LINEAR EQUATIONS IN VARIABLES WHICH LIE IN A MULTIPLICATIVE GROUP

J.-H. Evertse, H.P. Schlickewei, W.M. Schmidt

Abstract

Let K be a field of characteristic 0 and let n be a natural number. Let Γ be a subgroup of the multiplicative group $(K^*)^n$ of finite rank r. Given $a_1, \ldots, a_n \in K^*$ write $A(a_1, \ldots, a_n, \Gamma)$ for the number of solutions $\boldsymbol{x} = (x_1, \ldots, x_n) \in \Gamma$ of the equation $a_1 x_1 + \ldots + a_n x_n = 1$, such that no proper subsum of $a_1 x_1 + \ldots + a_n x_n$ vanishes. We derive an explicit upper bound for $A(a_1, \ldots, a_n, \Gamma)$ which depends only on the dimension n and on the rank r.

1   Introduction

Let K be an algebraically closed field of characteristic 0. Write K^* for its multiplicative group of nonzero elements, and let $(K^*)^n$ be the direct product consisting of n-tuples $\boldsymbol{x} = (x_1, \ldots, x_n)$ with $x_i \in K^*$ $(i = 1, \ldots, n)$. So for $\boldsymbol{x}, \boldsymbol{y} \in (K^*)^n$ we write $\boldsymbol{x} * \boldsymbol{y} = (x_1 y_1, \ldots, x_n y_n)$. Let Γ be a subgroup of $(K^*)^n$ and suppose $(a_1, \ldots, a_n) \in (K^*)^n$. We will be dealing with equations

$$(1.1) \qquad a_1 x_1 + \ldots + a_n x_n = 1$$

with $\boldsymbol{x} \in \Gamma$.

A solution $\boldsymbol{x}$ of (1.1) is called *non-degenerate* if no subsum of the left hand side of (1.1) vanishes, i.e., if $\sum_{i \in I} a_i x_i \neq 0$ for every nonempty subset I of $\{1, \ldots, n\}$. Write $A(a_1, \ldots, a_n; \Gamma)$ for the number of non-degenerate solutions $\boldsymbol{x} \in \Gamma$ of equation (1.1).

Now suppose that Γ has rank r. This means that there exists a finitely generated subgroup Γ_0 of Γ, again of rank r, such that the factor group Γ/Γ_0 is a torsion group. In other words, for any $(x_1, \ldots, x_n) \in \Gamma$ there exists a natural number k such that

$$\left(x_1^k, \ldots, x_n^k\right) \in \Gamma_0.$$

We prove

Theorem 1.1 *Suppose Γ has finite rank r. Then the number $A(a_1, \ldots, a_n; \Gamma)$ of non-degenerate solutions $\boldsymbol{x} \in \Gamma$ of equation (1.1) satisfies the estimate*

(1.2) $$A(a_1, \ldots, a_n; \Gamma) \le A(n, r) = \exp((6n)^{3n}(r+1)).$$

The significant feature in our Theorem is its uniformity. Our bound (1.2) depends only upon the dimension of the variety V defined by equation (1.1) and upon the rank r of the group Γ. We also remark that once we have an estimate of the type

$$A(a_1, \ldots, a_n; \Gamma) \le f(a_1, \ldots, a_n; n, r)$$

with a function f depending only on $a_1, \ldots, a_n$, n and r, then we get immediately

$$A(a_1, \ldots, a_n; \Gamma) \le g(n, r)$$

where g is a function of n and r only. To see this, it suffices to consider the equation

$$y_1 + \ldots + y_n = 1$$

and to ask for solutions $\boldsymbol{y}$ in the group generated by $(a_1, \ldots, a_n)$ and Γ (which has rank $\le r + 1$).

It is conceivable that the function $A(n, r)$ we have given in (1.2) is far from best possible. In particular no special care has been taken for the numerical constants in (1.2). However *any function* $\widetilde{A}(n, r)$ which is suitable in (1.2) indeed has to depend on both n and r.

As for the dependence on n we give the following example. Pick elements $\alpha_1, \ldots, \alpha_n \in K^*$ with $\alpha_i \ne 1$ and $\alpha_i \ne \alpha_j$ $(1 \le i, j \le n, \ i \ne j)$ and consider the equation

(1.3) $$\begin{vmatrix} 1 & , & \ldots & , & 1 & , & 1 \\ \alpha_1 & , & \ldots & , & \alpha_n & , & 1 \\ & & \vdots & & & & \vdots \\ \alpha_1^{n-1} & , & \ldots & , & \alpha_n^{n-1} & , & 1 \\ x_1 & , & \ldots & , & x_n & , & 1 \end{vmatrix} = 0.$$

This yields an equation

(1.4) $$b_1 x_1 + \ldots + b_n x_n = 1$$

with $b_i \in K^*$. But clearly (1.4) has the n solutions $\boldsymbol{x}_i = (x_{1i}, \ldots, x_{ni}) = (\alpha_1^i, \ldots, \alpha_n^i)$ $(i = 0, \ldots, n-1)$. Moreover, in the generic case, these will be non-degenerate solutions. Therefore $\widetilde{A}(n, 1) \ge n$. Bavencoffe and Bézivin [1] have given a more sophisticated example which even shows that

$$\widetilde{A}(n, 1) \ge c\, n^2$$

2

where c is an absolute constant.

On the other hand, suppose $n = p - 1$ where p is a prime. Let ζ be a primitive p-th root of unity. Then

$$-\zeta - \zeta^2 - \ldots - \zeta^{p-1} = 1,$$

and the same is true for any permutation of the roots on the left hand side. Therefore, for $n = p - 1$ we have $\widetilde{A}(n, 0) \geq n!$. We do not know what should be in general the correct order of dependence on n in $\widetilde{A}(n, r)$.

As for the dependence on r, Erdős, Stewart and Tijdeman [7] have constructed an example which shows that

$$\widetilde{A}(2, r) \geq \exp\left(c\left(\frac{r}{\log r}\right)^{\frac{1}{2}}\right)$$

where c is an absolute constant. This example may be extended to give

$$\widetilde{A}(n, r) \geq \exp\left(c(n)\left(\frac{r}{\log r}\right)^{\frac{n-1}{n}}\right)$$

where $c(n)$ depends only upon n. It has been conjectured that the correct order of magnitude in r should be of the shape

$$\exp\left(c(n)\left(\frac{r}{\log r}\right)^{\frac{n}{n+1}}\right)$$

or even

$$\exp\left(c(n)\ r^{\frac{n}{n+1}}\right).$$

For $n = 2$, the assertion of Theorem 1.1 has been proved earlier. Schlickewei [21] showed that $A(a_1, a_2, \Gamma) \leq c(r)$ and Beukers and Schlickewei [2] proved that we may take

(1.5) $$c(r) = 2^{9(r+1)},$$

which clearly is much better than our bound $A(2, r)$.

For arbitrary n and for $r = 0$, i.e., when we are asking for solutions of equation (1.1) in roots of unity, Schlickewei [20] proved that we do not get more than $2^{4n!}$ non-degenerate solutions. This has been considerably improved by Evertse [11]. He obtained the bound

$$(n + 1)^{3(n+1)^2},$$

and this is much better than our bound $A(n, 0)$ in (1.2).

3

In all other cases, i.e., when $n \geq 3$ and $r \geq 1$, Theorem 1.1 is new. Previously, bounds involving only the dimension n and the rank r of the group Γ had been obtained only in the case when Γ is the n-fold product of the group of S-units of a number field. We briefly review what was known in the literature. Before we do so, let us remark that instead of the group $\Gamma \subset (K^*)^n$ we could have considered a group $\Gamma' \subset K^*$ of finite rank r', say, and we could have asked for solutions of (1.1) with $x_i \in \Gamma'$. The difference is only minor, as the direct product $(\Gamma')^n$ then is a subgroup of $(K^*)^n$ of rank $n r'$.

Writing $A'(a_1, \ldots, a_n; \Gamma')$ and $A'(n, r)$ for the quantities in (1.2) with respect to $\Gamma' \subset K^*$ we therefore see that

$$A'(n, r) \leq A(n, nr).$$

The classical instances of equation (1.1) are S-unit equations. Let F be a number field, let S be a finite set of places of F containing all the archimedean ones and write $\Gamma(S) \subset F^*$ for the group of S-units of F. For $n = 2$ and for $F = \mathbb{Q}$, Mahler [14] has shown that

$$A'(a_1, a_2; \Gamma(S)) < \infty.$$

Lang [13] has extended Mahler's result to arbitrary number fields and also to the case of arbitrary fields K of characteristic 0 and groups $\Gamma \subset K^*$ of finite rank.

For general $n \geq 2$, Evertse [9] and van der Poorten and Schlickewei [15] have shown that

$$A'(a_1, \ldots, a_n; \Gamma(S)) < \infty.$$

The first quantitive result in our context is due to Evertse [8]. He proved for sets S of cardinality s

(1.6) $$A'(a_1, a_2; \Gamma(S)) \leq 3 \cdot 7^{4s}.$$

Notice that the group $\Gamma(S)$ is finitely generated and has rank $s - 1$. Therefore (1.6) may be viewed as a special instance of a result of type (1.2) (cf. also (1.5)).

For arbitrary $n \geq 2$, Schlickewei [17] proved that

(1.7) $$A'(a_1, \ldots, a_n; \Gamma(S)) \leq c(n, s)$$

where c is a function depending on n and s only. So (1.7) again is of the same type as (1.2). The best explicit value for $c(n, s)$ is due to Evertse [10]. He proved

(1.8) $$c(n, s) \leq 2^{35n^4 s}.$$

Now suppose Γ is an arbitrary finitely generated subgroup of rank r of the multiplicative group F^* of a number field F of degree d. Taking for S the places in $M_\infty(F)$ and those

4

finite places whose associated prime ideal divides some of the generators of Γ, we see that Γ will be a subgroup of the group $\Gamma(S)$ of S-units. However the rank $s-1$ of $\Gamma(S)$ may be much larger than the rank r of the original group Γ. So in general, even for groups $\Gamma \subset F^*$ the bound $A'(n,r)$ we obtain with (1.2) will be much better than the bound of type (1.6) or (1.8) we get using the group $\Gamma(S)$. Another disadvantage of $\Gamma(S)$ is the fact that $s = |S| \geq d/2$, d being the degree of F. Therefore the device of estimating $A'(a_1, \ldots, a_n; \Gamma)$ by $A'(a_1, \ldots, a_n; \Gamma(S))$ implicitly always introduces a dependence upon the degree of F in the bound.

Schlickewei [19] has estimated $A'(a_1, \ldots, a_n; \Gamma)$ in terms of n, r and d. And here Schlickewei and Schmidt [24] have shown that

$$(1.9) \qquad A'(a_n, \ldots, a_n; \Gamma) \leq (2d)^{41n^3 r} r^{n^2 r}.$$

The essential difference between (1.9) and (1.2) is the occurrence of the degree d in (1.9). The problem in the current paper is to estimate a quantity like the one on the left hand side of (1.9) avoiding any dependence on d. We will come back to this at the end of this section.

It is well known that results on equations (1.1) are closely related to results on multiplicities of linear recurrence sequences. A *linear recurrence sequence of order n* is a sequence $\{u_m\}_{m \in \mathbb{Z}}$ of elements in our field K satisfying a relation

$$(1.10) \qquad u_{m+n} = c_1 u_{m+n-1} + \ldots + c_n u_m \quad (m \in \mathbb{Z}).$$

Here $c_1, \ldots, c_n$ are fixed elements from K. We assume that $n > 0$ and that relation (1.10) is minimal, i.e., that u_m does not satisfy a relation of type (1.10) for some $n' < n$. Then we have in particular
$$(1.11) \qquad c_n \neq 0$$
(and $\{u_m\}$ is not the zero sequence). Define the *companion polynomial* by

$$(1.12) \qquad G(z) = z^n - c_1 z^{n-1} - \ldots - c_n = \prod_{\rho=1}^{r} (z - \alpha_\rho)^{\sigma_\rho}$$

with distinct roots α_ρ of respective multiplicities σ_ρ $(\rho = 1, \ldots, r)$. By (1.11), $\alpha_\rho \neq 0$ for $\rho = 1, \ldots, r$. Then we have a representation

$$(1.13) \qquad u_m = \sum_{\rho=1}^{r} f_\rho(m) \alpha_\rho^m$$

where the f_ρ are polynomials. It follows from the minimality of relation (1.10) that $f_\rho(x)$ has degree $\sigma_\rho - 1$ $(\rho = 1, \ldots, r)$. The sequence $\{u_m\}$ is called *non-degenerate* if no quotient α_i/α_j $(1 \leq i < j \leq r)$ is a root of unity.

5

We say that the sequence $\{u_m\}$ is *simple* if the companion polynomial $G(z)$ has only simple zeros. In that case the quantities σ_ρ in (1.12) are all equal to 1, so the polynomials f_ρ in (1.13) are constants and we have

$$(1.14) \qquad\qquad u_m = a_1 \, \alpha_1^m + \ldots + a_n \, \alpha_n^m \quad (m \in \mathbb{Z})$$

with non-zero coefficients $a_i \in K$ and with distinct elements $\alpha_i \in K^*$.

Write $\mathcal{S}(u_m)$ for the set of zeros of $\{u_m\}$, i.e., for the set of solutions $k \in \mathbb{Z}$ of the equation

$$(1.15) \qquad\qquad\qquad\qquad u_k = 0.$$

When $\{u_m\}$ has order 1, then trivially $\mathcal{S}(u_m) = \emptyset$. Therefore from now on we will only consider sequences $\{u_m\}$ of order $n \geq 2$.

The classical theorem of Skolem–Mahler–Lech says that for arbitrary linear recurrence sequences $\{u_m\}$ of order ≥ 2, $\mathcal{S}(u_m)$ is the union of a finite set of integers and a finite number of arithmetic progressions. This implies in particular that for non-degenerate sequences $\{u_m\}$ the set $\mathcal{S}(u_m)$ is finite.

An old conjecture says that for non-degenerate sequences $\{u_m\}$ of order $n \geq 2$ the cardinality of $\mathcal{S}(u_m)$ is bounded in terms of n only. For $n = 2$, by non-degeneracy it is obvious that $|\mathcal{S}(u_m)| \leq 1$. Schlickewei [22] proved the conjecture for $n = 3$. Beukers and Schlickewei [2] derived for non-degenerate sequences $\{u_m\}$ of order 3 the bound

$$|\mathcal{S}(u_m)| \leq 61.$$

For non-degenerate sequences $\{u_m\}$ of *rational numbers* and of arbitrary order n, the conjecture was proved by Schlickewei [18].

We now study *simple* recurrence sequences $\{u_m\}$ (never mind whether degenerate or not). For such sequences, in view of (1.14), equation (1.15) becomes

$$(1.16) \qquad\qquad a_1 \, \alpha_1^k + \ldots + a_n \, \alpha_n^k = 0 \quad (k \in \mathbb{Z}).$$

Applying Theorem 1.1 to groups Γ of rank ≤ 1 we deduce

Theorem 1.2 *Let K be an algebraically closed field of characteristic 0. Suppose $n \geq 3$ and let $\{u_m\}_{m \in \mathbb{Z}}$ be a simple linear recurrence sequence in K of order n. Then there are integers $k_1, \ldots, k_{q_1}$ and arithmetic progressions $T_1, \ldots, T_{q_2}$ of the shape*

$$T_i = \{a_i + t\, v_i \mid t \in \mathbb{Z}\}, \quad a_i, v_i \in \mathbb{Z}, \quad v_i \neq 0 \quad (i = 1, \ldots, q_2),$$

where

$$(1.17) \qquad\qquad\qquad q_1 + q_2 \leq \exp((6n)^{3n}),$$

such that

$$\mathcal{S}(u_m) = \{k \in \mathbb{Z} \mid u_k = 0\} = \{k_1, \ldots, k_{q_1}\} \cup T_1 \cup \ldots \cup T_{q_2}.$$

In particular, if $\{u_m\}$ is non-degenerate, then $\mathcal{S}(u_m)$ has cardinality

$$(1.18) \qquad\qquad |\mathcal{S}(u_m)| \leq \exp((6n)^{3n}).$$

Theorem 1.2 is a uniform quantitative version of the Skolem–Mahler–Lech theorem. In the meantime, W.M. Schmidt [27] has proved that *for any non-degenerate sequence $\{u_m\}$ (even if not simple) the set $\mathcal{S}(u_m)$ has cardinality bounded in terms of the order n only.*

The bound obtained by Schmidt in this more general setting is triply exponential in n. Moreover, in his recent paper [28], Schmidt has also proved that Theorem 1.2 is true in general and not only for simple sequences. However, again instead of (1.17) he gets a bound which is triply exponential in n.

The new ingredients in our proof are as follows. On the one hand we apply the absolute version of the Subspace Theorem due to Evertse and Schlickewei [12]. On the other hand we use a result of Schmidt [26] on lower bounds for heights of points on varieties.

In proving our Theorems, by a specialization argument we may restrict ourselves to the situation when in (1.1) (or in (1.16) respectively) all quantities involved are algebraic. Indeed it suffices to prove a result of type (1.9), but without dependence upon the degree d of the number field.

An application of the Subspace Theorem then gives an assertion on the "large" solutions of equation (1.1). In fact the bound it gives for the number of "large" solutions depends only upon the "good" parameters n and r. So for the quantitative result all depends upon the parameters showing up in the definition of "small". Usually in this definition the parameters n and d showed up. Thus in estimating the number of "small" solutions the parameter d could not be avoided. In a recent paper [12], Evertse and Schlickewei have proved a new absolute quantitative version of the Subspace Theorem which in turn makes use of the absolute Minkowski Theorem established by Roy and Thunder [16]. The definition of "small" in the absolute Subspace Theorem does not depend upon the degree d at all.

Unfortunately this does not suffice yet. To handle the "small" solutions usually one applies a gap principle. For this purpose one needs a *lower* bound for the height of a small solution. Traditionally, this was achieved via Dobrowolski's theorem [6]. But here again the degree d comes in. To overcome this difficulty we apply lower bounds for heights of points on varieties as given in recent work of Zhang [29], Bombieri and Zannier [3], and in explicit form for the first time by Schmidt [26].

Remark In recent work [4], [5], David and Philippon have proved a slight sharpening of Schmidt's results [26]. It is easily seen that with this sharpening the bound for $A(n, r)$ given in (1.2) can be improved to

$$A(n, r) \leq \exp((r + 1) \exp(c_1 n)).$$

Similarly, the bound (1.17) can be improved to

$$q_1 + q_2 \leq \exp \exp(c_1 n).$$

Here c_1 is an absolute constant.

2 Algebraic Points

In the case when in (1.1) all quantities involved are algebraic we can prove a slightly more general result.

Let F be a number field. Write $M(F)$ for the set of its places. For each $v \in M(F)$ we let $|\;|_v$ be the associated absolute value such that for $x \in \mathbb{Q}$ we have

$$(2.1) \qquad |x|_v = \begin{cases} |x| & \text{if } v|\infty \\ |x|_p & \text{if } v|p, \end{cases}$$

where p is a prime number and where $|p|_p = p^{-1}$. We denote the completion of F at the place v by F_v; similarly for $p \in M(\mathbb{Q})$, $\mathbb{Q}_p$ denotes the completion of $\mathbb{Q}$ at p (so that $\mathbb{Q}_\infty = \mathbb{R}$, the field of real numbers). The *normalized* absolute value $\|\;\|_v$ on F then is defined by

$$(2.2) \qquad \|x\|_v = |x|_v^{[F_v:\mathbb{Q}_p]/[F:\mathbb{Q}]} \quad \text{if } v|p.$$

We write $\overline{\mathbb{Q}}$ for the algebraic closure of $\mathbb{Q}$. Given $\boldsymbol{x} = (x_1, \ldots, x_n) \in \overline{\mathbb{Q}}^n$, we define the absolute multiplicative height $H(\boldsymbol{x})$ as follows: we choose a number field F such that $\boldsymbol{x} \in F^n$ and we put

$$(2.3) \qquad H(\boldsymbol{x}) = \prod_{v \in M(F)} \max\{1, \|x_1\|_v, \ldots, \|x_n\|_v\}.$$

Notice that (2.3) does not depend on the choice of F. We define the absolute logarithmic height $h(\boldsymbol{x})$ by

$$(2.4) \qquad h(\boldsymbol{x}) = \log H(\boldsymbol{x}).$$

In [23], Schlickewei and Schmidt proved the following result. *Let F be a number field of degree d. Let*

$$(2.5) \qquad \Gamma \subset (F^*)^n \text{ be a finitely generated subgroup with } \operatorname{rank} \Gamma = r.$$

8

Consider the equation

(2.6)
$$y_1 + \ldots + y_n = 1,$$

to be solved in vectors $\boldsymbol{y} = (y_1, \ldots, y_n) \in F^n$ of the shape

(2.7)
$$\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z} \quad \text{with} \quad \boldsymbol{x} \in \Gamma, \quad \boldsymbol{z} \in (\mathbb{Q}^*)^n, \quad h(\boldsymbol{z}) \leq \frac{1}{4n^2} h(\boldsymbol{x}).$$

Then the set of solutions $\boldsymbol{y}$ of (2.6), (2.7) is contained in the union of not more than

(2.8)
$$2^{30n^2}(32n^2)^r d^{3r+2n}$$

proper linear subspaces of F^n.

Instead of (2.5), we now suppose

(2.9)
$$\Gamma \text{ is a subgroup of } (\overline{\mathbb{Q}}^*)^n \text{ of rank } r.$$

So now Γ is not necessarily finitely generated. (On the other hand, we notice that (2.9) is more special than the setting studied in Section 1, where we assumed $\Gamma \subset (K^*)^n$ for some algebraically closed field K of characteristic 0, so that in fact implicitly we assumed that $\overline{\mathbb{Q}} \subset K$.)

Again we consider equation (2.6). However, instead of (2.7) we now ask for solutions $\boldsymbol{y} \in (\overline{\mathbb{Q}}^*)^n$ of the shape

(2.10) $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z} \quad \text{with} \quad \boldsymbol{x} \in \Gamma, \quad \boldsymbol{z} \in (\overline{\mathbb{Q}}^*)^n, \quad h(\boldsymbol{z}) \leq n^{-1} \exp(-(4n)^{3n})(1 + h(\boldsymbol{x})).$

We prove

Theorem 2.1 *Let $n \geq 2$. Suppose that Γ is a subgroup of $(\overline{\mathbb{Q}}^*)^n$ of finite rank r. Then the set of points $\boldsymbol{y} \in \overline{\mathbb{Q}}^n$ satisfying (2.6) and (2.10) is contained in the union of not more than*

(2.11)
$$B(n, r) = \exp((5n)^{3n}(r+1))$$

proper linear subspaces of $\overline{\mathbb{Q}}^n$.

It turns out that Theorem 1.1 as well as Theorem 1.2 follow from Theorem 2.1. Indeed in Section 3 we give a specialization argument which reduces the situation we encounter in Section 1 to a setting where all quantities are algebraic. In Section 4 we then prove Theorem 1.1 by means of induction using Theorem 2.1. In Section 5, Theorem 1.2 will be deduced from Theorem 1.1. The remainder of the paper, starting with Section 6, then is devoted to the proof of Theorem 2.1.

3 Specialization

Let K be the field from Section 1. Since K is algebraically closed and has characteristic equal to zero, we may suppose that $\overline{\mathbb{Q}} \subset K$.

Lemma 3.1 *Let $U = \{u_1, \ldots, u_k\}$ be a finite subset of K. Then there exists a ring homomorphism*

$$(3.1) \qquad\qquad \varphi : \overline{\mathbb{Q}}[U] \longrightarrow \overline{\mathbb{Q}}$$

whose restriction to $\overline{\mathbb{Q}}$ is the identity.

Proof We recall the proof of this well-known fact. Let $\mathcal{J}$ be the ideal of polynomials $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_k]$ with $f(u_1, \ldots, u_k) = 0$. Clearly $1 \notin \mathcal{J}$ and therefore $\mathcal{J} \neq \overline{\mathbb{Q}}[X_1, \ldots, X_k]$. Thus by Hilbert's Nullstellensatz there exists a point $\boldsymbol{c} = (c_1, \ldots, c_k) \in \overline{\mathbb{Q}}^k$ with $f(\boldsymbol{c}) = 0$ for each $f \in \mathcal{J}$. The ring $\overline{\mathbb{Q}}[U] = \overline{\mathbb{Q}}[u_1, \ldots, u_k]$ consists of all expressions $g(u_1, \ldots, u_k)$ with $g \in \overline{\mathbb{Q}}[X_1, \ldots, X_k]$. We consider the diagram

$$\overline{\mathbb{Q}}[u_1, \ldots, u_k] \longrightarrow \overline{\mathbb{Q}}[X_1, \ldots, X_k]/\mathcal{J} \longrightarrow \overline{\mathbb{Q}}$$

where the mappings are given by

$$g(u_1, \ldots, u_k) \longmapsto g \bmod \mathcal{J} \longmapsto g(c_1, \ldots, c_k).$$

These mappings are well-defined ring homomorphisms leaving $\overline{\mathbb{Q}}$ invariant. Their composition yields the desired homomorphism φ in (3.1).

In order to prove Theorem 1.1, it will suffice to show that any *finite* subset M of the set of non-degenerate solutions of equation (1.1) has cardinality

$$(3.2) \qquad\qquad \leq A(n, r).$$

Write $M = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$ with $\boldsymbol{x}_i = (x_{i1}, \ldots, x_{in})$ $(i = 1, \ldots, m)$. We want to map M injectively to a set of non-degenerate solutions of an equation of type (1.1) where however $\boldsymbol{a} = (a_1, \ldots, a_n) \in \overline{\mathbb{Q}}^n$ and $\Gamma \subset (\overline{\mathbb{Q}}^*)^n$. We will then be in a position to apply Theorem 2.1.

Let $U = \{u_1, \ldots, u_k\} \subset K$ be the set consisting of the following elements:

$$(3.3) \qquad\qquad a_1, \ldots, a_n;$$

$$(3.4) \qquad\qquad x_{ij} \quad (i = 1, \ldots, m; \, j = 1, \ldots, n);$$

10

$$(3.5) \qquad \sum_{j \in I} a_j \, x_{ij} \quad (i = 1, \ldots, m; \; I \subset \{1, \ldots, n\}, \; I \neq \emptyset);$$

$$(3.6) \qquad x_{i_1, j} - x_{i_2, j} \quad (1 \leq i_1 < i_2 \leq m; \; j = 1, \ldots, n);$$

(3.7)   the multiplicative inverses of all non-zero numbers in (3.3)–(3.6).

Let φ be a ring homomorphism from $\overline{\mathbb{Q}}\,[U]$ into $\overline{\mathbb{Q}}$ as in Lemma 3.1. By (3.7), the non-zero elements in U are units in the ring $\overline{\mathbb{Q}}\,[U]$. Therefore they are mapped by φ to non-zero elements of $\overline{\mathbb{Q}}$.

Write $a'_j = \varphi(a_j)$, $x'_{ij} = \varphi(x_{ij})$, $\boldsymbol{x}'_i = (x'_{i1}, \ldots, x'_{in})$ $(i = 1, \ldots, m; \; j = 1, \ldots, n)$. Then by (1.1) we get

$$(3.8) \qquad a'_1 \, x'_{i1} + \ldots + a'_n \, x'_{in} = \varphi \left(\sum_{j=1}^{n} a_j \, x_j \right) = 1 \quad (i = 1, \ldots, m).$$

The numbers in (3.5), by non-degeneracy, are non-zero. Therefore their images under φ are non-zero as well. We may conclude that

$$(3.9) \qquad \sum_{j \in I} a'_j \, x'_{ij} \neq 0 \quad (i = 1, \ldots, m; \; I \subset \{1, \ldots, n\}, \; I \neq \emptyset).$$

Moreover, the non-zero numbers in (3.6) have non-zero images. This implies that $\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_m$ are distinct.

Let Γ_1 be the subgroup of Γ generated by $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$. Then Γ_1 has rank $\leq r$. We infer from (3.7) that $\Gamma_1 \subset (\overline{\mathbb{Q}}\,[U])^n$. Let Γ'_1 be the multiplicative subgroup of $(\overline{\mathbb{Q}}^*)^n$ generated by $\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_n$. Then Γ'_1 is the image of Γ_1 under the group homomorphism

$$(x_1, \ldots, x_n) \longmapsto (\varphi(x_1), \ldots, \varphi(x_n)).$$

We may conclude that Γ'_1 has rank $\leq r$.

Altogether we see that $\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_m$ are distinct, non-degenerate solutions of the equation

$$(3.10) \qquad a'_1 \, x'_1 + \ldots + a'_n \, x'_n = 1$$

to be solved in vectors

$$(3.11) \qquad \boldsymbol{x}' = (x'_1, \ldots, x'_n) \in \Gamma'_1.$$

Here $a'_1, \ldots, a'_n \in \overline{\mathbb{Q}}^*$ and Γ'_1 is a subgroup of $(\overline{\mathbb{Q}}^*)^n$ of rank $\leq r$.

Notice that $A(n, r)$ in (1.2) satisfies

$$A(n, r_1) < A(n, r_2) \quad \text{for} \quad r_1 < r_2.$$

Therefore we have shown

Lemma 3.2 *In order to prove Theorem* 1.1, *we may suppose without loss of generality that* $K = \overline{\mathbb{Q}}$.

4 Deduction of Theorem 1.1 from Theorem 2.1

In view of Lemma 3.2, we may suppose that $K = \overline{\mathbb{Q}}$. Under this hypothesis we show that equation (1.1) does not have more than

$$A(n, r)$$

non-degenerate solutions $\boldsymbol{x} \in \Gamma$, where

$$(4.1) \qquad\qquad A(n, r) = \exp((6n)^{3n}(r + 1))$$

as in (1.2).

The case $n = 1$ is obvious. Now suppose $n > 1$ and our claim to be shown for $n' < n$.

Let $B(n, r)$ be the quantity from (2.11) in Theorem 2.1. Write Γ' for the group generated by $\boldsymbol{a} = (a_1, \ldots, a_n)$ and Γ. So if $\boldsymbol{x}$ runs through Γ, the point $\boldsymbol{y} = \boldsymbol{a} * \boldsymbol{x}$ runs through Γ'. Clearly Γ' has rank $\leq r + 1$. Thus the solutions $\boldsymbol{x} \in \Gamma$ of (1.1) give rise to solutions $\boldsymbol{y} \in \Gamma'$ of the equation

$$(4.2) \qquad\qquad y_1 + \ldots + y_n = 1.$$

Applying Theorem 2.1 with $\boldsymbol{z} = (1, \ldots, 1)$ to equation (4.2) and the group Γ', we may infer that the set of solutions $\boldsymbol{y} \in \Gamma'$ of (4.2) (never mind whether degenerate or not) is contained in the union of $B(n, r + 1)$ proper linear subspaces of $\overline{\mathbb{Q}}^n$. Consequently, also the set of solutions $\boldsymbol{x} \in \Gamma$ of equation (1.1) is contained in the union of

$$(4.3) \qquad\qquad \leq B(n, r + 1)$$

proper linear subspaces of $\overline{\mathbb{Q}}^n$.

Let V be one of these subspaces, defined by an equation

$$(4.4) \qquad\qquad \sum_{i \in I} b_i \, x_i = 0$$

where I is a subset of $\{1, \ldots, n\}$ of cardinality $|I| \geq 2$, and where $b_i \neq 0$ for $i \in I$. Let J be a non-empty subset of I and consider those $\boldsymbol{x} \in \Gamma \cap V$ for which

$$(4.5) \qquad\qquad \sum_{i \in J} b_i \, x_i = 0,$$

12

but no proper non-empty subsum of (4.5) vanishes. Thus $2 \leq |J| \leq n$.

Let us suppose for the moment that $J = \{1, \ldots, \ell\}$. Writing $c_i = -b_i/b_1$ we get with $w_i = x_i/x_1$ $(i = 2, \ldots, \ell)$

$$(4.6) \qquad \sum_{i=2}^{\ell} c_i \, w_i = 1.$$

Now $(x_1, \ldots, x_\ell, x_{\ell+1}, \ldots, x_n) \in \Gamma$, therefore $(w_2, \ldots, w_\ell)$ lies in the group Γ_1 consisting of $(\ell - 1)$-tuples such that

$$(4.7) \qquad (u, u \, w_2, \ldots, u \, w_\ell, u_{\ell+1}, \ldots, u_n) \in \Gamma$$

for some $u, u_{\ell+1}, \ldots, u_n$. Let Γ_2 be the group of elements

$$(4.8) \qquad (x, \ldots, x, x_{\ell+1}, \ldots, x_n) \in \Gamma.$$

The map

$$(x_1, x_2, \ldots, x_\ell, x_{\ell+1}, \ldots, x_n) \longmapsto \left(\frac{x_2}{x_1}, \ldots, \frac{x_\ell}{x_1} \right)$$

is a surjective homomorphism $\Gamma \to \Gamma_1$ with kernel Γ_2. Therefore, when $\operatorname{rank} \Gamma_i = r_i$ we have $r_1 + r_2 = r$.

By induction the equation (4.6) has at most $A(\ell - 1, r_1)$ non-degenerate solutions. When $(w_2, \ldots, w_\ell)$ is such a solution, fix $u, u_{\ell+1}, \ldots, u_n$ with (4.7). The original solution $\boldsymbol{x}$ of (1.1) is of the form

$$(4.9) \qquad (x, x \, w_2, \ldots, x \, w_\ell, x_{\ell+1}, \ldots, x_n),$$

so that

$$(4.10) \qquad b \, x + \sum_{i=\ell+1}^{n} a_i \, x_i = 1$$

with $b = a_1 + \sum_{i=2}^{\ell} a_i \, w_i$. If the solution $\boldsymbol{x}$ of (1.1) is non-degenerate, then so is the solution $(x, x_{\ell+1}, \ldots, x_n)$ of (4.10).

Taking the quotient of (4.7), (4.9) we see that $(x/u, \ldots, x/u, x_{\ell+1}/u_{\ell+1}, \ldots, x_n/u_n) \in \Gamma_2$. With the notation $x' = x/u$, $x_i' = x_i/u_i$ $(i = \ell + 1, \ldots, n)$, (4.10) becomes

$$(4.11) \qquad b'x' + \sum_{i=\ell+1}^{n} a_i' \, x_i' = 1$$

where $b' = b \, u$, $a_i' = a_i \, u_i$ $(i = \ell + 1, \ldots, n)$. By induction, and since $n - \ell + 1 < n$, (4.11) has not more than $A(n - \ell + 1, r_2)$ non-degenerate solutions. Combining this with the

bound $A(\ell - 1, r_1)$ for the number of solutions of (4.6), we see that (4.5) gives rise to not more than

(4.12) $$A(\ell - 1, r_1)\, A(n - \ell + 1, r_2) \leq A(n - 1, r)$$

solutions of (1.1); the last inequality is a consequence of

$$A(a, r_1)\, A(b, r_2) \leq A(a + b - 1, r_1 + r_2),$$

which follows from the definition (4.1) of $A(n, r)$. Taking account of the possible subsets J of I, we see that each subspace V contains at most $2^n A(n - 1, r)$ solutions. We still have to multiply this by the number $B(n, r + 1)$ of subspaces. In this way we obtain a bound

$$2^n A(n - 1, r) B(n, r + 1).$$

This is

$$2^n \exp((6(n - 1))^{3(n-1)}(r + 1)) \exp((5n)^{3n}(r + 2)) < \exp((6n)^{3n}(r + 1)),$$

and Theorem 1.1 follows.

5   Proof of Theorem 1.2

Let $\{u_m\}$ be a simple linear recurrence sequence of order $n \geq 2$ contained in an algebraically closed field K of characteristic 0. To simplify our exposition, single elements of $\mathbb{Z}$ will also be called arithmetic progressions (indeed they may be viewed as arithmetic progressions with difference 0). Thus we have to show that the set

$$\mathcal{S}(u_m) = \{k \in \mathbb{Z} \mid u_k = 0\}$$

is the union of at most

(5.1) $$W(n) = \exp((6n)^{3n})$$

arithmetic progressions.

We proceed by induction on n. For $n = 2$, our assertion is obvious. Assume $n \geq 3$. Recall that

$$u_m = a_1\, \alpha_1^m + \ldots + a_n\, \alpha_n^m$$

for certain non-zero elements $a_1, \ldots, a_n, \alpha_1, \ldots, \alpha_n \in K$. Hence $\mathcal{S}(u_m)$ is the set of solutions $k \in \mathbb{Z}$ of

(5.2) $$a_1\, \alpha_1^k + \ldots + a_n\, \alpha_n^k = 0.$$

14

First consider those $k \in \mathbb{Z}$ for which no proper subsum of the left-hand side of (5.2) vanishes. For each such k, the vector

$$\left((\alpha_1/\alpha_n)^k, \ldots, (\alpha_{n-1}/\alpha_n)^k \right)$$

is a non-degenerate solution of

$$(5.3) \qquad \left(-\frac{a_1}{a_n} \right) x_1 + \ldots + \left(-\frac{a_{n-1}}{a_n} \right) x_{n-1} = 1 \ \text{ in } \ \boldsymbol{x} = (x_1, \ldots, x_{n-1}) \in \Gamma,$$

where Γ is the group generated by $(\alpha_1/\alpha_n, \ldots, \alpha_{n-1}/\alpha_n)$. Clearly Γ has rank ≤ 1. So by Theorem 1.1, equation (5.3) has at most

$$(5.4) \qquad\qquad\qquad A(n-1, 1) = \exp((6(n-1))^{3(n-1)} 2)$$

non-degenerate solutions. As can be easily verified, for each solution $(x_1, \ldots, x_{n-1})$ of (5.3) the set of $k \in \mathbb{Z}$ with $\left((\alpha_1/\alpha_n)^k, \ldots, (\alpha_{n-1}/\alpha_n)^k \right) = (x_1, \ldots, x_{n-1})$ is an arithmetic progression. Consequently, the set of $k \in \mathbb{Z}$ such that no proper subsum of the left-hand side of (5.2) vanishes, is the union of at most $A(n-1, 1)$ arithmetic progressions.

Let I be a proper, non-empty subset of $\{1, \ldots, n\}$ and consider those solutions $k \in \mathbb{Z}$ of (5.2) for which
$$(5.5) \qquad\qquad\qquad\qquad \sum_{i \in I} a_i \, \alpha_i^k = 0.$$

Each such k also satisfies
$$(5.6) \qquad\qquad\qquad\qquad \sum_{i \notin I} a_i \, \alpha_i^k = 0.$$

Suppose I has cardinality ℓ. Since $a_i \neq 0$ $(i = 1, \ldots, n)$, we get $2 \leq \ell \leq n - 2$. By induction, the set of $k \in \mathbb{Z}$ with (5.5) is the union of at most $W(\ell)$ arithmetic progressions. Also by induction, the set of $k \in \mathbb{Z}$ with (5.6) is the union of at most $W(n - \ell)$ arithmetic progressions. The intersection of two arithmetic progressions is either empty, or again an arithmetic progression. In view of (5.6) and since $\ell \leq n - 2$, $n - \ell \leq n - 2$, the set of $k \in \mathbb{Z}$ with (5.2), (5.5) is the union of at most

$$
\begin{aligned}
W(\ell)W(n - \ell) \ & \leq \ \exp((6\ell)^{3\ell}) \exp((6(n - \ell))^{3(n-\ell)}) \\
& \leq \ \exp((6(n - 1))^{3(n-1)}) \ = \ W(n - 1)
\end{aligned}
$$

arithmetic progressions.

Taking into account all possible subsets I of $\{1, \ldots, n\}$, we infer that the set of solutions $k \in \mathbb{Z}$ of (5.2) for which some subsum of the left-hand side of (5.2) vanishes is contained in the union of at most $2^n W(n - 1)$ arithmetic progressions. Recall from (5.4) that the

15

set of $k \in \mathbb{Z}$ with (5.2) for which no subsum of (5.2) vanishes is the union of at most $A(n-1,1)$ arithmetic progressions. So altogether, by (5.1), (5.4), the set of solutions of (5.2) is the union of at most

$$\exp((6(n-1))^{3(n-1)}2) + 2^n \exp((6(n-1))^{3(n-1)}) \leq \exp((6n)^{3n}) = W(n)$$

arithmetic progressions.

Now suppose that $\{u_m\}$ is non-degenerate. Assume that $\mathcal{S}(u_m)$, that is the set of solutions of (5.2), contains an arithmetic progression $\{a + vt \mid t \in \mathbb{Z}\}$ with $v \neq 0$. Then

$$(5.7) \qquad a_1 \, \alpha_1^a (\alpha_1^v)^t + \ldots + a_n \, \alpha_n^a (\alpha_n^v)^t = 0 \ \text{ for every } \ t \in \mathbb{Z}.$$

Applying (5.7) with $t = 0, \ldots, n-1$, and observing that $a_i \, \alpha_i^a \neq 0$ for $i = 1, \ldots, n$, we infer that the Vandermonde determinant $\det (\alpha_i^{vt})_{i=1,\ldots,n;\, t=0,\ldots,n-1}$ is zero. This is possible only if there are $i \neq j$ with $\alpha_i^v = \alpha_j^v$. But this contradicts the assumption that $\{u_m\}$ is non-degenerate.

We conclude that $\mathcal{S}(u_m)$ does not contain an infinite arithmetic progression. It follows that for non-degenerate $\{u_m\}$ the set $\mathcal{S}(u_m)$ has cardinality $\leq W(n)$. This proves Theorem 1.2.

6 A Reduction

We now turn to the proof of Theorem 2.1. Similarly as in the argument used in Section 3 in the deduction of Theorem 1.1, we claim that in order to prove Theorem 2.1 it will suffice to show that any *finite* set M of points $\boldsymbol{y} \in \overline{\mathbb{Q}}^n$ satisfying (2.6) and (2.10) is contained in the union of not more than

$$(6.1) \qquad \exp((5n)^{3n}(r+1))$$

proper linear subspaces of $\overline{\mathbb{Q}}^n$.

To verify this claim we prove

Lemma 6.1 *Let $n \geq 2$ and $w \geq 1$ be integers. Let K be a field. Let N be a subset of K^n having the following property:*
Any finite subset M of N is contained in the union of not more than w proper linear subspaces of K^n.
Then N itself is contained in the union of not more than w proper linear subspaces of K^n.

Proof By a subspace we shall mean a *proper* linear subspace of K^n.

Given a finite subset M of N, we denote by $a(M)$ the minimum of the quantities

$$\sum_{i=1}^{w} \dim T_i,$$

where $\{T_1, \ldots, T_w\}$ runs through the collection of unordered w-tuples of subspaces with

$$M \subset T_1 \cup \ldots \cup T_w.$$

Let $\mathfrak{S}(M)$ be the collection of all w-tuples of subspaces $\{T_1, \ldots, T_w\}$ with $M \subset T_1 \cup \ldots \cup T_w$ and $\sum_{i=1}^{w} \dim T_i = a(M)$.

Now suppose $\{T_1, \ldots, T_w\} \in \mathfrak{S}(M)$. Then T_i $(i = 1, \ldots, w)$ is generated by a subset of M. Otherwise we could replace T_i by the smaller subspace, generated by $T_i \cap M$, thus making $\sum_{i=1}^{w} \dim T_i$ smaller without affecting $M \subset T_1 \cup \ldots \cup T_w$.

We may conclude that for each of the subspaces T_i there are only finitely many possibilities. Consequently, $\mathfrak{S}(M)$ is finite. Denote its cardinality by $b(M)$.

For any finite subset M of N we have $a(M) \leq (n-1)w$. Hence there is such a subset M for which $a(M)$ attains its maximum a_0, say. We now choose among all finite subsets M of N having $a(M) = a_0$ a set M_0 such that

$$b(M_0) = \min_M \{b(M) \mid a(M) = a_0\}.$$

If M is any finite subset of N with $M \supseteq M_0$ then $\mathfrak{S}(M) = \mathfrak{S}(M_0)$. Indeed suppose $\{T_1, \ldots, T_w\} \in \mathfrak{S}(M)$. So in particular $M_0 \subset T_1 \cup \ldots \cup T_w$. On the other hand $\sum_{i=1}^{w} \dim T_i = a(M) \leq a_0$. The definition of a_0 implies that $a(M) = a_0$ and therefore $\{T_1, \ldots, T_w\} \in \mathfrak{S}(M_0)$, hence $\mathfrak{S}(M) \subset \mathfrak{S}(M_0)$. The inclusion $\mathfrak{S}(M_0) \subset \mathfrak{S}(M)$ follows from the minimality of $b(M_0)$.

Pick $\{T_1, \ldots, T_w\} \in \mathfrak{S}(M_0)$. We claim that

$$N \subset T_1 \cup \ldots \cup T_w.$$

Indeed let $\boldsymbol{y} \in N$ and consider the finite set $M = M_0 \cup \{\boldsymbol{y}\}$. We have shown that $\{T_1, \ldots, T_w\} \in \mathfrak{S}(M)$. So in particular we have

$$\boldsymbol{y} \in T_1 \cup \ldots \cup T_w.$$

This proves our claim and the assertion of the lemma follows.

We now consider a finite set $M = \{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m\}$ of points $\boldsymbol{y}_i \in \overline{\mathbb{Q}}^n$ satisfying (2.6) and (2.10). So we have

$$\boldsymbol{y}_i = \boldsymbol{x}_i * \boldsymbol{z}_i$$

with

$$\boldsymbol{x}_i \in \Gamma, \ \ \boldsymbol{z}_i \in (\overline{\mathbb{Q}}^*)^n, \ \ h(\boldsymbol{z}_i) \leq n^{-1} \exp(-(4n)^{3n})(1 + h(\boldsymbol{x}_i)) \ \ (i = 1, \ldots, m).$$

Let F be a number field such that

$$\boldsymbol{x}_i, \ \boldsymbol{z}_i \in F^n \ \ (i = 1, \ldots, m).$$

Write Γ' for the subgroup of Γ generated by $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$. Then Γ' is a finitely generated subgroup of $(F^*)^n$ of rank $\leq r$. Therefore, in order to prove (6.1) for a finite set M (and therefore also Theorem 2.1) it will suffice to prove

Proposition 6.2 *Suppose $n \geq 2$. Let F be a number field. Let Γ be a finitely generated subgroup of $(F^*)^n$ of rank r. Then the set of points $\boldsymbol{y} = (y_1, \ldots, y_n)$ satisfying*

$$(6.2) \qquad\qquad y_1 + \ldots + y_n = 1,$$

$$(6.3) \qquad \boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z} \ \text{ with } \ \boldsymbol{x} \in \Gamma, \ \boldsymbol{z} \in (F^*)^n, \ h(\boldsymbol{z}) \leq n^{-1} \exp(-(4n)^{3n})(1 + h(\boldsymbol{x}))$$

is contained in the union of not more than

$$(6.4) \qquad\qquad \exp((5n)^{3n}(r+1))$$

proper linear subspaces of F^n.

The remainder of the paper deals with the proof of Proposition 6.2.

7 Heights in Multiplicative Groups

For points $\boldsymbol{x} = (x_1, \ldots, x_n) \in \overline{\mathbb{Q}}^n \setminus \{\boldsymbol{0}\}$ and a number field F such that $x_i \in F$ $(i = 1, \ldots, n)$, we have defined in (2.3) and (2.4) respectively the absolute multiplicative height

$$(7.1) \qquad\qquad H(\boldsymbol{x}) = \prod_{v \in M(F)} \max\{1, \|x_1\|_v, \ldots, \|x_n\|_v\}$$

as well as the absolute logarithmic height $h(\boldsymbol{x}) = \log H(\boldsymbol{x})$. Thus, for $\boldsymbol{x} \in F^n$

$$(7.2) \qquad\qquad h(\boldsymbol{x}) = \sum_{v \in M(F)} \max\{0, \log \|x_1\|_v, \ldots, \log \|x_n\|_v\}.$$

Both, $H(\boldsymbol{x})$ as well as $h(\boldsymbol{x})$, do not depend upon the particular number field F such that $\boldsymbol{x} \in F^n$. In the special case when $n = 1$, (7.2) yields for $x \in \overline{\mathbb{Q}}^*$ and a number field F such that $x \in F$

$$(7.3) \qquad h(x) = \sum_{v \in M(F)} \max\{0, \log \|x\|_v\} = \frac{1}{2} \sum_{v \in M(F)} |\log \|x\|_v|$$

(the last equation is a consequence of the product formula).

Then

$$h\left(\frac{1}{x}\right) = h(x), \quad h(xy) \le h(x) + h(y).$$

For $\boldsymbol{x} = (x_1, \dots, x_n) \in \left(\overline{\mathbb{Q}}^*\right)^n$ we define moreover

$$(7.4) \qquad h_s(\boldsymbol{x}) = \sum_{i=1}^n h(x_i).$$

Using (7.2)–(7.4) we see that

$$(7.5) \qquad h(\boldsymbol{x}) \le h_s(\boldsymbol{x}) \le n \, h(\boldsymbol{x}).$$

Denoting as before by $*$ the product operation in $\left(\overline{\mathbb{Q}}^*\right)^n$, so that $(x_1, \dots, x_n) * (y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$, we have
$$(7.6) \qquad h(\boldsymbol{x} * \boldsymbol{y}) \le h(\boldsymbol{x}) + h(\boldsymbol{y})$$

and similarly for h_s. Further h_s (but not h) is invariant under replacing $\boldsymbol{x}$ by its inverse $\boldsymbol{x}^{-1}$ in $\left(\overline{\mathbb{Q}}^*\right)^n$, so that
$$(7.7) \qquad h_s(\boldsymbol{x}^{-1}) = h_s(\boldsymbol{x}).$$

From now on we fix the number field F. We let $\Gamma \subseteq (F^*)^n$ be a finitely generated group of rank $r > 0$. Let $\boldsymbol{a}_1, \dots, \boldsymbol{a}_r$ be a set of generators of Γ, so that the elements of Γ are of the shape
$$(7.8) \qquad \boldsymbol{x} = \boldsymbol{\xi} * \boldsymbol{a}_1^{u_1} * \dots * \boldsymbol{a}_r^{u_r}$$

where $(u_1, \dots, u_r)$ runs through $\mathbb{Z}^r$, and $\boldsymbol{\xi}$ runs through the torsion group $T(\Gamma) = \Gamma \cap U^n$ of Γ, where U is the group of roots of unity of F. For $\boldsymbol{u} = (u_1 \dots, u_r) \in \mathbb{Z}^r$ set

$$(7.9) \qquad \psi(\boldsymbol{u}) = h_s(\boldsymbol{a}_1^{u_1} * \dots * \boldsymbol{a}_r^{u_r}).$$

For $v \in M(F)$ put
$$\alpha_{ijv} = \log \|a_{ij}\|_v \quad (1 \le i \le r, \ 1 \le j \le n)$$

where $\boldsymbol{a}_i = (a_{i1}, \dots, a_{in})$. Then by the product formula $\sum_{v \in M(F)} \alpha_{ijv} = 0$ ($1 \le i \le r$, $1 \le j \le n$). Let S be the subset of $M(F)$ consisting of those v's such that $\alpha_{ijv} \ne 0$ for

some pair i, j $(1 \le i \le r,\ 1 \le j \le n)$. Then also $\sum_{v \in S} \alpha_{ijv} = 0$ $(1 \le i \le r,\ 1 \le j \le n)$.
For $\boldsymbol{\xi} \in \mathbb{R}^r$ put

$$(7.10) \qquad g_{jv}(\boldsymbol{\xi}) = \sum_{i=1}^{r} \alpha_{ijv}\,\xi_i \quad (1 \le j \le n,\ v \in M(F));$$

then again

$$(7.11) \qquad \sum_{v \in S} g_{jv}(\boldsymbol{\xi}) = 0 \ \ (1 \le j \le n) \ \text{ and } \ g_{jv}(\boldsymbol{\xi}) = 0 \ \text{ for } \ v \notin S \ \ (1 \le j \le n).$$

Since by (7.8)

$$(7.12) \qquad \log \|x_j\|_v = \log \|a_{1j}^{u_1} \ldots a_{rj}^{u_r}\|_v = \sum_{i=1}^{r} \alpha_{ijv}\,u_i = g_{jv}(\boldsymbol{u}),$$

we have from (7.3), (7.9)

$$\psi(\boldsymbol{u}) \;=\; \sum_{j=1}^{n} h(a_{1j}^{u_1} \ldots a_{rj}^{u_r}) \;=\; \frac{1}{2} \sum_{j=1}^{n} \sum_{v \in M(F)} |g_{jv}(\boldsymbol{u})|$$

$$=\; \frac{1}{2} \sum_{j=1}^{n} \sum_{v \in S} |g_{jv}(\boldsymbol{u})|.$$

More generally, for $\boldsymbol{\xi} \in \mathbb{R}^r$ set

$$(7.13) \qquad \psi(\boldsymbol{\xi}) \;=\; \frac{1}{2} \sum_{v \in M(F)} \sum_{j=1}^{n} |g_{jv}(\boldsymbol{\xi})|.$$

Then

    (a) $\psi(\boldsymbol{\xi}) \ge 0$ for $\boldsymbol{\xi} \in \mathbb{R}^r$,

    (b) $\psi(\alpha\,\boldsymbol{\xi}) = |\alpha|\,\psi(\boldsymbol{\xi})$ for $\boldsymbol{\xi} \in \mathbb{R}^r,\ \alpha \in \mathbb{R}$,

    (c) $\psi(\boldsymbol{\xi} + \boldsymbol{\eta}) \le \psi(\boldsymbol{\xi}) + \psi(\boldsymbol{\eta})$ for $\boldsymbol{\xi}, \boldsymbol{\eta} \in \mathbb{R}^r$.

Since $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ are multiplicatively independent, the components of $\boldsymbol{a}_1^{u_1} * \ldots * \boldsymbol{a}_r^{u_r}$ will all be roots of unity only if $\boldsymbol{u} = \boldsymbol{0}$. Therefore according to Dobrowolski [6], for $\boldsymbol{u} \in \mathbb{Z}^r \setminus \{\boldsymbol{0}\}$ we have

$$\psi(\boldsymbol{u}) > \frac{c_1}{d}\,(\log\log 3d \,/\, \log 3d)^3$$

where $d = [F : \mathbb{Q}]$ and where $c_1 > 0$ is an absolute constant. In particular, there is a constant $c > 0$ such that

    (d) $\psi(\boldsymbol{u}) \ge c > 0$ for $\boldsymbol{u} \in \mathbb{Z}^r \setminus \{\boldsymbol{0}\}$.

In [25], Lemma 3 it is shown that since the function ψ satisfies (a)–(d), the set $\Psi \subset \mathbb{R}^r$ given by

$$(7.14) \qquad\qquad \Psi = \{\boldsymbol{\xi} \in \mathbb{R}^r \mid \psi(\boldsymbol{\xi}) \leq 1\}$$

is a *symmetric, convex body.*

8   Special Points

Let F, Γ, $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ be as in Section 7. When $\boldsymbol{x} \in \Gamma$, set

$$(8.1) \qquad\qquad h = h(\boldsymbol{x}), \quad H = H(\boldsymbol{x}) = e^h, \quad h_s = h_s(\boldsymbol{x}).$$

Express $\boldsymbol{x}$ as in (7.8). So, if $\boldsymbol{x} \in \Gamma$ and $\boldsymbol{u} \in \mathbb{Z}^r$ are related by (7.8), we have (7.9), i.e.,

$$(8.2) \qquad\qquad h_s = h_s(\boldsymbol{x}) = \psi(\boldsymbol{u}).$$

Let $\Psi = \{\boldsymbol{\xi} \in \mathbb{R}^r \mid \psi(\boldsymbol{\xi}) \leq 1\}$ be the set (7.14). Put

$$(8.3) \qquad\qquad q = 4n.$$

Given $\boldsymbol{\rho} \in \mathbb{R}^r$, an element $\boldsymbol{x} \in \Gamma$ will be called $\boldsymbol{\rho}$-special if $h > 0$ (in (8.1)) and if

$$(8.4) \qquad\qquad \boldsymbol{u} \in \frac{h}{q}\,\Psi + h\,\boldsymbol{\rho}.$$

The right hand side of (8.4) signifies $\dfrac{h}{q}\,\Psi$ translated by $h\,\boldsymbol{\rho}$.

We quote Lemma 8.1 of [23].

Lemma 8.1 *Let Φ be a symmetric convex body in $\mathbb{R}^r$. Suppose $\lambda > 0$. Then $\lambda\,\Phi$ can be covered by not more than*
$$(8.5) \qquad\qquad (2\lambda + 4)^r$$
translates of Φ.

We apply Lemma 8.1 with Φ replaced by $\dfrac{1}{q}\,\Psi$ and with $\lambda\,\Phi$ replaced by $n\,\Psi$. We may conclude that $n\,\Psi$ may be covered by

$$\leq (2qn + 4)^r = Z$$

translates of $\dfrac{1}{q}\,\Psi$, say by $\dfrac{1}{q}\,\Psi + \boldsymbol{\rho}_i$ $(i = 1, \ldots, Z)$.

Now when $\boldsymbol{x}$ satisfies (8.1), then by (7.5), (7.9), (8.2) the point $\boldsymbol{u} \in \mathbb{Z}^r$ related to $\boldsymbol{x}$ via (7.8) lies in

$$h_s \, \Psi \subset h \, n \, \Psi.$$

Thus $\boldsymbol{x}$ is special for at least one of $\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_Z$. We have shown

Corollary 8.2 *There exist elements* $\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_Z \in \mathbb{R}^r$ *with*

$$(8.6) \qquad\qquad\qquad Z = (2qn + 4)^r$$

such that any $\boldsymbol{x} \in \Gamma$ *is special for at least one of* $\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_Z$.

We remark moreover that our construction implies that we may take $\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_Z$ with

$$(8.7) \qquad\qquad\qquad \boldsymbol{\rho}_i \in \left(n + \frac{1}{q} \right) \Psi \quad (i = 1, \ldots, Z).$$

In the sequel, we will apply the material developed so far to the solutions $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z}$ of (6.2), (6.3).

9 Properties of Large Special Solutions

We now study solutions $\boldsymbol{y}$ of (6.2), (6.3).

A solution $\boldsymbol{y}$ *will be called* large *if it has a representation* $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z}$ *as in (6.3) such that*

$$(9.1) \qquad\qquad\qquad h(\boldsymbol{x}) > 4n \log n.$$

Solutions $\boldsymbol{y}$ *of (6.2), (6.3) that are not large will be called* small.

If the group Γ has rank 0, then all elements $\boldsymbol{x} \in \Gamma$ have $h(\boldsymbol{x}) = 0$. So, large solutions do only exist when rank $\Gamma > 0$.

A solution $\boldsymbol{y}$ *of (6.2), (6.3) is called* $\boldsymbol{\rho}$-*special if, with* $\boldsymbol{x}, \boldsymbol{z}$ *as in (6.3), the point* $\boldsymbol{x}$ *is* $\boldsymbol{\rho}$-*special.*

In this section we derive properties of large $\boldsymbol{\rho}$-special solutions $\boldsymbol{y}$. This will allow us in Section 10 to deduce an upper bound for the number of subspaces needed to cover the set of large solutions of (6.2), (6.3).

Suppose that $\boldsymbol{\rho} \in \left(n + \frac{1}{q} \right) \Psi$ is fixed. Set

$$(9.2) \qquad\qquad m_{jv} = \begin{cases} g_{jv}(\boldsymbol{\rho}) & (v \in M(F), \ 1 \le j \le n) \\ 0 & (v \in M(F), \ j = 0). \end{cases}$$

In view of (7.11) we have

(9.3) $$\sum_{v \in S} m_{jv} = 0 \quad (j = 0, \ldots, n), \quad m_{jv} = 0 \text{ for } v \notin S, \ j = 0, \ldots, n.$$

Further, since $\boldsymbol{\rho} \in \left(n + \dfrac{1}{q}\right)\Psi$, by (9.2), (7.13) and the definition of Ψ in (7.14)

(9.4) $$\sum_{v \in M(F)} \sum_{j=0}^{n} |m_{jv}| = 2\psi(\boldsymbol{\rho}) \leq 2\left(n + \frac{1}{q}\right).$$

Now let $\boldsymbol{x} \in \Gamma$ be $\boldsymbol{\rho}$-special, so that with $\boldsymbol{u}$ as in (7.8) we have (8.4) with $h = h(\boldsymbol{x})$. Then for any $v \in M(F)$ and for $j = 1, \ldots, n$

(9.5) $$g_{jv}(\boldsymbol{u}) = h(g_{jv}(\boldsymbol{\rho}) + q^{-1}\, g_{jv}(\boldsymbol{\xi})) = h\, m_{jv} + \frac{h}{q}\, g_{jv}(\boldsymbol{\xi})$$

with some $\boldsymbol{\xi} \in \Psi$. Writing $g_{0v}(\boldsymbol{\xi}) = 0$ for $v \in M(F)$ and for $\boldsymbol{\xi} \in \mathbb{R}^r$, (9.5) will be true for $j = 0$ as well.

It follows from (9.2), (9.5) that

(9.6) $$\sum_{v \in M(F)} \sum_{j=0}^{n} |g_{jv}(\boldsymbol{u}) - h\, m_{jv}| = \frac{h}{q} \sum_{v \in M(F)} \sum_{j=0}^{n} |g_{jv}(\boldsymbol{\xi})| \leq \frac{h}{q}.$$

For $v \in M(F)$ let $L_0^{(v)}, \ldots, L_n^{(v)}$ be the linear forms in $\boldsymbol{Y} = (Y_1, \ldots, Y_n)$ given by

(9.7)
$$
\begin{aligned}
L_0^{(v)}(\boldsymbol{Y}) &= Y_1 + \ldots + Y_n \\
L_1^{(v)}(\boldsymbol{Y}) &= Y_1 \\
&\vdots \\
L_n^{(v)}(\boldsymbol{Y}) &= Y_n.
\end{aligned}
$$

Lemma 9.1 *Let $\boldsymbol{\rho}$ be as above. There are n-element subsets $\mathcal{I}(v)$ of $\{0, \ldots, n\}$ defined for $v \in M(F)$ and there are numbers ℓ_{jv} ($v \in M(F)$, $j \in \mathcal{I}(v)$) with the following properties.*

(9.8) $$\mathcal{I}(v) = \{1, \ldots, n\} \quad \text{for} \quad v \notin S,$$

(9.9) $$\ell_{jv} = 0 \quad \text{for} \quad v \notin S, \ j \in \mathcal{I}(v),$$

(9.10) $$\sum_{v \in M(F)} \sum_{j \in \mathcal{I}(v)} \ell_{jv} = 0, \qquad \sum_{v \in M(F)} \sum_{j \in \mathcal{I}(v)} |\ell_{jv}| \leq 1.$$

Moreover, any large $\boldsymbol{\rho}$-special solution $\boldsymbol{y}$ of (6.2), (6.3) satisfies the inequality

(9.11) $$\prod_{v \in M(F)} \max_{j \in \mathcal{I}(v)} \left\{ \frac{\|L_j^{(v)}(\boldsymbol{y})\|_v}{Q^{\ell_{jv}}} \right\} \leq Q^{-\frac{1}{2n(4n+1)}},$$

where $Q = H(\boldsymbol{x})^{4n+1}$. Here $\boldsymbol{x} \in \Gamma$ is a point in the representation $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z}$ according to (6.3).

Proof For $v \in S$ let $j(v) \in \{0, \dots, n\}$ be a subscript with

$$(9.12) \qquad m_{j(v),v} = \max\{m_{0v}, \dots, m_{nv}\}.$$

We define $\mathcal{I}(v) = \{0, \dots, n\} \setminus \{j(v)\}$ $(v \in S)$. For $v \notin S$, $\mathcal{I}(v)$ is already defined in (9.8). By our definition of S in Section 7, any solution $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z}$ as in (6.3) has by (7.11), (7.12)

$$(9.13) \qquad \begin{aligned} h &= h(\boldsymbol{x}) = \sum_{v \in S} \max\{0, \log\|x_1\|_v, \dots, \log\|x_n\|_v\} \\ &= \sum_{v \in S} \max\{g_{0v}(\boldsymbol{u}), g_{1v}(\boldsymbol{u}), \dots, g_{nv}(\boldsymbol{u})\}. \end{aligned}$$

Given $\boldsymbol{x}$, pick for each $v \in S$ an element $i(v) \in \{0, \dots, n\}$ with $g_{i(v),v}(\boldsymbol{u}) = \max\{g_{0v}(\boldsymbol{u}), \dots, g_{nv}(\boldsymbol{u})\}$. Then by (9.13)

$$\sum_{v \in S} g_{i(v),v}(\boldsymbol{u}) = h.$$

Thus in view of (9.6), we may infer that

$$h \sum_{v \in S} m_{i(v),v} \geq \sum_{v \in S} g_{i(v),v}(\boldsymbol{u}) - \frac{h}{q} = h\left(1 - \frac{1}{q}\right).$$

In particular, by (9.12) we obtain

$$(9.14) \qquad \sum_{v \in S} m_{j(v),v} \geq 1 - \frac{1}{q}.$$

Let s be the cardinality of S and write

$$(9.15) \qquad \gamma = \frac{1}{ns} \sum_{v \in S} m_{j(v),v}.$$

We now define numbers c_{jv} $(v \in M(F), \ j \in \mathcal{I}(v))$ by

$$(9.16) \qquad c_{jv} = \begin{cases} m_{jv} + \gamma & \text{for} \quad v \in S, \ j \in \mathcal{I}(v) \\ 0 & \text{for} \quad v \notin S, \ j \in \mathcal{I}(v). \end{cases}$$

We infer from (9.3), (9.4), (9.15) that

$$(9.17) \qquad \sum_{v \in M(F)} \sum_{j \in \mathcal{I}(v)} c_{jv} = 0, \qquad \sum_{v \in M(F)} \sum_{j \in \mathcal{I}(v)} |c_{jv}| \leq 4\left(n + \frac{1}{q}\right).$$

So far we have only used the fact that our solution $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z}$ of (6.2), (6.3) is $\boldsymbol{\rho}$-special.

24

However, $\boldsymbol{y}$ is also supposed to be large. Under this additional hypothesis we now derive an upper bound for the quantity

$$A = \prod_{v \in M(F)} \max_{j \in \mathcal{I}(v)} \left\{ \frac{\|L_j^{(v)}(\boldsymbol{y})\|_v}{H^{c_{jv}}} \right\},$$

where $H = H(\boldsymbol{x})$.

Write $\boldsymbol{y} = (y_1, \ldots, y_n)$, $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{z} = (z_1, \ldots, z_n)$. Put $y_0 = x_0 = z_0 = 1$. Notice that by (6.2) and (9.7) we then have for each $v \in M(F)$

$$L_j^{(v)}(\boldsymbol{y}) = y_j \quad \text{for} \quad j = 0, \ldots, n.$$

Hence by (9.14), (9.15), (9.16)

$$
\begin{aligned}
A &= \prod_{v \in M(F)} \max_{j \in \mathcal{I}(v)} \left\{ \frac{\|y_j\|_v}{H^{c_{jv}}} \right\} \\
&= H^{-\frac{1}{n} \sum_{v \in S} m_{j(v),v}} \prod_{v \in M(F)} \max_{j \in \mathcal{I}(v)} \left\{ \frac{\|y_j\|_v}{H^{m_{jv}}} \right\} \\
(9.18) \qquad &\leq H^{-\frac{1}{n} + \frac{1}{nq}} \prod_{v \in M(F)} \max_{j \in \mathcal{I}(v)} \left\{ \frac{\|y_j\|_v}{H^{m_{jv}}} \right\} \\
&\leq H^{-\frac{1}{n} + \frac{1}{nq}} \left(\prod_{v \in M(F)} \max_{0 \leq j \leq n} \|z_j\|_v \right) \left(\prod_{v \in M(F)} \max_{0 \leq j \leq n} \left\{ \frac{\|x_j\|_v}{H^{m_{jv}}} \right\} \right) \\
&= H^{-\frac{1}{n} + \frac{1}{nq}} H(\boldsymbol{z}) \prod_{v \in M(F)} \max_{0 \leq j \leq n} \left\{ \frac{\|x_j\|_v}{H^{m_{jv}}} \right\}.
\end{aligned}
$$

(6.3) and (9.1) entail

$$
\begin{aligned}
(9.19) \qquad H(\boldsymbol{z}) &\leq \exp\left(n^{-1} \exp(-(4n)^{3n})(1 + h(\boldsymbol{x})) \right) \\
&\leq \exp\left(n^{-1} \exp(-(4n)^{3n})((4n \log n)^{-1} + 1)h(\boldsymbol{x}) \right) \leq H^{1/(8n)}.
\end{aligned}
$$

On the other hand by (7.12) and (9.2), (9.5), (9.6)

$$(9.20) \qquad \prod_{v \in M(F)} \max_{0 \leq j \leq n} \left\{ \frac{\|x_j\|_v}{H^{m_{jv}}} \right\} \leq H^{1/q}.$$

Combination of (9.18)–(9.20) yields with our value q from (8.3)

$$(9.21) \qquad \prod_{v \in M(F)} \max_{j \in \mathcal{I}(v)} \left\{ \frac{\|L_j^{(v)}(\boldsymbol{y})\|_v}{H^{c_{jv}}} \right\} \leq H^{-\frac{1}{n} + \frac{1}{nq} + \frac{1}{8n} + \frac{1}{q}} \leq H^{-\frac{1}{2n}}.$$

We now renormalize with our parameter $Q = H(\boldsymbol{x})^{4n+1} = H^{4n+1}$. Writing

$$\ell_{jv} = \frac{c_{jv}}{4n+1} \qquad (v \in M(F), \ j \in \mathcal{I}(v))$$

we obtain with (9.16), (9.17) and with q as in (8.3) assertions (9.9) and (9.10). Moreover, (9.21) gives (9.11).

10   Large Solutions

To deal with the large solutions, we use the absolute version of the Subspace Theorem, due to Evertse and Schlickewei [12]. The following Proposition 10.1 is a very special case of Theorem 2.1 of [12].

For $v \in M(F)$ let the linear forms $L_0^{(v)}(\boldsymbol{Y}), \ldots, L_n^{(v)}(\boldsymbol{Y})$ be as in (9.7). Moreover, let $\mathcal{I}(v)$ and the tuple (ℓ_{jv}) $(v \in M(F), j \in \mathcal{I}(v))$ be as in Lemma 9.1.

Proposition 10.1 *Suppose $0 < \delta < 1$. There are proper linear subspaces $T_1, \ldots, T_t$ of F^n with*

(10.1)
$$t \leq 2^{2(n+9)^2} \delta^{-n-4}$$

with the following property:
As Q runs through the values satisfying

(10.2)
$$Q > n^{2/\delta},$$

the set of solutions $\boldsymbol{y} \in F^n$ of the inequalities

(10.3)
$$\prod_{v \in M(F)} \max_{j \in \mathcal{I}(v)} \left\{ \frac{\|L_j^{(v)}(\boldsymbol{y})\|_v}{Q^{\ell_{jv}}} \right\} \leq Q^{-\delta}$$

is contained in the union

$$T_1 \cup \ldots \cup T_t.$$

We apply Proposition 10.1 with $Q = H(\boldsymbol{x})^{4n+1}$ (where $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z}$ with $\boldsymbol{x} \in \Gamma$ according to (6.3)), and with $\delta = \dfrac{1}{2n(4n+1)}$. By Lemma 9.1, given $\boldsymbol{\rho}$, any large $\boldsymbol{\rho}$-special solution $\boldsymbol{y}$ of (6.2), (6.3) satisfies (10.3) with sets $\mathcal{I}(v)$ and a tuple (ℓ_{jv}) $(v \in M(F), j \in \mathcal{I}(v))$ which depend only on $\boldsymbol{\rho}$.

With our values of Q and δ, (10.2) becomes $H(\boldsymbol{x})^{4n+1} > n^{4n(4n+1)}$, or equivalently

$$h(\boldsymbol{x}) > 4n \log n.$$

In view of (9.1) this means that Propositon 10.1 is adequate to deal with the large $\boldsymbol{\rho}$-special solutions $\boldsymbol{y}$ of (6.2), (6.3).

By (10.1), a single $\boldsymbol{\rho}$ gives rise to

$$\leq 2^{2(n+9)^2}(8n^2 + 2n)^{n+4}$$

subspaces. Using Corollary 8.2 and the definition of q in (8.3) we obtain

Corollary 10.2 *The set of large solutions $\boldsymbol{y}$ of* (6.2), (6.3) *is contained in the union of not more than*

$$2^{2(n+9)^2}(8n^2 + 2n)^{n+4+r}$$

proper linear subspaces of F^n.

11 Small Solutions

We still have to deal with the small solutions $\boldsymbol{y}$ of (6.2), (6.3).

For this purpose we use results on the number of points on varieties which have small height. The first *explicit* estimate in that context is due to W. Schmidt [26]. We quote here a special case of Theorem 4 of [26].

Proposition 11.1 *Let $\boldsymbol{b} = (b_1, \ldots, b_n) \in \left(\overline{\mathbb{Q}}^*\right)^n$. Put*

$$(11.1) \qquad\qquad q_0(n) = \exp((4n)^{3n}).$$

Then the equation

$$(11.2) \qquad\qquad b_1 w_1 + \ldots + b_n w_n = 1$$

has at most $q_0(n)$ non-degenerate solutions $\boldsymbol{w} = (w_1, \ldots, w_n) \in \left(\overline{\mathbb{Q}}^*\right)^n$ with

$$(11.3) \qquad\qquad h_s(\boldsymbol{w}) < q_0(n)^{-1}.$$

We remark that S. David and P. Philippon [4], [5] recently have proved a sharpening of Proposition 11.1. They have shown that with

$$q_1(n) = 2^{2^{c_1 n}},$$

where c_1 is an explicit absolute constant, equation (11.2) has at most $q_1(n)$ non-degenerate solutions $\boldsymbol{w}$ with

$$h_s(\boldsymbol{w}) < q_1(n)^{-3/4}.$$

Here, we will give details on the basis of Proposition 11.1.

W. Schmidt, in Theorem 5 of [26], also has derived an upper bound for the number of non-degenerate solutions $\boldsymbol{w}$ of (11.2) when $\boldsymbol{w}$ lies in a group $\Gamma \subset (\overline{\mathbb{Q}}^*)^n$ of rank r and has

$$(11.4) \qquad\qquad h_s(\boldsymbol{w}) \leq C.$$

In our context we ask for the number of points $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z}$ satisfying (6.2), (6.3). But our $\boldsymbol{y}$ only "essentially" belongs to Γ (in the sense defined by (6.3)). Moreover, instead of (11.4), which in our context would be $h_s(\boldsymbol{y}) \leq C$, we only have a weaker hypothesis of type

$$(11.5) \qquad\qquad h_s(\boldsymbol{x}) \leq C.$$

To derive a bound in this more general setting, we follow the argument given in [26].

By (6.3), $\boldsymbol{y} = \boldsymbol{x} * \boldsymbol{z}$ with

$$(11.6) \qquad\qquad \boldsymbol{x} \in \Gamma \quad \text{and} \quad h(\boldsymbol{z}) \leq n^{-1}\exp(-(4n)^{3n})(1 + h(\boldsymbol{x})).$$

Suppose first that $\operatorname{rank}\Gamma = 0$.
Then $h(\boldsymbol{x}) = 0$. Therefore, by (7.5), (7.6),

$$
\begin{aligned}
(11.7) \quad h_s(\boldsymbol{y}) \;&\leq\; h_s(\boldsymbol{x}) + h_s(\boldsymbol{z}) \;=\; h_s(\boldsymbol{z}) \\
&\leq\; n\, n^{-1}\exp(-(4n)^{3n})(1 + h(\boldsymbol{x})) \;=\; \exp(-(4n)^{3n}) \;=\; q_0(n)^{-1}.
\end{aligned}
$$

We apply Proposition 11.1 with $\boldsymbol{b} = (1, \ldots, 1)$ and conclude that (6.2) does not have more than

$$(11.8) \qquad\qquad q_0(n)$$

non-degenerate solutions $\boldsymbol{y}$ satisfying (11.7). We point out that our choice of the function $n^{-1}\exp(-(4n)^{3n})$ in (6.3) is motivated uniquely to guarantee (11.7).

We now treat the case when $r = \operatorname{rank}\Gamma > 0$.
Hypothesis (11.5), in view of (7.5) and (9.1), now reads as

$$(11.9) \qquad\qquad h_s(\boldsymbol{x}) \leq 4n^2 \log n.$$

Let $\boldsymbol{u} \in \mathbb{Z}^r$ be the point related to $\boldsymbol{x} \in \Gamma$ by (7.8). Combination of (7.9) and (11.9) gives

$$(11.10) \qquad\qquad \psi(\boldsymbol{u}) \leq 4n^2 \log n.$$

We quote Lemma 4 of [25].

Lemma 11.2 *Let* $\psi : \mathbb{R}^r \to \mathbb{R}$ *be a function satisfying* (a)–(d) *in Section* 7. *Let* U *be a set of points in* $\mathbb{R}^r$ *such that*

$$(11.11) \qquad\qquad \psi(\boldsymbol{u} - \boldsymbol{v}) \geq \delta_0 > 0$$

for $\boldsymbol{u} \neq \boldsymbol{v}$ in U. Then the number of $\boldsymbol{u} \in U$ with

$$\text{(11.12)} \qquad\qquad\qquad \psi(\boldsymbol{u}) \leq C$$

is

$$\text{(11.13)} \qquad\qquad\qquad \leq ((2C/\delta_0) + 1)^r.$$

Let V be the subset of points $\boldsymbol{u} \in \mathbb{Z}^r$ satisfying (11.10). We apply Lemma 11.2 with U being a maximal subset of V such that

$$\text{(11.14)} \qquad\qquad \psi(\boldsymbol{u} - \boldsymbol{v}) \geq \frac{1}{2} q_0(n)^{-1} \quad \text{for} \quad \boldsymbol{u} \neq \boldsymbol{v} \quad \text{in} \quad U.$$

Here $q_0(n)$ is as in Proposition 11.1. So we take $C = 4n^2 \log n$ and $\delta_0 = \frac{1}{2} q_0(n)^{-1}$. By (11.13) and (11.1) we may infer that U has cardinality

$$\text{(11.15)} \qquad\qquad |U| \leq (16n^2(\log n)q_0(n) + 1)^r \leq (16n^3 q_0(n))^r.$$

Moreover by the definition of U, for any $\boldsymbol{u} \in \mathbb{Z}^r$ satisfying (11.10), there exists $\boldsymbol{u}_0 \in U$ such that

$$\text{(11.16)} \qquad\qquad \psi(\boldsymbol{u} - \boldsymbol{u}_0) < \frac{1}{2} q_0(n)^{-1}.$$

Again using (7.8), (7.9) we may infer that there is a subset Δ of Γ with cardinality

$$\text{(11.17)} \qquad\qquad |\Delta| \leq (16n^3 q_0(n))^r$$

such that for any $\boldsymbol{x} \in \Gamma$ with (11.9) there is an element $\boldsymbol{b} \in \Delta$ having

$$\text{(11.18)} \qquad\qquad h_s(\boldsymbol{x} * \boldsymbol{b}^{-1}) < \frac{1}{2} q_0(n)^{-1}.$$

Now let $\boldsymbol{y}$ be a small solution of (6.2), (6.3), i.e., a solution with $h(\boldsymbol{x}) \leq 4n \log n$.

We choose $\boldsymbol{b} \in \Delta$ satisfying (11.18). Combination of (6.3), (7.5), (7.6), (11.1), (11.18) yields

$$\text{(11.19)} \quad
\begin{aligned}
h_s(\boldsymbol{y} * \boldsymbol{b}^{-1}) \ &\leq \ h_s(\boldsymbol{z}) + h_s(\boldsymbol{x} * \boldsymbol{b}^{-1}) \ \leq \ n\, h(\boldsymbol{z}) + h_s(\boldsymbol{x} * \boldsymbol{b}^{-1}) \\
&\leq \ n \exp(-(5n)^{3n})(1 + 4n \log n) + \frac{1}{2} q_0(n)^{-1} \ < \ q_0(n)^{-1}.
\end{aligned}$$

We conclude that for any small non-degenerate solution $\boldsymbol{y}$ of (6.2), (6.3) there exists $\boldsymbol{b} \in \Delta$ with (11.19).

Write $\boldsymbol{w} = \boldsymbol{y} * \boldsymbol{b}^{-1}$. Then $\boldsymbol{w}$ is a solution of (11.2), (11.3). By Proposition 11.1, given $\boldsymbol{b}$, there are at most $q_0(n)$ points $\boldsymbol{w}$ with (11.2), (11.3). We may conclude that each $\boldsymbol{b} \in \Delta$ gives rise to at most $q_0(n)$ non-degenerate small solutions $\boldsymbol{y}$ of (6.2).

29

Introducing the factor $(16n^3 q_0(n))^r$ from (11.17) for the number of possible choices of $\boldsymbol{b}$, we see that altogether we cannot have more than

(11.20)
$$q_0(n)(16n^3 q_0(n))^r$$

non-degenerate small solutions.

Comparing (11.20) with (11.8) we observe that indeed the bound (11.20) is true for any value of $r = \operatorname{rank} \Gamma$.

All other *small* solutions are degenerate, i.e., some subsum on the left hand side of (6.2) vanishes. The number of subsums is $\leq 2^n$. Hence the degenerate solutions may be covered by the union of $\leq 2^n$ proper linear subspaces.

To summarize, we have proved

Corollary 11.3 *The set of small solutions of* (6.2), (6.3) *is contained in the union of not more than*
$$2^n + q_0(n)\left(16n^3 q_0(n)\right)^r$$
proper linear subspaces of F^n. *Here* $q_0(n)$ *is given by* (11.1), *i.e.,* $q_0(n) = \exp((4n)^{3n})$.

12   Proof of Proposition 6.2

We collect the results of Sections 10 and 11. From Corollary 10.2 we get
$$\leq 2^{2(n+9)^2}(8n^2 + 2n)^{n+4+r}$$

subspaces for the large solutions. From Corollary 11.2 we obtain
$$\leq 2^n + (16n^3)^r \left(\exp((4n)^{3n})\right)^{r+1}$$

subspaces for the small solutions.

Therefore, to cover the set of all solutions $\boldsymbol{y}$ of (6.2), (6.3)
$$2^{2(n+9)^2}(8n^2 + 2n)^{n+4+r} + 2^n + (16n^3)^r \left(\exp((4n)^{3n})\right)^{r+1} < \exp((5n)^{3n}(r + 1))$$

subspaces will suffice. This completes the proof of Proposition 6.2.

References

[1] E. Bavencoffe and J.-P. Bézivin. Une famille remarquable de suites récurrentes linéaires. Monatsh. Math **120** (1995), 189-203.

[2] F. Beukers and H.P. Schlickewei. The equation $x + y = 1$ in finitely generated groups. Acta Arith. **78** (1996), 189-199.

[3] E. Bombieri and U. Zannier. Algebraic Points on Subvarieties of $\boldsymbol{G}_m^n$. Intern. Math. Research Notices **7** (1995), 333-347.

[4] S. David and P. Philippon. Minorations des hauteurs normalisées des sous-variétés des tores. Ann. Scuola Norm. Sup. Pisa, Cl. Sci. (4), **28** (1999), 489-543.

[5] S. David and P. Philippon. Errata à: Minorations des hauteurs normalisées des sous-variétés des tores. Ann. Scuola Norm. Sup. Pisa, Cl. Sci. (4), **29** (2000), 729-731.

[6] E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. Acta Arith. **34** (1979), 391-401.

[7] P. Erdős, C.L. Stewart and R. Tijdeman. Some diophantine equations with many solutions. Compos. Math. **66** (1988), 37-56.

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

[9] J.-H. Evertse. On sums of S-units and linear recurrences. Compos. Math. **53** (1984), 225-244.

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

[11] J.-H. Evertse. The number of solutions of linear equations in roots of unity. Acta Arith. **89** (1999), 45-51.

[12] J.-H. Evertse and H.P. Schlickewei. A quantitative version of the absolute Subspace Theorem. J. reine angew. Math. (To appear).

[13] S. Lang. Integral points on curves. Publ. Math. I.H.E.S. **6** (1960), 27-43.

[14] K. Mahler. Zur Approximation algebraischer Zahlen I: Über den größten Primteiler binärer Formen. Math. Ann. **107** (1933), 691-730.

[15] A.J. van der Poorten and H.P. Schlickewei. The growth condition for recurrence sequences. Macquarie Univ. Math. Rep. 82-0041, North Ryde, Australia (1982).

[16] D. Roy and J.L. Thunder. An absolute Siegel's Lemma. J. reine angew. Math. **476** (1996), 1-26.

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

[18] H.P. Schlickewei. Multiplicities of recurrence sequences. Acta Math. **176** (1996), 171-243.

[19] H.P. Schlickewei. Linear equations over finitely generated groups. Preprint (1994).

[20] H.P. Schlickewei. Equations in roots of unity. Acta Arith. **76** (1996), 99-108.

[21] H.P. Schlickewei. Equations $ax + by = 1$. Preprint (1994).

[22] H.P. Schlickewei. The multiplicity of binary recurrences. Invent. Math. **129** (1997), 11-36.

[23] H.P. Schlickewei and W.M. Schmidt. The number of solutions of polynomial-exponential equations. Compos. Math. **120** (2000), 193-225.

[24] H.P. Schlickewei and W.M. Schmidt. Linear equations with variables which lie in a multiplicative group. Preprint (1994).

[25] W.M. Schmidt. Heights of Algebraic Points Lying on Curves or Hypersurfaces. Proc. A.M.S. **124** (1996), 3003-3013.

[26] W.M. Schmidt. Heights of points on subvarieties of $\boldsymbol{G}_m^n$. In: Sém. de théorie de nombres de Paris, 1993-1994 (ed. S. David), 157-187. Cambridge Univ. Press, 1996.

[27] W.M. Schmidt. The zero multiplicity of linear recurrences. Acta Math. **182** (1999), 243-282.

[28] W.M. Schmidt. Zeros of linear recurrences. Publ. Math. Debrecen **56** (2000), 609-630.

[29] S. Zhang. Positive line bundles on arithmetic varieties. Journal A.M.S. **8** (1995), 187-221.

J.-H. Evertse
Dept. of Mathematics and Computer Science
Rijksuniversiteit te Leiden
Niels Bohrweg 1
P.O. Box 9512
2300 RA Leiden
The Netherlands
e-mail: evertse@math.leidenuniv.nl

H.P. Schlickewei
Fachbereich Mathematik
Universität Marburg
Lahnberge
35032 Marburg
Germany
e-mail: hps@mathematik.uni-marburg.de

W.M. Schmidt
Dept. of Mathematics
University of Colorado
Boulder, CO 80309-0395
U.S.A.
e-mail: schmidt@euclid.colorado.edu