The Subspace Theorem and Applications

Hans Peter Schlickewei

Abstract. We discuss recent results on simultaneous approximation of algebraic numbers by rationals and applications to diophantine equations.

1991 Mathematics Subject Classification: 11J68,11D61
Keywords and Phrases: Subspace Theorem, Unit Equations, Recurrence Sequences

In 1955 K. F. Roth [15] proved: *Suppose α is an algebraic number and suppose $\varepsilon > 0$. Then the inequality*

$$\left|\alpha - \frac{x}{y}\right| < y^{-2-\varepsilon} \tag{0.1}$$

has only finitely many rational solutions $\frac{x}{y}$. This result is best possible since by Dirichlet's classical theorem any real irrational number α has infinitely many rational approximations satisfying

$$\left|\alpha - \frac{x}{y}\right| < y^{-2}.$$

In 1972 W. M. Schmidt [22] generalized Roth's Theorem to n dimensions. He proved the following:

Subspace Theorem. *Let $L_i = \alpha_{i1}X_1 + \cdots + \alpha_{in}X_n$ $(i = 1, \dots, n)$ be linearly independent linear forms with algebraic coefficients. Suppose $\varepsilon > 0$. Consider the inequality*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \| \mathbf{x} \|^{-\varepsilon}, \quad \mathbf{x} \in \mathbb{Z}^n, \tag{0.2}$$

where $\| \mathbf{x} \| = (x_1^2 + \cdots + x_n^2)^{\frac{1}{2}}$.
Then there exist proper linear subspaces $T_1, \dots, T_t$ of $\mathbb{Q}^n$ such that the set of solutions of (0.2) is contained in the union

$$T_1 \cup \cdots \cup T_t. \tag{0.3}$$

Recently an alternative proof of the Subspace Theorem has been given by Faltings and Wüstholz [12].

It is an easy consequence of a theorem of Minkowski that there exist forms $L_1, \dots, L_n$ as above with the following property: For any finite collection of proper linear subspaces $S_1, \dots, S_t$ of $\mathbb{Q}^n$ the set of solutions of

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < 1, \quad \mathbf{x} \in \mathbb{Z}^n$$

is not contained in $S_1 \cup \cdots \cup S_t$. So the Subspace Theorem, just as Roth's Theorem is best possible.

W. M. SCHMIDT in 1975 has extended his theorem to the case when the variables $\mathbf{x} = (x_1, \cdots, x_n)$ are integers of a fixed number field K. Moreover the theorem has been generalized by DUBOIS and RHIN [4] and independently by SCHLICKEWEI [17] to include p-adic valuations.

The results mentioned so far are all qualitative, and we may ask the following two questions:

i) Given $\varepsilon > 0$ and linear forms $L_1, \ldots, L_n$ as in the Subspace Theorem, is it possible to determine the subspaces $T_1, \ldots, T_t$ in (0.3) effectively, i.e., to give an algorithm to compute $T_1, \ldots, T_t$?

ii) What can be said about the number t of subspaces $T_1, \ldots, T_t$ needed in (0.3) to cover the set of solutions of (0.2)?

Question (i) is one of the most famous open problems in Diophantine Approximations. Indeed the method of proof for the Subspace Theorem, the so called Thue-Siegel-Roth-Schmidt method, is highly ineffective.

As for question (ii), in the last 15 years quite some progress was made. So in the remainder of the talk we will discuss results on question (ii).

1 THE QUANTITATIVE SUBSPACE THEOREM

The Thue-Siegel-Roth-Schmidt method does not provide an algorithm to determine the set of solutions of (0.1) or the subspaces occurring in (0.2), (0.3). However it does give *upper bounds* for the *number* of solutions of (0.1) or of subspaces in (0.2), (0.3). One of the main tools in giving such upper bounds are "gap principles". We illustrate the easiest case:
Let us consider the inequality

$$\left|\alpha - \frac{x}{y}\right| < y^{-2-\varepsilon} \tag{1.1}$$

in rational numbers $\frac{x}{y}$ with $y > 0$. For any two different solutions $\frac{x_1}{y_1}, \frac{x_2}{y_2}$ of (1.1) with $y_1 < y_2$ we get

$$\frac{1}{y_1 y_2} \leq \left|\frac{x_1}{y_1} - \frac{x_2}{y_2}\right| \leq \left|\frac{x_1}{y_1} - \alpha\right| + \left|\alpha - \frac{x_2}{y_2}\right| \leq 2y_1^{-2-\varepsilon}.$$

So if $\frac{x_1}{y_1}, \ldots, \frac{x_k}{y_k}$ are different solutions of (1.1) with $y_1 < y_2 < \ldots < y_k$ and with the y_i-s in an interval of the type $(Q, Q^E]$ with $Q^{\frac{\varepsilon}{2}} > 2$ and $E > 1$, then

$$k \leq 1 + \frac{\log E}{\log(1 + \frac{\varepsilon}{2})}.$$

In the proof of Roth's Theorem we have the following situation: There exists a certain value Q_0, depending upon α and ε, such that for solutions $\frac{x}{y}$ of (0.1) with $y > Q_0$ we can find m disjoint intervals $(Q_1, Q_1^E], \ldots, (Q_m, Q_m^E]$ having

$$y \in (Q_1, Q_1^E] \cup \cdots \cup (Q_m, Q_m^E].$$

So the above gap principle shows that we cannot have more than

$$m\left(1+\frac{\log E}{\log(1+\frac{\varepsilon}{2})}\right)$$

large solutions. Now Roth's method gives

$$m \le c_1(\varepsilon,d) \quad \text{and} \quad E \le c_2(\varepsilon,d),$$

where d is the degree of α. Thus the number of solutions $\frac{x}{y}$ of (0.1) with y "large" does not exceed a certain function $c(d,\varepsilon)$ depending only upon the degree d of α and upon the parameter ε.

To derive a similar statement in the situation of the Subspace Theorem, we first need a generalization of the gap principle to higher dimensions. Apart from this, there are a number of rather delicate problems in the geometry of numbers to be dealt with for dimension > 2. The pioneering work in this context is due to W. M. SCHMIDT [23] (1989). He proved:

Let $0 < \varepsilon < 1$. Suppose that the forms $L_1,\dots,L_n$ have $\det(L_1,\dots,L_n) = 1$ and that the coefficients of the forms are contained in a number field K with $[K:\mathbb{Q}] = d$. Then there are proper linear subspaces $T_1,\dots,T_t$ of $\mathbb{Q}^n$ where

$$t \le (2d)^{2^{26n}\varepsilon^{-2}} \tag{1.2}$$

such that the set of solutions $\mathbf{x}$ of (0.2) is contained in the union of $T_1,\dots,T_t$ and the ball

$$\| \mathbf{x} \| \le \max\{(n!)^{8/\varepsilon}, H(L_1),\dots,H(L_n)\}, \tag{1.3}$$

where $H(L_i)$ is the height of the coefficient vector of the form L_i ($1 \le i \le n$).

VOJTA [27] has shown that there exist finitely many subspaces $T_1,\dots,T_l$ which are effectively computable and which do not depend upon ε, such that all but finitely many solutions $\mathbf{x}$ of (0.2) are contained in the union $T_1 \cup \dots \cup T_l$. It seems to be very difficult to give an upper bound for the number of exceptional solutions (which in fact will depend upon ε).

Neither one of SCHMIDT'S and VOJTA'S results implies the other one.

SCHMIDT'S result (1.2), (1.3) has been extended by SCHLICKEWEI [18] to the case when the variables $(x_1,\dots,x_n)$ are taken from the field K instead of $\mathbb{Q}$ and also to a finite set S of absolute values on K. To cover the "large" solutions we do not need more than

$$c(n,\varepsilon,d,s) \tag{1.4}$$

proper linear subspaces of K^n. Here s is the cardinality of the set S of absolute values under consideration.

2 IMPROVEMENTS ON THE QUANTITATIVE SUBSPACE THEOREM.

i) The bound for the number t of subspaces given in (1.2) is doubly exponential in n and exponential in ε^{-1}. Its origin essentially may be found in Roth's Lemma:

This is a criterion to guarantee that a polynomial $P(X_1,\dots,X_m)$ with integer coefficients does not vanish with too high order at a rational point $(\frac{x_1}{y_1},\dots,\frac{x_m}{y_m})$. A much more powerful multiplicity estimate has been provided by FALTINGS [11] with his product theorem. Explicit versions of FALTINGS' result were derived independently by EVERTSE [6] and by FERRETTI [13]. As a consequence EVERTSE [7] obtained a substantial improvement of the bounds (1.2) and (1.4) in terms of the dependence upon n and ε^{-1}.

ii) A completely different problem is the question which parameters in the bounds (1.2) and (1.4) are really necessary. As will be seen, to minimize the number of parameters showing up in the bounds is a quite relevant task for applications to diophantine equations. In dealing with inequality (0.2), it turns out that it suffices to study a problem on simultaneous inequalities. It is clear that for any solution $\mathbf{x}$ of (0.2) there exist real numbers $c_1,\dots,c_n$ with

$$c_1+\ldots+c_n\le -\varepsilon \tag{2.1}$$

and

$$|L_1(\mathbf{x})|\le \|\,\mathbf{x}\,\|^{c_1},\dots,|L_n(\mathbf{x})|\le \|\,\mathbf{x}\,\|^{c_n}\,. \tag{2.2}$$

Indeed it suffices to study (2.1), (2.2) for a fixed tuple $c_1,\dots,c_n$. Such inequalities have been investigated by SCHLICKEWEI [19]. In the current situation he was able to replace the bound $c(n,\varepsilon,d,s)$ from (1.4) for the number of subspaces by a bound

$$c(n,\varepsilon). \tag{2.3}$$

So here in comparison with (1.4) the dependence on d and s is avoided. However (2.3) still is only valid for the "large" solutions $\mathbf{x}$, and the definition of "large" is in terms of a function

$$c(n,\varepsilon,d,L_i). \tag{2.4}$$

Let us briefly discuss why in (2.4) the parameter d shows up. In the proof of the Subspace Theorem an important ingredient is the theorem of Minkowski on the successive minima $\lambda_1,\dots,\lambda_n$ of convex bodies. By Minkowski we have

$$\frac{2^n}{n!}\le \lambda_1\ldots\lambda_n V\le 2^n, \tag{2.5}$$

where V is the volume of the convex body. If we deal with the Subspace Theorem for a number field K, we use the generalization of Minkowski's estimate (2.5) to number fields given by MCFEAT [14] and by BOMBIERI and VAALER [2]. However the analogue of (2.5) involves the discriminant of the field as a factor in the upper bound.

In a recent paper, ROY and THUNDER [16] have proved a version of Minkowski's theorem where they do not restrict the variables $\mathbf{x}$ anymore to a number field. They allow arbitrary elements $\mathbf{x}\in\overline{\mathbb{Q}}^n$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. They derive an inequality which essentially is of the same shape as

(2.5). In particular, with their approach they get rid of the discriminant factor in the upper bound.

This new result of Roy and Thunder turns out to be extremely useful in our context. It has been applied in a joint paper by Evertse and Schlickewei [9].

Roughly speaking, the main consequences derived in [9] are as follows.

a) We can now consider inequalities such as (0.2) (or the p-adic generalization) allowing arbitrary solutions $\mathbf{x} \in \overline{\mathbb{Q}}^n$ (instead of only solutions in K^n). The assertion of the theorem then is that the set of all large solutions is contained in the union of finitely many proper subspaces of $\overline{\mathbb{Q}}^n$ (*Absolute Subspace Theorem*).

b) If we consider simultaneous inequalities such as (2.1), (2.2) with solutions $\mathbf{x} \in \overline{\mathbb{Q}}^n$, then again we have to distinguish small and large solutions. The set of large solutions may be covered by

$$c(n, \varepsilon) \tag{2.6}$$

proper subspaces of $\overline{\mathbb{Q}}^n$ (similar bound as in (2.3)). However, in contrast with (2.4) the large solutions now are defined in terms of a function

$$c(n, \varepsilon, L_i) \tag{2.7}$$

only. So in (2.7), in comparison with (2.4), the dependence on the parameter d is avoided.

3 Applications to norm form equations.

Let $L(X_1, \dots, X_n) = \alpha_1 X_1 + \dots + \alpha_n X_n$ be a linear form with coefficients in a number field K of degree d. Denote the embeddings of K into $\overline{\mathbb{Q}}$ by $\alpha \to \alpha^{(i)}$ and write $L^{(i)}(\mathbf{X}) = \alpha_1 X_1 + \dots + \alpha_n X_n$. Put

$$N(L(\mathbf{X})) = \prod_{i=1}^{d} L^{(i)}(\mathbf{X}).$$

By a norm form equation we mean an equation of the type

$$N(L(\mathbf{x})) = m \quad \text{in} \quad \mathbf{x} \in \mathbb{Z}^n. \tag{3.1}$$

Here m is a fixed nonzero rational number. Note that the left hand side of (3.1) is a homogeneous polynomial of degree d in the variables x_i with rational coefficients.

Under suitable and rather natural hypotheses about the linear form L, which we summarize briefly by saying that $N(L(\mathbf{X}))$ is a "nondegenerate" norm form, Schmidt [22] has shown as a consequence of the Subspace Theorem that equation (3.1) has only finitely many solutions $\mathbf{x}$. Using his quantitative result (1.2), in [24] he derived an explicit uniform upper bound for the number of solutions of (3.1) of the shape $c(n, d, m)$. Here the significant feature is that the bound does not depend upon the coefficients of the form L. This proves the n-dimensional analogue of a conjecture made by SIEGEL in 1929. The corresponding result for $n = 2$ had been proved by EVERTSE in 1984 already. EVERTSE [5], applying his version of the quantitative Subspace Theorem, obtained a considerable improvement on the bound given by SCHMIDT. Further EVERTSE and GYŐRY [8] have studied equations with more general forms, the so called decomposable form equations.

4 UNIT EQUATIONS

Let K be a field of characteristic zero. Let $a_1, \ldots, a_n$ be fixed nonzero elements in K. Consider the equation

$$a_1 x_1 + \ldots + a_n x_n = 1. \tag{4.1}$$

We call a solution $(x_1, \ldots, x_n)$ of (4.1) nondegenerate if no nonempty subsum on the left hand side of (4.1) vanishes. Applying the absolute quantitative Subspace Theorem by EVERTSE and SCHLICKEWEI, discussed in section 2, in a recent paper EVERTSE, SCHLICKEWEI and W. M. SCHMIDT [10] proved the following:

Let G be a finitely generated subgroup of the multiplicative group K^* of nonzero elements of K. Suppose G has rank r. Then the number of nondegenerate solutions $(x_1, \ldots, x_n) \in G^n$ of equation (4.1) does not exceed

$$\exp\bigl(n^{cn}(r+1)\bigr). \tag{4.2}$$

Here c is an absolute constant.

To prove such a result, we first observe that using a specialization argument, it suffices to deal with the case when K is a number field. Once we have reached this situation, after the transformation $Y_i = a_i X_i$, we may apply the Subspace Theorem to the linear forms in $Y_1, \ldots, Y_n$ given by $L_1(Y_1, \ldots, Y_n) = Y_1, \ldots, L_n(Y_1, \ldots, Y_n) = Y_n, L_{n+1}(Y_1, \ldots, Y_n) = Y_1 + \ldots + Y_n$. Actually we need the p-adic version of the Subspace Theorem, where S, the set of absolute values, consists of all archimedean absolute values of K together with those finite absolute values corresponding to the prime ideals dividing the coefficients a_i and the generators of the group G. In this application ε turns out to be a function of n only.

The results given in section 0 simply imply that we get only finitely many solutions. The results of section 1, in view of (1.4) give a bound depending upon the degree d of the number field K and upon the cardinality s of the set S. In particular, if at the beginning K is not a number field, our result will depend upon the specialization. Moreover in general, the parameter s will be much larger than the rank r of the group G. In [19] SCHLICKEWEI introduced a method which in conjunction with (2.3) allows it to derive a bound for the number of large solutions of (4.1) which in fact does not involve the cardinality s of S but only the rank r of the original group G. So (2.3) already would give a bound of type (4.2) for the number of large solutions.

There remain the small solutions. Before we had the bound (2.7) from the Absolute Subspace Theorem, the definition of the small solutions always depended on the degree of the number field K. Clearly then the specialization argument has a deadly impact, as then the degree of the number field, we end up with after the specialization, appears in the final result.

It is at this point where the Absolute Subspace Theorem comes in. Here the small solutions are defined in terms of the forms L_i, of n and of ε only. In view of the particular shape of our forms L_i and as ε is a function of n only, the small solutions by (2.7) now are defined in terms of n only. In particular the definition of the size of the small solutions is completely independent of the number field obtained with the specialization argument.

To exploit successfully this bound for the small solutions, we needed a new gap principle. Here the results of Zhang [29], [30] on lower bounds for the heights of points on varieties are crucial. Using the elementary method introduced in this context by Zagier [28], in dimension 2 such a new gap principle was first given in a paper by Schlickewei and Wirsing [21]. For general n, Bombieri and Zannier [3] gave an elementary proof of Zhang's result and obtained a gap principle which is suitable for our purposes. This has been improved substantially by W. M. Schmidt [25].

Results on equation (4.1) apply in particular to linear recurrence sequences, i.e., to sequences $\{u_n\}_{n\in\mathbb{Z}}$ satisfying a relation

$$u_{n+k} = a_{k-1}u_{n+k-1} + \ldots + a_0 u_n. \tag{4.3}$$

Here we assume that $a_0 \neq 0$ and that we have initial values $(u_0, \ldots, u_{k-1}) \neq (0, \ldots, 0)$. Writing

$$G(z) = z^k - a_{k-1}z^{k-1} - \ldots - a_0 = \prod_{i=1}^{r}(z-\alpha_i)^{\rho_i} \tag{4.4}$$

with distinct roots α_i of multiplicity ρ_i, it is well known that we have

$$u_n = \sum_{i=1}^{r} f_i(n)\alpha_i^n, \tag{4.5}$$

where the f_i are polynomials of respective degrees $\leq \rho_i - 1$. An old conjecture says that for a nondegenerate sequence u_n of order k the equation

$$u_n = 0 \quad (n \in \mathbb{Z})$$

does not have more than $c(k)$ solutions, where $c(k)$ is a function depending on k only.

For $k = 3$, this conjecture has been proved by Schlickewei [20]. Later Beukers and Schlickewei [1] derived the estimate $c(3) \leq 61$. For general k and for sequences u_n such that the companion polynomial $G(z)$ given in (4.4) has only simple zeros, in view of (4.5), the conjecture is an easy consequence of the theorem of Evertse, Schlickewei and W. M. Schmidt [10] on equation (4.1). In fact, if the zeros α_i in (4.4) are simple the polynomials f_i in (4.5) reduce to constants. The general case of the conjecture with arbitrary polynomial coefficients has been settled recently by W. M. Schmidt [26].

REFERENCES

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

[2] Bombieri, E., Vaaler, J.: *On Siegel's Lemma*, Invent. Math. 73 (1983), 11–32.

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

[4] Dubois, E., Rhin, G.: *Approximations rationnelles simultanées de nombres algébriques réels et de nombres algébriques p-adiques*, Journées Arithmétiques de Bordeaux, Astérisque 24–25 (1975), 211–227.

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

[6] Evertse, J.-H.: *An explicit version of Faltings' Product Theorem and an improvement of Roth's Lemma*, Acta Arith. 73 (1995), 215–248.

[7] Evertse, J.-H.: *An improvement of the quantitative Subspace theorem*, Comp. Math. 101 (1996), 225–311.

[8] Evertse, J.-H., Győry: *The number of families of solutions of decomposable form equations*, Acta Arith. 80 (1997), 367–394.

[9] Evertse, J.-H., Schlickewei, H.P.: *A quantitative version of the absolute Subspace Theorem*, to appear.

[10] Evertse, J.-H., Schlickewei, H. P., Schmidt, W. M.: *Linear equations with variables which lie in a multiplicative group*, to appear.

[11] Faltings, G.: *Diophantine approximation on abelian varieties*, Ann. of Math. 133 (1991), 549–576.

[12] Faltings, G., Wüstholz, G.: *Diophantine approximations on projective spaces*, Inv. math. 116 (1994), 109–138.

[13] Ferretti, R.: *An effective version of Faltings' Product Theorem*, Forum Math. 8 (1996), 401–427

[14] McFeat, R.B.: *Geometry of numbers in adèle spaces*, Dissertationes Mathematicae 88, PWN Polish Scientific Publishers, Warsaw 1971

[15] Roth, K. F.: *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1–20.

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

[17] Schlickewei, H. P.: *The $\wp$-adic Thue-Siegel-Roth-Schmidt theorem*, Arch. Math. 29 (1977), 267–270.

[18] Schlickewei, H. P.: *The quantitative Subspace Theorem for number fields*, Compos. Math. 82 (1992), 245–274.

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

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

[21] Schlickewei, H.P., Wirsing, E.: *Lower bounds for the heights of solutions of linear equations*, Invent. Math. 129 (1997), 1–10.

[22] Schmidt, W. M.: *Norm form equations*, Ann. of Math. 96 (1972), 526–551.

[23] Schmidt, W. M.: *The Subspace Theorem in diophantine approximation*, Compos. Math 69 (1989), 121–173.

[24] Schmidt, W. M.: *The number of solutions of norm form equations*, Transactions A.M.S. 317 (1990), 197–227.

[25] Schmidt, W. M.: *Heights of points on subvarieties of* $\mathbb{G}_m^n$, Séminaire de théorie des nombres de Paris, 1993-1994 (ed. by S. David), 157–187, Cambridge Un. Press, 1996.

[26] Schmidt, W. M.: *The zero multiplicity of linear recurrence sequences*, to appear.

[27] Vojta, P.: *A refinement of Schmidt's subspace theorem*, Amer. J. Math. 111 (1989), 489–518.

[28] Zagier, D.: *Algebraic numbers close to both* 0 *and* 1, Math. Computation 61 (1993), 485–491.

[29] Zhang, S.: *Positive line bundles on arithmetic surfaces*, Annals of Math. 136 (1992), 569–587.

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

Hans Peter Schlickewei
Fachbereich Mathematik
Philipps-Universität Marburg
Lahnberge
D-35032 Marburg
Germany