

QUADRATIC GEOMETRY OF NUMBERS

HANS PETER SCHLICKWEI AND WOLFGANG M. SCHMIDT

ABSTRACT. We give upper bounds for zeros of quadratic forms. For example we prove that for any nondegenerate quadratic form $\mathfrak{F}(x_1, \dots, x_n)$ with rational integer coefficients which vanishes on a d -dimensional rational subspace ($d > 0$) there exist sublattices $\Gamma_0, \Gamma_1, \dots, \Gamma_{n-d}$ of \mathbf{Z}^n of rank d , on which \mathfrak{F} vanishes, with the following properties:

$$\text{rank}(\Gamma_0 \cap \Gamma_i) = d - 1, \quad \text{rank}(\Gamma_0 \cup \Gamma_1 \cup \dots \cup \Gamma_{n-d}) = n$$

and

$$(\det \Gamma_0)^{n-d} \det \Gamma_1 \cdots \det \Gamma_{n-d} \ll F^{(n-d)^2},$$

where F is the maximum modulus of the coefficients of \mathfrak{F} .

1. Introduction. Let Λ be a lattice of determinant Δ in n -dimensional Euclidean space E^n . Let

$$(1) \quad \mathfrak{F}(\mathbf{X}) = \sum_{i=1}^n \sum_{j=1}^n f_{ij} X_i X_j$$

be a quadratic form with $f_{ij} = f_{ji}$ which assumes only integral values at the points (x_1, \dots, x_n) of Λ . Put

$$(2) \quad F = F(\mathfrak{F}) = \left(\sum_{i=1}^n \sum_{j=1}^n f_{ij}^2 \right)^{1/2}.$$

Suppose there is some point of Λ , other than the origin, at which $\mathfrak{F}(x_1, \dots, x_n) = 0$. It was proved by Cassels [2] in the case $\Lambda = \mathbf{Z}^n$ and by Birch and Davenport [1] in the general case that then there is such a point which satisfies the estimate

$$(3) \quad \|\mathbf{x}\| = (x_1^2 + \dots + x_n^2)^{1/2} \ll F^{(n-1)/2} \Delta.$$

Here and in the sequel, the constant implied by \ll depends only upon n . Recently Schlickewei [5] generalized (3) in the following way. Suppose that

$$(4) \quad 0 < d < n$$

and that \mathfrak{F} vanishes on a d -dimensional sublattice Γ of Λ . Then there is such a sublattice satisfying

$$(5) \quad \det \Gamma \ll F^{(n-d)/2} \Delta.$$

Received by the editors April 14, 1986.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 11D09, 11H55; Secondary 11H99, 11H50.

In his paper [4] Davenport asked for an inequality involving n linearly independent lattice points at which \mathfrak{F} vanishes. He says that he is able to prove such an inequality only for two independent lattice points.

More precisely he shows that for $d = 1$ in (4) there exist two linearly independent points \mathbf{x} and \mathbf{y} of Λ such that

$$(6) \quad \mathfrak{F}(\mathbf{x}) = \mathfrak{F}(\mathbf{y}) = 0$$

and

$$(7) \quad \|\mathbf{x}\| \cdot \|\mathbf{y}\| \ll F^{n-1} \Delta^2.$$

Schulze-Pillot [6] established inequalities involving n linearly independent zeros. One of his results is as follows. Suppose \mathfrak{F} is nondegenerate and has a nontrivial zero in Λ . Then there exist n linearly independent lattice points $\mathbf{x}_0, \dots, \mathbf{x}_{n-1}$ with $\mathfrak{F}(\mathbf{x}_i) = 0$ ($i = 0, \dots, n - 1$) and with

$$(8) \quad \|\mathbf{x}_0\|^{n-1} \|\mathbf{x}_1\| \cdots \|\mathbf{x}_{n-1}\| \ll F^{(n-1)^2} \Delta^{2(n-1)}.$$

It is the purpose of this paper to prove a theorem which contains all the results quoted above as particular cases.

THEOREM 1. *Let \mathfrak{F} be a quadratic form as in (1), which assumes integral values at the points of the lattice Λ . Let $0 < d < n$ and suppose \mathfrak{F} has rank $> n - d$. Suppose moreover that \mathfrak{F} vanishes on a d -dimensional sublattice Γ of Λ . Then there exist d -dimensional sublattices $\Gamma_0, \Gamma_1, \dots, \Gamma_{n-d}$ of Λ with the following properties:*

- (i) *For each i ($i = 0, 1, \dots, n - d$) \mathfrak{F} vanishes on Γ_i .*
- (ii) *For each j ($j = 1, \dots, n - d$) $\Gamma_0 \cap \Gamma_j$ has dimension $d - 1$.*
- (iii) *The union of $\Gamma_0, \Gamma_1, \dots, \Gamma_{n-d}$ spans E^n .*
- (iv) *For each j ($j = 1, \dots, n - d$)*

$$(9) \quad \det \Gamma_0 \det \Gamma_j \ll F^{n-d} \Delta^2.$$

It is clear that (9) immediately implies that there is a d -dimensional sublattice Γ of Λ on which \mathfrak{F} vanishes with $\det \Gamma \ll F^{(n-d)/2} \Delta$ which is the main result of [5].

Moreover for $d = 1$ we have an extension of Davenport's Theorem [4]. A direct consequence of Theorem 1 is

COROLLARY. *Let the hypotheses be the same as in Theorem 1. Then the lattices $\Gamma_0, \Gamma_1, \dots, \Gamma_{n-d}$ satisfy*

$$(10) \quad \det \Gamma_0^{n-d} \det \Gamma_1 \cdots \det \Gamma_{n-d} \ll F^{(n-d)^2} \Delta^{2(n-d)}.$$

If $d = 1$, this is Schulze-Pillot's Theorem 2 [6], as quoted in (8). The following example shows that Theorem 1 is best possible. Consider the form

$$\mathfrak{F}(\mathbf{X}) = 0 \cdot X_1^2 + \cdots + 0 \cdot X_{d-1}^2 - (X_{d+1} - lX_d)^2 - (X_{d+2} - lX_{d+1})^2 - \cdots - (X_n - lX_{n-1})^2$$

where l is a large integer. Take $\Lambda = \mathbf{Z}^n$. Here \mathfrak{F} has rank $n - d + 1$ and it vanishes on the d -dimensional sublattice generated by $\mathbf{e}_1, \dots, \mathbf{e}_{d-1}, \mathbf{e}_d + l\mathbf{e}_{d+1} + l^2\mathbf{e}_{d+2} + \cdots + l^{n-d-1}\mathbf{e}_{n-1} + (l^{n-d} + 1)\mathbf{e}_n$, where $\mathbf{e}_1, \dots, \mathbf{e}_n$ is the canonical basis of E^n . Now any nontrivial integral zero of the nonsingular part of \mathfrak{F} , $X_d^2 - (X_{d+1} - lX_d)^2 - \cdots - (X_n - lX_{n-1})^2$ has

$$\max_{d \leq i \leq n} |x_i| \gg l^{n-d} \gg F^{(n-d)/2}.$$

In fact this is Kneser’s well-known counterexample, cf. Cassels [3]. Therefore any d -dimensional sublattice Γ on which \mathfrak{F} vanishes has $\det \Gamma \gg F^{(n-d)/2}$. Hence Theorem 1 and the Corollary are best possible.

The following result gives an estimate for the determinant of n linearly independent lattice points at which \mathfrak{F} vanishes.

THEOREM 2. *Let \mathfrak{F} be a quadratic form as in (1). Suppose that \mathfrak{F} is nonsingular and assumes integral values at the points of the lattice Λ . Suppose moreover that there exists a d -dimensional sublattice Γ of Λ with $d > 0$ on which \mathfrak{F} vanishes. Then there exist linearly independent points $\mathbf{x}_1, \dots, \mathbf{x}_n$ in Λ with $\mathfrak{F}(\mathbf{x}_i) = 0$ ($i = 1, \dots, n$) and*

$$(11) \quad |\det(\mathbf{x}_1, \dots, \mathbf{x}_n)| \ll |\det \mathfrak{F}|^{(n-d)/2d} \Delta^{n/d}.$$

The case $d = 1$ of Theorem 2 was shown by Schulze-Pillot [6].

2. The case $d = n - 1$. We may assume that \mathfrak{F} is primitive, i.e., there is no integer $m > 1$ such that $m^{-1}\mathfrak{F}$ assumes only integral values on Λ . This is equivalent to the condition that the \mathbf{Z} -module generated by the values $\mathfrak{F}(\mathbf{x})$ with $\mathbf{x} \in \Lambda$ is \mathbf{Z} .

By hypothesis \mathfrak{F} vanishes on an $(n - 1)$ -dimensional linear subspace, which is defined by a linear equation $L_0(\mathbf{x}) = 0$. Therefore we have either

$$(i) \quad \mathfrak{F}(\mathbf{X}) = L_0(\mathbf{X})L_1(\mathbf{X})$$

with nonproportional linear forms L_0, L_1

or

$$(ii) \quad \mathfrak{F}(\mathbf{X}) = cL_0(\mathbf{X})^2.$$

We call a sublattice Γ of Λ primitive if $\Gamma = \Lambda \cap S(\Gamma)$, where $S(\Gamma)$ is the subspace of E^n generated by Γ .

LEMMA 1. *If \mathfrak{F} is of type (i), then there are exactly two primitive $(n - 1)$ -dimensional sublattices Γ_0, Γ_1 of Λ on which \mathfrak{F} vanishes. Any $(n - 1)$ -dimensional sublattice on which \mathfrak{F} vanishes is contained in either Γ_0 or Γ_1 . If \mathfrak{F} is of type (ii) there is exactly one primitive $(n - 1)$ -dimensional sublattice Γ_0 on which \mathfrak{F} vanishes. Any $(n - 1)$ -dimensional sublattice on which \mathfrak{F} vanishes is contained in Γ_0 .*

PROOF. There is a nonsingular linear transformation A such that $\Lambda = A\mathbf{Z}^n$. The form $\mathfrak{F}^*(\mathbf{X}) = \mathfrak{F}(A\mathbf{X})$ maps \mathbf{Z}^n into \mathbf{Z} . Here \mathfrak{F}^* is of type (i) resp. (ii) if and only if \mathfrak{F} is of type (i) resp. (ii). It suffices to prove the assertion for \mathfrak{F}^* . So we may restrict ourselves to the case $\Lambda = \mathbf{Z}^n$.

Now \mathfrak{F} vanishes on an $(n - 1)$ -dimensional sublattice of \mathbf{Z}^n , hence on a subspace $L_0(\mathbf{x}) = 0$ where L_0 has rational coefficients.

If (i) holds, then L_1 has rational coefficients as well. The equations $L_0(\mathbf{x}) = 0$ resp. $L_1(\mathbf{x}) = 0$ define two different rational hyperplanes S_0, S_1 . It is clear that $\Gamma_0 = \mathbf{Z}^n \cap S_0$ and $\Gamma_1 = \mathbf{Z}^n \cap S_1$ have the desired properties.

If (ii) holds, then $\Gamma_0 = \mathbf{Z}^n \cap S_0$ where again S_0 is the subspace defined by $L_0(\mathbf{x}) = 0$.

The case $d = n - 1$ of Theorem 1 is a consequence of the following proposition.

PROPOSITION. *If \mathfrak{F} is of type (i), then*

$$(12) \quad \Delta^2 F \leq \det \Gamma_0 \det \Gamma_1 \leq \sqrt{2} \Delta^2 F.$$

If \mathfrak{F} is of type (ii), then

$$(13) \quad \Delta^2 F \leq (\det \Gamma_0)^2 \leq \sqrt{2} \Delta^2 F.$$

To deduce Theorem 1 in the case $d = n - 1$, we remark that if \mathfrak{F} is of type (i) it has rank 2, whereas a form \mathfrak{F} of type (ii) has rank 1. Since we assume in Theorem 1 rank $\mathfrak{F} > n - d$, we may conclude that \mathfrak{F} is of type (i), and Theorem 1 holds with the lattices Γ_0 and Γ_1 of (12).

PROOF OF THE PROPOSITION. If \mathfrak{F} is of type (i), the intersection $\Gamma^* = \Gamma_0 \cap \Gamma_1$ is an $(n - 2)$ -dimensional sublattice of Λ . Let $\mathbf{a}_1, \dots, \mathbf{a}_{n-2}$ be a basis of Γ^* . Choose $\mathbf{b}_0, \mathbf{b}_1$ such that $\mathbf{a}_1, \dots, \mathbf{a}_{n-2}, \mathbf{b}_i$ is a basis of Γ_i ($i = 0, 1$). This is possible since $\Gamma_i \cap S(\Gamma^*) = \Gamma^*$, where $S(\Gamma^*)$ is the subspace generated by Γ^* . (If $n = 2$, \mathbf{b}_i is a basis of Γ_i .) Put

$$(14) \quad M_i(\mathbf{X}) = \det(\mathbf{a}_1, \dots, \mathbf{a}_{n-2}, \mathbf{b}_i, \mathbf{X}) \quad (i = 0, 1),$$

i.e., the determinant with rows $\mathbf{a}_1, \dots, \mathbf{a}_{n-2}, \mathbf{b}_i, \mathbf{X}$. Then M_i is a nonzero linear form which vanishes on Γ_i . Hence M_i is proportional to L_i ($i = 0, 1$).

If \mathfrak{F} is of type (ii), let $\mathbf{a}_1, \dots, \mathbf{a}_{n-1}$ be a basis of Γ_0 and put

$$(15) \quad M(\mathbf{X}) = \det(\mathbf{a}_1, \dots, \mathbf{a}_{n-1}, \mathbf{X}).$$

As in case (i) we see that M is proportional to L_0 .

We need the following

LEMMA 2. *If \mathfrak{F} is of type (i), then*

$$(16) \quad \mathfrak{F}(\mathbf{X}) = \Delta^{-2} M_0(\mathbf{X}) M_1(\mathbf{X}),$$

where M_i is defined in (14).

If \mathfrak{F} is of type (ii), then

$$(17) \quad \mathfrak{F}(\mathbf{X}) = \Delta^{-2} M(\mathbf{X})^2,$$

where M is as in (15).

PROOF. We shall treat only case (i), since case (ii) may be done in a completely analogous way.

Let Λ' be the sublattice of Λ with basis $\mathbf{a}_1, \dots, \mathbf{a}_{n-2}, \mathbf{b}_0, \mathbf{b}_1$. Let I be the index of Λ' in Λ . (14) implies that any $\mathbf{y} \in \Lambda'$ satisfies

$$\Delta^{-2} M_0(\mathbf{y}) M_1(\mathbf{y}) \in \Delta^{-2} (\det(\mathbf{a}_1, \dots, \mathbf{a}_{n-2}, \mathbf{b}_0, \mathbf{b}_1))^2 \mathbf{Z} = \Delta^{-2} (\det \Lambda')^2 \mathbf{Z} = I^2 \mathbf{Z}.$$

Hence $\Delta^{-2} M_0(\mathbf{y}) M_1(\mathbf{y})$ is an integral multiple of I^2 . Since any $\mathbf{x} \in \Lambda$ is of the shape $\mathbf{x} = I^{-1} \mathbf{y}$ where $\mathbf{y} \in \Lambda'$, we may infer that

$$\Delta^{-2} M_0(\mathbf{x}) M_1(\mathbf{x}) \in \mathbf{Z} \quad \text{for any } \mathbf{x} \in \Lambda$$

Therefore the right-hand side in (16) is a quadratic form which assumes integral values on Λ . Since it is proportional to \mathfrak{F} , it suffices to show that it is primitive. Notice that

$$\Delta^{-2} M_0(\mathbf{b}_0 + \mathbf{b}_1) M_1(\mathbf{b}_0 + \mathbf{b}_1) = \Delta^{-2} (\det \Lambda')^2 = I^2.$$

By the remark made at the beginning of this section it will suffice to find a $\mathbf{g} \in \Lambda$ with

$$\Delta^{-2}M_0(\mathbf{g})M_1(\mathbf{g}) = v \quad \text{and} \quad \text{g. c. d.}(I^2, v) = 1.$$

Since $\Lambda \cap S_0 = \Gamma_0$, there exists a basis of Λ of the shape $\mathbf{a}_1, \dots, \mathbf{a}_{n-2}, \mathbf{b}_0, \mathbf{h}$. Therefore the group Λ/Γ_0 is cyclic and this implies that Λ/Λ' is cyclic as well.

Suppose $\mathbf{g} \in \Lambda$ represents a class which generates Λ/Λ' . \mathbf{g} may be written as

$$\mathbf{g} = I^{-1}(u_1\mathbf{a}_1 + \dots + u_{n-2}\mathbf{a}_{n-2} + v_0\mathbf{b}_0 + v_1\mathbf{b}_1)$$

with integers $u_1, \dots, u_{n-2}, v_0, v_1$ satisfying $\text{g. c. d.}(u_1, \dots, u_{n-2}, v_0, v_1, I) = 1$. If we have $\text{g. c. d.}(I, v_0) = m$ then

$$(I/m)\mathbf{g} = m^{-1}(u_1\mathbf{a}_1 + \dots + u_{m-2}\mathbf{a}_{n-2} + v_1\mathbf{b}_1) + (v_0/m)\mathbf{b}_0$$

lies in Λ . Here the second summand on the right-hand side is in Λ , hence the same holds true for the first one. We may infer that the first summand lies in Γ_1 . As a consequence we see that m divides all coefficients u_i, v_j , and therefore $m = 1$.

Hence we get $\text{g. c. d.}(I, v_0) = 1$ and similarly $\text{g. c. d.}(I, v_1) = 1$. Since we have $\Delta^{-2}M_0(\mathbf{g})M_1(\mathbf{g}) = v_0v_1$, with $\text{g. c. d.}(I^2, v_0v_1) = 1$, the assertion of Lemma 2 follows in case (i).

Now the proof of the Proposition may be easily finished. Suppose we are in case (i). Write

$$\bar{M}_i(\mathbf{X}) = u_{i1}X_1 + \dots + u_{in}X_n \quad (i = 0, 1)$$

and

$$(18) \quad |M_i| = (u_{i1}^2 + \dots + u_{in}^2)^{1/2} \quad (i = 0, 1).$$

The coefficients u_{ij} of M_i are the determinants of order $n - 1$ of the matrix with rows $\mathbf{a}_1, \dots, \mathbf{a}_{n-2}, \mathbf{b}_i$. Therefore we have

$$(19) \quad |M_i| = \det \Gamma_i \quad (i = 0, 1).$$

By assertion (16) of Lemma 2, the coefficients f_{ij} of \mathfrak{F} satisfy

$$f_{ij} = \frac{1}{2}\Delta^{-2}(u_{0i}u_{1j} + u_{1i}u_{0j}) \quad (1 \leq i, j \leq n),$$

and we obtain using (18)

$$\begin{aligned} F^2 &= \sum_{i=1}^n \sum_{j=1}^n f_{ij}^2 \\ &= \frac{1}{4}\Delta^{-4} \sum_{i=1}^n \sum_{j=1}^n (u_{0i}u_{1j} + u_{1i}u_{0j})^2 \\ (20) \quad &= \frac{1}{2}\Delta^{-4} \left(\left(\sum_{i=1}^n u_{0i}^2 \right) \left(\sum_{j=1}^n u_{1j}^2 \right) + \left(\sum_{i=1}^n u_{0i}u_{1i} \right)^2 \right) \\ &= \frac{1}{2}\Delta^{-4} \left(|M_0|^2|M_1|^2 + \left(\sum_{i=1}^n u_{0i}u_{1i} \right)^2 \right). \end{aligned}$$

On the other hand by Cauchy’s inequality and in view of (19) we have

$$(21) \quad 0 \leq \left(\sum_{i=1}^n u_{0i} u_{1i} \right)^2 \leq |M_0|^2 |M_1|^2 = (\det \Gamma_0)^2 (\det \Gamma_1)^2.$$

Combination of (20) and (21) yields

$$\frac{1}{2} \Delta^{-4} (\det \Gamma_0)^2 (\det \Gamma_1)^2 \leq F^2 \leq \Delta^{-4} (\det \Gamma_0)^2 (\det \Gamma_1)^2,$$

which is the assertion of the Proposition in case (i).

The proof in case (ii) goes along completely analogous lines, using (17) in Lemma 2 instead of (16).

3. Proof of Theorem 1. Let Γ_0 be a d -dimensional sublattice of Λ on which \mathfrak{F} vanishes and such that $\det \Gamma_0$ is minimal. Then Γ_0 is a primitive sublattice of Λ . Let $S(\Gamma_0)$ be the subspace generated by Γ_0 . Let S^\perp be the subspace of dimension $n - d$ which is perpendicular to $S(\Gamma_0)$ with respect to the Euclidean inner product. The projection of Λ on S^\perp is a lattice Γ_0^\perp . Since Γ_0 is primitive we have

$$\det \Gamma_0 \det \Gamma_0^\perp = \det \Lambda = \Delta.$$

A well-known result in reduction theory says that Γ_0^\perp has a basis $\mathbf{p}_1, \dots, \mathbf{p}_{n-d}$ satisfying

$$(23) \quad |\mathbf{p}_1| \cdots |\mathbf{p}_{n-d}| \ll \det \Gamma_0^\perp = \Delta / \det \Gamma_0.$$

Here we may assume moreover that

$$(24) \quad |\mathbf{p}_1| \leq |\mathbf{p}_2| \leq \cdots \leq |\mathbf{p}_{n-d}|.$$

LEMMA 3. *Suppose \mathfrak{F} has rank $> n - d$. Then*

$$|\mathbf{p}_1| \cdots |\mathbf{p}_{n-d-1}| \gg F^{-(n-d-1)/2}.$$

PROOF. We shall prove that there exists an integer l with $0 \leq l \leq (n - d - 1)/2$ having the following properties:

There are pairs $(1, i_1), (2, i_2), \dots, (l, i_l)$ of $2l$ distinct numbers among $\{1, 2, \dots, n - d - 1\}$ satisfying

$$(25) \quad F |\mathbf{p}_\lambda| |\mathbf{p}_{i_\lambda}| \gg 1 \quad (1 \leq \lambda \leq l)$$

and

$$(26) \quad F |\mathbf{p}_{l+1}|^2 \gg 1.$$

It is clear that the assertion of Lemma 3 follows at once from (24), (25) and (26).

We proceed to deduce the existence of l . Let $\mathbf{x}_1, \dots, \mathbf{x}_d$ be a basis of Γ_0 satisfying

$$(27) \quad |\mathbf{x}_1| \leq |\mathbf{x}_2| \leq \cdots \leq |\mathbf{x}_d|$$

and

$$(28) \quad |\mathbf{x}_1| \cdots |\mathbf{x}_d| \gg \det \Gamma_0.$$

In general, the points $\mathbf{p}_1, \dots, \mathbf{p}_{n-d}$ will not lie in Λ . However there exist points

$$(29) \quad \mathbf{z}_\nu = \lambda_{1\nu} \mathbf{x}_1 + \cdots + \lambda_{d\nu} \mathbf{x}_d + \mathbf{p}_\nu \in \Lambda \quad (1 \leq \nu \leq n - d).$$

Here we may suppose that

$$(30) \quad |\lambda_{i\nu}| \leq \frac{1}{2} \quad (1 \leq i \leq d, 1 \leq \nu \leq n - d).$$

Let $\mathfrak{F}(\mathbf{X}, \mathbf{Y})$ be the symmetric bilinear form associated with \mathfrak{F} which has $\mathfrak{F}(\mathbf{X}, \mathbf{X}) = \mathfrak{F}(\mathbf{X})$. Since $\text{rank } \mathfrak{F} > n - d$ and since \mathfrak{F} vanishes on the d -dimensional subspace $S(\Gamma_0)$ there exist a point $\mathbf{x} \in \Gamma_0$ and a ν ($1 \leq \nu \leq n - d$) such that

$$(31) \quad \mathfrak{F}(\mathbf{x}, \mathbf{z}_\nu) \neq 0.$$

Let r be the smallest among the numbers ν satisfying (31). We distinguish the cases $r = 1$ and $r > 1$.

If $r = 1$, we consider the $(d + 1)$ -dimensional sublattice Λ' of Λ generated by Γ_0 and \mathbf{z}_1 . We have

$$(32) \quad \det \Lambda' = \det \Gamma_0 |\mathbf{p}_1|.$$

Consider the restriction \mathfrak{F}' of \mathfrak{F} to the $(d + 1)$ -dimensional subspace S' generated by Λ' . Now \mathfrak{F}' vanishes on the d -dimensional sublattice Γ_0 of Λ' . Since $\mathfrak{F}(\Gamma_0, \mathbf{z}_1) \neq 0$ we are in the situation of case (i) of the Proposition, with n, Λ, \mathfrak{F} resp. replaced by $d + 1, \Lambda', \mathfrak{F}'$. Therefore there are two primitive sublattices of Λ' , both of dimension d on which \mathfrak{F}' vanishes. One of these lattices is Γ_0 . Let Γ'_0 be the other. Then by (12) we have

$$\det \Gamma_0 \det \Gamma'_0 \ll (\det \Lambda')^2 F' \ll (\det \Lambda')^2 F,$$

where F' is defined with respect to \mathfrak{F}' in the same way as F with respect to \mathfrak{F} . Using (32) and the fact that $\det \Gamma_0$ is minimal we get

$$(\det \Gamma_0)^2 \ll (\det \Gamma_0)^2 |\mathbf{p}_1|^2 F,$$

which means

$$(33) \quad F |\mathbf{p}_1|^2 \gg 1.$$

So if $r = 1$, (25) and (26) hold true with $l = 0$.

Now suppose $r > 1$. Recall the definition of \mathbf{z}_1 in (29). Since $\mathfrak{F}(\mathbf{x}, \mathbf{z}_1) = 0$ for all $\mathbf{x} \in \Gamma_0$ we have $\mathfrak{F}(\mathbf{z}_1) = \mathfrak{F}(\mathbf{p}_1) \in \mathbf{Z}$. Therefore if $\mathfrak{F}(\mathbf{p}_1) \neq 0$ we may infer that

$$F |\mathbf{p}_1|^2 \gg |\mathfrak{F}(\mathbf{p}_1)| \geq 1,$$

and again (25), (26) are satisfied with $l = 0$.

Consequently we may assume that \mathfrak{F} vanishes on the $(d + 1)$ -dimensional linear subspace S_{d+1} generated by Γ_0 and \mathbf{z}_1 . In particular \mathfrak{F} vanishes on the d -dimensional sublattice Γ generated by $\mathbf{x}_1, \dots, \mathbf{x}_{d-1}, \mathbf{z}_1$. As Γ_0 was chosen minimal we have

$$(34) \quad \det \Gamma_0 \leq \det \Gamma.$$

On the other hand by (29) we obtain

$$\begin{aligned} (\det \Gamma)^2 &= \det \begin{pmatrix} (\mathbf{x}_1, \mathbf{x}_1) & \cdots & (\mathbf{x}_1, \mathbf{x}_{d-1}) & (\mathbf{x}_1, \mathbf{z}_1) \\ \vdots & & \vdots & \vdots \\ (\mathbf{x}_{d-1}, \mathbf{x}_1) & \cdots & (\mathbf{x}_{d-1}, \mathbf{x}_{d-1}) & (\mathbf{x}_{d-1}, \mathbf{z}_1) \\ (\mathbf{z}_1, \mathbf{x}_1) & \cdots & (\mathbf{z}_1, \mathbf{x}_{d-1}) & (\mathbf{z}_1, \mathbf{z}_1) \end{pmatrix} \\ &= \lambda_{d1}^2 (\det \Gamma_0)^2 + |\mathbf{p}_1|^2 \det \begin{pmatrix} (\mathbf{x}_1, \mathbf{x}_1) & \cdots & (\mathbf{x}_1, \mathbf{x}_{d-1}) \\ \vdots & & \vdots \\ (\mathbf{x}_{d-1}, \mathbf{x}_1) & \cdots & (\mathbf{x}_{d-1}, \mathbf{x}_{d-1}) \end{pmatrix} \end{aligned}$$

where we have used the fact that \mathbf{p}_1 is perpendicular to $\mathbf{x}_1, \dots, \mathbf{x}_d$. Combining this with (28), (30) and (34) we get

$$|\mathbf{p}_1|^2 |\mathbf{x}_1|^2 \cdots |\mathbf{x}_{d-1}|^2 \gg |\mathbf{x}_1|^2 \cdots |\mathbf{x}_d|^2.$$

In view of (24) and (27) this means that

$$(35) \quad \min_{1 \leq i \leq n-d} |\mathbf{p}_i| \gg \max_{1 \leq j \leq d} |\mathbf{x}_j|.$$

Now \mathfrak{F} vanishes on the $(d+1)$ -dimensional subspace S_{d+1} generated by $\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{p}_1$ but it has rank $> n-d$. Therefore there exists an i_1 with $2 \leq i_1 \leq n-d-1$ such that

$$(36) \quad \mathfrak{F}(\mathbf{x}, \mathbf{z}_{i_1}) = \mathfrak{F}(\mathbf{x}, \mathbf{p}_{i_1}) \neq 0$$

for some $\mathbf{x} \in S_{d+1}$. Choose i_1 minimal. Since $\mathfrak{F}(\mathbf{x})$ assumes integral values on Λ , the bilinear form $\mathfrak{F}(\mathbf{x}, \mathbf{y})$ assumes values in $\frac{1}{2}\mathbf{Z}$ for \mathbf{x}, \mathbf{y} in Λ . Hence by (36) either

$$|\mathfrak{F}(\mathbf{x}_i, \mathbf{p}_{i_1})| \geq \frac{1}{2} \quad \text{for some } i \ (1 \leq i \leq d)$$

or

$$|\mathfrak{F}(\mathbf{p}_1, \mathbf{p}_{i_1})| \geq \frac{1}{2}.$$

Any of these two inequalities together with (35) imply

$$(37) \quad F|\mathbf{p}_1| |\mathbf{p}_{i_1}| \gg 1.$$

If (37) holds with $i_1 = 2$, then (25) and (26) are true with $l = 1$.

So we may assume $i_1 > 2$. Our next task then is to deal with \mathbf{p}_2 . Since i_1 in (36) was chosen minimal we have

$$(38) \quad \mathfrak{F}(\mathbf{x}, \mathbf{z}_2) = 0 \quad \text{for all } \mathbf{x} \in S_{d+1}.$$

Notice that (38) and (29) imply

$$(39) \quad \mathfrak{F}(\mathbf{z}_2) = \mathfrak{F}(\mathbf{p}_2) \in \mathbf{Z}.$$

We distinguish two cases:

Either

$$(40) \quad \mathfrak{F}(\mathbf{z}_2) = \mathfrak{F}(\mathbf{p}_2) \neq 0$$

or

$$(41) \quad \mathfrak{F}(\mathbf{z}_2) = \mathfrak{F}(\mathbf{p}_2) = 0.$$

If (40) holds, we have again (25) and (26) with $l = 1$. If (38) holds together with (41) then \mathfrak{F} vanishes on the $(d+2)$ -dimensional subspace S_{d+2} generated by $\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{z}_1, \mathbf{z}_2$. Since rank $\mathfrak{F} > n-d$, there is an $i_2 \in \{3, 4, \dots, n-d-1\}$, $i_2 \neq i_1$ such that

$$(42) \quad \mathfrak{F}(\mathbf{x}, \mathbf{z}_{i_2}) \neq 0 \quad \text{for some } \mathbf{x} \in S_{d+2}.$$

Notice that (42) is completely analogous to (36). In conjunction with (29) and (35) it yields

$$(43) \quad F|\mathbf{p}_2| |\mathbf{p}_{i_2}| \gg 1,$$

which is of the same type as the inequality (37). It is clear that by repeating our procedure in the same way as after (37) and collecting all inequalities of the type (37) and (43) we finally obtain the assertion of Lemma 3.

The proof of Theorem 1 is now finished easily. By (23) and Lemma 3 we have

$$(44) \quad |\mathbf{p}_{n-d}| \ll F^{(n-d-1)/2} \Delta (\det \Gamma_0)^{-1}.$$

Define vectors $\mathbf{p}'_1, \dots, \mathbf{p}'_{n-d}$ by

$$(45) \quad \mathbf{p}'_j = \begin{cases} \mathbf{p}_j & \text{if there exists an } \mathbf{x} \in \Gamma_0 \text{ with } \mathfrak{F}(\mathbf{x}, \mathbf{p}_j) \neq 0 \\ \mathbf{p}_j + \mathbf{p}_r & \text{otherwise, where } r \text{ is defined in (31)} \end{cases} \quad (1 \leq j \leq n-d).$$

We have

$$(46) \quad |\mathbf{p}'_j| \ll |\mathbf{p}_{n-d}| \quad (1 \leq j \leq n-d),$$

moreover the basis $\mathbf{x}_1, \dots, \mathbf{x}_d$ of Γ_0 together with $\mathbf{p}'_1, \dots, \mathbf{p}'_{n-d}$ as defined in (45) generate E^n . There exist points

$$\mathbf{z}'_j = \lambda'_{1j} \mathbf{x}_1 + \dots + \lambda'_{dj} \mathbf{x}_d + \mathbf{p}'_j \in \Lambda \quad (j = 1, \dots, n-d)$$

with suitable real coefficients λ'_{ij} , just as in (30).

For $j = 1, \dots, n-d$ consider the lattice Λ'_j generated by Γ_0 and \mathbf{z}'_j . We may apply the Proposition. Since $\mathfrak{F}(\Gamma_0, \mathbf{z}'_j) \neq 0$ we are in case (i) of Lemma 1, and there are two primitive sublattices of Λ'_j on which the restriction of \mathfrak{F} to Λ'_j vanishes. One is Γ_0 , let Γ_j be the other one. According to the Proposition we have

$$\det \Gamma_0 \det \Gamma_j \ll (\det \Lambda'_j)^2 F = (\det \Gamma_0)^2 |\mathbf{p}'_j|^2 F.$$

We now use (44) and (46) to get

$$\det \Gamma_0 \det \Gamma_j \ll \Delta^2 F^{n-d}$$

which is (9). Finally, it is clear from our construction that $\Gamma_0 \cap \Gamma_j$ has dimension $d-1$. Since $\Gamma_0, \Gamma_1, \dots, \Gamma_{n-d}$ span $\Gamma_0, \mathbf{p}'_1, \dots, \mathbf{p}'_{n-d}$, they also span E^n .

4. Proof of Theorem 2. There exist a diagonal matrix D with entries ± 1 and a nonsingular matrix A such that the matrix associated with \mathfrak{F} is $A^t D A$. The diagonal form $\hat{\mathfrak{F}}(\mathbf{X}) = \mathfrak{F}(A^{-1} \mathbf{X})$ assumes integral values on the lattice $A\Lambda$. If $\mathbf{y}_1, \dots, \mathbf{y}_n$ are linearly independent zeros of $\hat{\mathfrak{F}}$ on $A\Lambda$ satisfying

$$|\det(\mathbf{y}_1, \dots, \mathbf{y}_n)| \ll |\det \hat{\mathfrak{F}}|^{(n-d)/2d} (\det(A\Lambda))^{n/d} = |\det A|^{n/d} \Delta^{n/d},$$

then the vectors $\mathbf{x}_1 = A^{-1} \mathbf{y}_1, \dots, \mathbf{x}_n = A^{-1} \mathbf{y}_n$ are linearly independent zeros of \mathfrak{F} in Λ and we have

$$\begin{aligned} |\det(\mathbf{x}_1, \dots, \mathbf{x}_n)| &= |\det A|^{-1} |\det(\mathbf{y}_1, \dots, \mathbf{y}_n)| \\ &\ll |\det A|^{(n-d)/d} \Delta^{n/d} = |\det \mathfrak{F}|^{(n-d)/2d} \Delta^{n/d}. \end{aligned}$$

Therefore we may assume in the remainder of the paper that \mathfrak{F} has diagonal matrix with entries ± 1 . In particular this implies

$$(48) \quad F \gg \ll 1.$$

As in §3 let Γ_0 be a d -dimensional sublattice of Λ on which \mathfrak{F} vanishes and whose determinant is minimal. Let $\mathbf{x}_1, \dots, \mathbf{x}_d$ be a basis of Γ_0 as in (27). Moreover we consider again a basis $\mathbf{p}_1, \dots, \mathbf{p}_{n-d}$ of the projection of Λ on the $(n-d)$ -dimensional subspace perpendicular to Γ_0 . Recall that for $\mathbf{p}_1, \dots, \mathbf{p}_{n-d}$ we have (23) and (24).

LEMMA 4. *If \mathfrak{F} has rank n , then $|\mathbf{p}_1| \cdots |\mathbf{p}_{n-2d}| \gg 1$.*

PROOF. The proof goes along the same lines as that of Lemma 3. The only difference is that we have $\text{rank } \mathfrak{F} = n$, which gives

$$|\mathbf{p}_1| \cdots |\mathbf{p}_{n-2d}| \gg F^{-(n-2d)/2}.$$

The assertion now follows from (48).

Since $\text{rank } \mathfrak{F} = n$, there exists for any j ($1 \leq j \leq d$) an i_j ($i \leq i_j \leq n - d$) with

$$(49) \quad \mathfrak{F}(\mathbf{x}_j, \mathbf{p}_{i_j}) \neq 0$$

and such that moreover $i_j \neq i_k$ for $j \neq k$. Using (23), (24) and (28) we obtain in view of Lemma 4 that

$$(50) \quad |\mathbf{x}_1| \cdots |\mathbf{x}_d| \cdot |\mathbf{p}_{i_1}| \cdots |\mathbf{p}_{i_d}| \leq |\mathbf{x}_1| \cdots |\mathbf{x}_d| \cdot |\mathbf{p}_{n-2d+1}| \cdots |\mathbf{p}_{n-d}| \ll \Delta.$$

In general, the subscripts i_1, \dots, i_d are not ordered according to increasing size. However there is a permutation σ of $\{1, \dots, d\}$ such that the subscripts i_1, \dots, i_d we obtain from $\mathbf{x}_{\sigma(1)}, \dots, \mathbf{x}_{\sigma(d)}$ in that order satisfy

$$(51) \quad i_1 < i_2 < \cdots < i_d.$$

So (50) may be written as

$$(52) \quad |\mathbf{x}_{\sigma(1)}| \cdots |\mathbf{x}_{\sigma(d)}| \cdot |\mathbf{p}_{i_1}| \cdots |\mathbf{p}_{i_d}| \ll \Delta.$$

In particular (52) implies that there exists a k with $1 \leq k \leq d$ and

$$(53) \quad |\mathbf{x}_{\sigma(k)}| |\mathbf{p}_{n-2d+k}| \ll \Delta^{1/d}.$$

On the other hand we have by (24) and (51)

$$(54) \quad |\mathbf{p}_{i_k}| \leq |\mathbf{p}_{n-2d+k}|.$$

We now define vectors $\mathbf{p}''_1, \dots, \mathbf{p}''_{n-d}$ as follows.

For $j = 1, \dots, n - 2d$ we put

$$(55) \quad \mathbf{p}''_j = \begin{cases} \mathbf{p}_j & \text{if } \mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{p}_j) \neq 0, \\ \mathbf{p}_j + \mathbf{p}_{i_k} & \text{if } \mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{p}_j) = 0, \end{cases}$$

whereas for $j = n - 2d + l$ ($l = 1, \dots, d$) we put

$$(56) \quad \mathbf{p}''_j = \begin{cases} \mathbf{p}_j & \text{if } \mathfrak{F}(\mathbf{x}_{\sigma(l)}, \mathbf{p}_j) \neq 0, \\ \mathbf{p}_j + \mathbf{p}_{i_l} & \text{if } \mathfrak{F}(\mathbf{x}_{\sigma(l)}, \mathbf{p}_j) = 0. \end{cases}$$

Notice that (54) and (55) imply

$$(57) \quad |\mathbf{p}''_j| \ll |\mathbf{p}_{n-2d+k}| \quad (j = 1, \dots, n - 2d).$$

Similarly we obtain from (56)

$$(58) \quad |\mathbf{p}''_{n-2d+i}| \ll |\mathbf{p}_{n-2d+i}| \quad (i = 1, \dots, d).$$

The definition (55), (56) shows moreover that $\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{p}''_1, \dots, \mathbf{p}''_{n-d}$ are linearly independent. As in §3 we can find vectors $\mathbf{z}''_1, \dots, \mathbf{z}''_{n-d} \in \Lambda$ of the shape

$$(59) \quad \mathbf{z}''_\nu = \lambda''_{1\nu} \mathbf{x}_1 + \cdots + \lambda''_{d\nu} \mathbf{x}_d + \mathbf{p}''_\nu$$

with real coefficients $|\lambda''_{i\nu}| \leq \frac{1}{2}$ ($1 \leq i \leq d, 1 \leq \nu \leq n - d$).

We next define points $\mathbf{y}_1, \dots, \mathbf{y}_{n-d} \in \Lambda$ by

$$(60) \quad \mathbf{y}_\nu = \mathfrak{F}(\mathbf{z}_\nu'')\mathbf{x}_{\sigma(k)} - 2\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{z}_\nu'')\mathbf{z}_\nu'' \quad (1 \leq \nu \leq n - 2d),$$

$$(61) \quad \mathbf{y}_{n-2d+i} = \mathfrak{F}(\mathbf{z}_{n-2d+i}'')\mathbf{x}_{\sigma(i)} - 2\mathfrak{F}(\mathbf{x}_{\sigma(i)}, \mathbf{z}_{n-2d+i}'')\mathbf{z}_{n-2d+i}'' \quad (1 \leq i \leq d).$$

It follows from (55), (56), (59), (60), (61) and the fact that \mathfrak{F} vanishes on Γ_0 that $\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{y}_1, \dots, \mathbf{y}_{n-d}$ are linearly independent. For the points in (60) we have

$$\mathfrak{F}(\mathbf{y}_\nu) = -4\mathfrak{F}(\mathbf{z}_\nu'') (\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{z}_\nu''))^2 + 4\mathfrak{F}(\mathbf{z}_\nu'') (\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{z}_\nu''))^2 = 0,$$

and similiary for the points defined by (61).

As for the determinant of $\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{y}_1, \dots, \mathbf{y}_{n-d}$ we obtain

$$(62) \quad \begin{aligned} & |\det(\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{y}_1, \dots, \mathbf{y}_{n-d})| \\ &= |\det(\mathbf{x}_1, \dots, \mathbf{x}_d, 2\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{z}_1'')\mathbf{z}_1'', \dots, 2\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{z}_{n-2d}'')\mathbf{z}_{n-2d}'', \\ &\quad 2\mathfrak{F}(\mathbf{x}_{\sigma(1)}, \mathbf{z}_{n-2d+1}'')\mathbf{z}_{n-2d+1}'', \dots, 2\mathfrak{F}(\mathbf{x}_{\sigma(d)}, \mathbf{z}_{n-d}'')\mathbf{z}_{n-d}'')| \\ &= 2^{n-d} |\det(\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{z}_1'', \dots, \mathbf{z}_{n-d}'')| \prod_{\nu=1}^{n-2d} |\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{z}_\nu'')| \prod_{i=1}^d |\mathfrak{F}(\mathbf{x}_{\sigma(i)}, \mathbf{z}_{n-2d+i}'')| \\ &= 2^{n-d} |\det(\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{p}_1, \dots, \mathbf{p}_{n-d})| \prod_{\nu=1}^{n-2d} |\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{z}_\nu'')| \prod_{i=1}^d |\mathfrak{F}(\mathbf{x}_{\sigma(i)}, \mathbf{z}_{n-2d+i}'')|. \end{aligned}$$

Here we have used elementary matrix operations, together with (55), (56), (59), (60) and (61).

(23) and (28) imply

$$(63) \quad |\det(\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{p}_1, \dots, \mathbf{p}_{n-d})| = \Delta.$$

On the other hand by (59), (57), (48) and (53) we have

$$(64) \quad |\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{z}_\nu'')| = |\mathfrak{F}(\mathbf{x}_{\sigma(k)}, \mathbf{p}_\nu'')| \ll |\mathbf{x}_{\sigma(k)}| \cdot |\mathbf{p}_{n-2d+k}| \ll \Delta^{1/d} \quad (1 \leq \nu \leq n - 2d).$$

From (59), (58), (48) and (50) we infer that

$$(65) \quad \begin{aligned} & \prod_{i=1}^d |\mathfrak{F}(\mathbf{x}_{\sigma(i)}, \mathbf{z}_{n-2d+i}'')| \\ &= \prod_{i=1}^d |\mathfrak{F}(\mathbf{x}_{\sigma(i)}, \mathbf{p}_{n-2d+i}'')| \ll \prod_{i=1}^d |\mathfrak{F}(\mathbf{x}_{\sigma(i)}, \mathbf{p}_{n-2d+i})| \\ &\ll |\mathbf{x}_1| \cdots |\mathbf{x}_d| |\mathbf{p}_{n-2d+1}| \cdots |\mathbf{p}_{n-d}| \ll \Delta. \end{aligned}$$

Combining (62), (63), (64) and (65) we get

$$|\det(\mathbf{x}_1, \dots, \mathbf{x}_d, \mathbf{y}_1, \dots, \mathbf{y}_{n-d})| \ll \Delta^{(n-2d)/d} \cdot \Delta \cdot \Delta = \Delta^{n/d}.$$

REFERENCES

1. B. J. Birch and H. Davenport, *Quadratic equations in several variables*, Proc. Cambridge Philos. Soc. **54** (1958), 135–138.
2. J. W. S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Philos. Soc. **51** (1955), 262–264.

3. —, *Addendum to the paper: Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Philos. Soc. **52** (1956), 604.
4. H. Davenport, *Homogeneous quadratic equations*, Mathematika **18** (1971), 1–4.
5. H. P. Schlickewei, *Kleine Nullstellen homogener quadratischer Gleichungen*, Monatsh. Math. **100** (1985), 35–45.
6. R. Schulze-Pillot, *Small linearly independent zeros of quadratic forms*, Monatsh. Math. **95** (1983), 241–249.

ABTEILUNG MATHEMATIK II DER UNIVERSITÄT ULM, OBERER ESELSBERG, D-7900 ULM, WEST GERMANY (Current address of H. P. Schlickewei)

SCHOOL OF MATHEMATICS, THE INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540

Current address (W. M. Schmidt): Department of Mathematics, University of Colorado, Boulder, Colorado 80309-0426