independently of Birch and Merriman, I proved in 1973 (cf. [15, Part I]) an effective version for monic binary forms[2] $F \in \mathbb{Z}[X,Y]$ (i.e. with $F(1,0) = 1$). Further, I used an earlier version of Theorem C to prove (cf. [15, Part IV]) that for every monic binary form $F \in \mathbb{Z}[X,Y]$ with degree r and $D(F) \neq 0$ there is an $A \in \mathrm{SL}_2(\mathbb{Z})$ of the form $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ such that

$$H(F_A) \leq c_2 |D(F)|^{c_3}$$

where c_2, c_3 are effectively computable numbers depending only on r and the discriminant of the splitting field of F over $\mathbb{Q}$. On combining Theorem C with some new ideas, these effective results have recently been extended (cf. Evertse and Győry [8]) to all binary forms, making thereby effective the theorem of Birch and Merriman. Further, some generalizations have also been established for decomposable forms in $n \geq 2$ variables over $\mathbb{Z}$ (cf. Evertse and Győry [9], [10]). To present such a generalization, we have to introduce some further notions and notation.

Let $F(\mathbf{X}) = F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree r with splitting field K over $\mathbb{Q}$. Then it can be written as

[2] Most of the results of [15] were stated for polynomials in $\mathbb{Z}[X]$, but they can be easily reformulated for binary forms.

$F(\mathbf{X}) = l_1(\mathbf{X}) \dots l_r(\mathbf{X})$ where $l_1, \dots, l_r$ are linear forms with coefficients in K. Suppose that F is *squarefree* (i.e., that it is not divisible by the square of a linear form over K). Let $\mathcal{I}(F)$ denote the collection of linearly independent subsets $\{l_{i_1}, \dots, l_{i_n}\}$ of $\{l_1, \dots, l_r\}$ and assume that $\mathcal{I}(F) \neq \varnothing$. Denote by (α) the O_K-ideal generated by $\alpha \in K$, and by (l_i) the O_K-ideal generated by the coefficients of l_i, $i = 1, \dots, r$. Further, let $\det(l_{i_1}, \dots, l_{i_n})$ denote the coefficient determinant of $\{l_{i_1}, \dots, l_{i_n}\}$. Then there is a positive rational integer $D = D_{\mathbb{Z}}(F)$ such that

$$(D) = \prod_{\mathcal{I}(F)} \left\{ \frac{(\det(l_{i_1}, \dots, l_{i_n}))}{(l_{i_1}) \cdots (l_{i_n})} \right\}^2$$

where the product is taken over all sets $\{l_{i_1}, \dots, l_{i_n}\} \in \mathcal{I}(F)$. Further, the integer D does not depend on the choice of $l_1, \dots, l_r$, and $D_{\mathbb{Z}}(aF) = D_{\mathbb{Z}}(F)$ for all $a \in \mathbb{N}$. Hence we may assume that F is *primitive*, i.e. that its coefficients are relatively prime. $D_{\mathbb{Z}}(F)$ is called the *$\mathbb{Z}$-discriminant*[3] of F. For $\mathcal{I}(F) = \varnothing$, we put $D_{\mathbb{Z}}(F) = 0$. If for example F is a primitive, squarefree binary form then $D_{\mathbb{Z}}(F) = |D(F)|$. For $A \in \mathrm{SL}_n(\mathbb{Z})$, the decomposable forms $F(\mathbf{X}) \in \mathbb{Z}[X_1, \dots, X_n]$ and $F_A(\mathbf{X}) = F(A\mathbf{X})$ are called *equivalent*. Equivalent decomposable forms have the same $\mathbb{Z}$-discriminant.

Recently, we showed with Evertse [9], [10] the following.

THEOREM 10. *Let $F(\mathbf{X}) \in \mathbb{Z}[X_1, \dots, X_n]$ be a primitive, squarefree decomposable form of degree r with $D_{\mathbb{Z}}(F) > 0$ and splitting field K. Then there is an $A \in \mathrm{SL}_n(\mathbb{Z})$ such that*

$$H(F_A) \leq c_4 D_{\mathbb{Z}}(F)^{c_5} \tag{24}$$

where c_4, c_5 are effectively computable numbers which depend only on n, r and the discriminant D_K of K. Further, we have

$$r \leq 2^n - 1 + n \log D_{\mathbb{Z}}(F)/(\log 3). \tag{25}$$

For $n = 2$, (25) gives (23). One can prove (cf. [9]) that $|D_K| \leq c_6$ for some effectively computable number c_6 depending only on n, r and $D_{\mathbb{Z}}(F)$. Hence Theorem 10 implies the following.

[3] For polynomials in several variables there exists also another concept of discriminant; see e.g.[13].

COROLLARY. *For given $n \geq 2$ and $D > 0$, there are only finitely many equivalence classes of primitive, squarefree decomposable forms in $\mathbb{Z}[X_1, \ldots, X_n]$ with $D_{\mathbb{Z}}(F) = D$, and a full set of representatives of these classes can be effectively determined.*

For $n = 2$, this implies an effective version of the theorem of Birch and Merriman.

Both the results of [2], [15] and the theorems of [8], [9] and [10] have been extended to the case when the ground ring is the ring of S-integers of a number field. We note that in our papers [8], [9] and [10], several applications are given for example to algebraic numbers of given discriminant, to discriminant form inequalities, to small values of binary forms and decomposable forms at integral points and to arithmetical properties of discriminants of binary forms and decomposable forms.

The proofs of (24) and (25) will be published in [9] and [10], respectively. In the proof of (24), one of the main tools is Theorem C presented in § 7. The proof of Theorem 10 is long and complicated, hence we shall not outline it here. For instance, the proof of (24) takes about 25 pages.

Finally, we note that in the case $n = 2$, Evertse (private communication) has recently proved (24) with $c_5 = 21/(r-1)$. In his version the constant corresponding to c_4 is not, however, effectively computable.

References

[1] A. BAKER, *Transcendental Number Theory*, 3rd ed., Cambridge University Press, 1990.

[2] B.J. BIRCH and J.R.MERRIMAN, Finiteness theorems for binary forms with given discriminant, *Proc.London Math.Soc.* **25**(1972), 385-394.

[3] J.H. EVERTSE, On sums of S-units and linear recurrences, *Compositio Math.* **53**(1984), 225-244.

[4] J.H. EVERTSE, On equations in S-units and the Thue-Mahler equation, *Invent.Math.* **75**(1984), 561-584.

[5] J.H. EVERTSE, Decomposable form equations with a small linear scattering, to appear.

[6] J.H. EVERTSE and K. GYŐRY, Finiteness criteria for decomposable form equations, *Acta Arith.* **50**(1988), 357-379.

[7] J.H. EVERTSE and K. GYŐRY, On the numbers of solutions of weighted unit equations, *Compositio Math.* **66**(1988), 329-354.

[8] J.H. EVERTSE and K. GYŐRY, Effective finiteness results for binary forms with given discriminant, *Compositio Math.* **79**(1991), 169-204.

[9] J.H. EVERTSE and K. GYŐRY, Effective finiteness theorems for decomposable forms of given discriminant, *Acta Arith.*, to appear.

[10] J.H. EVERTSE and K. GYŐRY, Discriminants of decomposable forms, to appear.

[11] J.H. EVERTSE, K. GYŐRY, C.L. STEWART and R. TIJDEMAN, S-unit equations and their applications, *New Advances in Transcendence Theory* (A. Baker ed.), pp.110-174. Cambridge University Press, 1988.

[12] J.H. EVERTSE, K. GYŐRY, C.L. STEWART and R. TIJDEMAN, On S-unit equations in two unknowns, *Invent.Math.* **92**(1988), 461-477.

[13] I.M. GELFAND, A.V. ZELEVINSKY and M.M. KARPANOV, On discriminants of polynomials of several variables (Russian), *Functional Anal.and Appl.* **24**(1990), 1-4.

[14] K. GYŐRY, On the irreducibility of a class of polynomials I, II, III, IV, *Publ.Math.Debrecen* **18**(1971), 289-307; **19**(1972), 293-326; *J.Number Theory* **15** (1982), 164-181; *Acta Arith.*, to appear.

[15] K. GYŐRY, On polynomials with integer coefficients and given discriminant I, II, III, IV, V, *Acta Arith.* **23** (1973), 419-426; *Publ.Math.Debrecen* **21** (1974), 125-144; **23** (1976), 141-165; **25** (1978), 155-167; *Acta Math. Hungar.* **32** (1978), 175-190.

[16] K. GYŐRY, On the number of solutions of linear equations in units of an algebraic number field, *Comment.Math.Helv.* **54** (1979), 583-600.

[17] K. GYŐRY, On certain graphs composed of algebraic integers of a number field and their applications I, *Publ.Math.Debrecen* **27** (1980), 229-242.

[18] K. GYŐRY, On arithmetic graphs associated with integral domains I, II, in "*A Tribute to Paul Erdős*" (A.Baker, B.Bollobás, A.Hajnal eds.), Cambridge University Press, 1990, pp.207-222; in "*Sets, Graphs and Numbers*", Coll.Math.Soc.J.Bolyai **59**, North-Holland Publ.Comp., to appear.

[19] K. GYŐRY, Upper bounds for the numbers of solutions of unit equations in two unknowns, to appear.

[20] K. GYŐRY, On the numbers of families of solutions of decomposable form equation systems, to appear.

[21] K. GYŐRY and A. SCHINZEL, On a conjecture of Posner and Rumsey, in preparation.

[22] L. HAJDÚ, Some applications of the effective Dirichlet unit theorem, *Publ. Math. Debrecen*, to appear.

[23] CH. HERMITE, Sur l'introduction des variables continues dans la théorie des nombres, *J. reine Angew. Math.* **41** (1851), 191-216.

[24] J.L. LAGRANGE, Recherches d'arithmétique, *Nouv.Mém.Acad.Berlin*, 1773, pp.265-312. *Oeuvres*, III, pp.693-758.

[25] M. LAURENT, Equations diophantiennes exponentielles, *Invent. Math.* **78** (1984), 299-327.

[26] A.J. VAN DER POORTEN and H.P. SCHLICKEWEI, The growth conditions for recurrence sequences, Report 82.0041, Macquarie University, N.S.W.Australia, 1982.

[27] A.J. VAN DER POORTEN and H.P. SCHLICKEWEI, Additive relations in fields, *J.Austral.Math.Soc.*(Series A) **51** (1991), 154-170.

[28] E.C. POSNER and H. RUMSEY, JR., Polynomials that divide infinitely many trinomials, *Michigan Math.J.* **12** (1965), 339-348.

[29] H.P. SCHLICKEWEI, The $\mathfrak{p}$-adic Thue-Siegel-Roth-Schmidt Theorem, *Archiv Math.* **29** (1977), 267-270.

[30] H.P. SCHLICKEWEI, On norm form equations, *J.Number Theory* **9** (1977), 370-380.

[31] H.P. SCHLICKEWEI, S-unit equations over number fields, *Invent. Math.***102** (1990), 95-107.

[32] H.P. SCHLICKEWEI, The quantitative subspace theorem for number fields, to appear.

[33] W.M. SCHMIDT, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.* **191**(1971), 1-20.

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

[35] W.M. SCHMIDT, The subspace theorem in diophantine approximations, *Compositio Math.* **69** (1989), 121-173.

[36] W.M. SCHMIDT, The number of solutions of norm form equations, *Trans. Amer. Math. Soc.* **317** (1990), 197-227.

[37] T.N. SHOREY and R. TIJDEMAN, *Exponential diophantine equations*, Cambridge University Press, 1986.

Kálmán Győry
Mathematical Institute
Kossuth Lajos University
H–4010 Debrecen, Hungary