ACTA ARITHMETICA
XV (1969)

# A problem of Schinzel on lattice points

by

WOLFGANG M. SCHMIDT (Boulder, Colo.)

**1.** THEOREM. *Let $\Lambda$ be a lattice of integer points in Euclidean $E^n$ and let $\Lambda^+$ be the set of lattice points with nonnegative coordinates. There exists a finite set $S$ of points of $\Lambda^+$ such that every point $\boldsymbol{g}$ of $\Lambda^+$ may be written*

$$\boldsymbol{g} = c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n \tag{1}$$

*with $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ in $S$ and with nonnegative integer coefficients $c_1, \ldots, c_n$.*

The truth of this theorem had been conjectured by Schinzel, who proved the case $n = 2$ by means of continued fractions [1]. He originally wanted to use the theorem to prove results on polynomials, but later found a way to avoid it.

Notation. Write $E^t$ for the coordinate plane consisting of points $(x_1, \ldots, x_t, 0, \ldots, 0)$ and $E^{t+}$ for the subset of $E^t$ when $x_1 \geqslant 0, \ldots, x_t \geqslant 0$. We also shall write $E^+ = E^{n+}$. Let $K^+$ be the set of points $\boldsymbol{x} \in E^+$ with length $|\boldsymbol{x}| = 1$.

$\boldsymbol{B} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ will be called a *basis* of $\Lambda^+$ if $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ lie in $\Lambda^+$ and form a basis of $\Lambda$. Given such a basis $\boldsymbol{B}$, let $C(\boldsymbol{B})$ be the cone consisting of the points

$$\boldsymbol{x} = \lambda_1\boldsymbol{u}_1 + \ldots + \lambda_r\boldsymbol{u}_n \tag{2}$$

with nonnegative coefficients $\lambda_i$. If a lattice point $\boldsymbol{g}$ lies in $C(\boldsymbol{B})$, then these coefficients will be integers.

Hence the following proposition will suffice for the proof of our theorem.

PROPOSITION 1. *There are finitely many bases $\boldsymbol{B}_1, \ldots, \boldsymbol{B}_m$ of $\Lambda^+$ such that*

$$\bigcup_{i=1}^{m} C(\boldsymbol{B}_i) = E^+. \tag{3}$$

The case $n = 1$ of Proposition 1 is obvious; we may then take $m = 1$. We shall derive the case of dimension $n$ from the case $n-1$.

---

[1] In the course of the proof of Lemma 5 of *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), pp. 1-34.

By homogeneity it will suffice to find bases $\boldsymbol{B}_1, \dots, \boldsymbol{B}_m$ such that

$$\bigcup_{i=1}^{m} C(\boldsymbol{B}_i)$$

covers $K^+$. Now $K^+$ is compact, and hence it will be enough to show that every $\boldsymbol{x}$ in $K^+$ is contained in a neighborhood $N(\boldsymbol{x})$ in $K^+$ which is open with respect to $K^+$ and which is contained in a finite union of sets $C(\boldsymbol{B})$.

Using homogeneity again we infer that it will suffice to prove the following proposition.

PROPOSITION 2. *Every $\boldsymbol{x} \neq 0$ in $E^+$ is contained in a neighborhood $N(\boldsymbol{x})$ in $E^+$ which is open with respect to $E^+$ and which is contained in a finite union of cones $C(\boldsymbol{B})$.*

**2.** We now proceed to prove Proposition 2 when $\boldsymbol{x}$ is not contained in an $(n-1)$-dimensional rational subspace. In particular, $\boldsymbol{x}$ does not lie in a coordinate plane.

Consider $n$-tuples of linearly independent points $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ of $\Lambda^+$ such that

(4) $$\boldsymbol{x} = \lambda_1 \boldsymbol{u}_1 + \dots + \lambda_n \boldsymbol{u}_n \quad \text{with} \quad \lambda_1 > 0, \dots, \lambda_n > 0.$$

There do in fact exist such $n$-tuples: Let $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ be points of $\Lambda^+$ which lie on the positive coordinate axes. Such points exist since $\Lambda$ is a sublattice of the integer lattice. Since all the coordinates of $\boldsymbol{x}$ are positive, $\boldsymbol{x}$ has a representation as in (4) with positive coefficients.

Let $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ be an $n$-tuple of this type such that the absolute value of the determinant $|\boldsymbol{u}_1, \dots, \boldsymbol{u}_n|$ is least possible. We claim that $\boldsymbol{B} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ is a basis of $\Lambda^+$.

Otherwise, there would be a point $\boldsymbol{u}' \neq 0$ in $\Lambda$ with

$$\boldsymbol{u}' = \mu_1 \boldsymbol{u}_1 + \dots + \mu_n \boldsymbol{u}_n$$

and $0 \leqslant \mu_i < 1$ $(i = 1, \dots, n)$. We may assume without loss of generality that $\mu_1 > 0, \dots, \mu_s > 0$, $\mu_{s+1} = \dots = \mu_n = 0$. We may further assume that

$$\lambda_1/\mu_1 \leqslant \lambda_2/\mu_2 \leqslant \dots \leqslant \lambda_s/\mu_s$$

where $\lambda_1, \dots, \lambda_s$ are given by (4).

The points $\boldsymbol{u}', \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ are linearly independent. A short computation shows that

$$\boldsymbol{x} = \lambda_1' \boldsymbol{u}' + \lambda_2' \boldsymbol{u}_2 + \dots + \lambda_n' \boldsymbol{u}_n$$

with

$$\lambda_1' = \lambda_1/\mu_1, \qquad \lambda_i' = \mu_i \left( \frac{\lambda_i}{\mu_i} - \frac{\lambda_1}{\mu_1} \right) \quad (2 \leqslant i \leqslant s),$$

$$\lambda_i' = \lambda_i \quad (s < i \leqslant n).$$



Hence the coefficients $\lambda_j'$ are nonnegative, and since $\boldsymbol{x}$ lies in no rational subspace, they are in fact positive. Moreover, the absolute value of $|\boldsymbol{u}', \boldsymbol{u}_2, \dots, \boldsymbol{u}_n|$ is smaller than the absolute value of $|\boldsymbol{u}_1, \dots, \boldsymbol{u}_n|$, and this contradicts the choice of $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$.

Hence $\boldsymbol{B} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ is in fact a basis of $\Lambda^+$ and by (4) $\boldsymbol{x}$ lies in the interior of $C(\boldsymbol{B})$. Hence there is a neighborhood $N(\boldsymbol{x})$ of $\boldsymbol{x}$ which is contained in $C(\boldsymbol{B})$.

**3.** Now suppose $\boldsymbol{x}$ is contained in an $(n-1)$-dimensional rational subspace, but in no $(n-1)$-dimensional coordinate plane. Let $k$ be the smallest integer such that $\boldsymbol{x}$ lies in a $k$-dimensional rational subspace $R^k$ but in no $(k-1)$-dimensional such space. We have

(5) $$1 \leqslant k \leqslant n-1.$$

Let $R^{k+} = R^k \cap E^+$. Since $\boldsymbol{x}$ is in the interior of $E^+$, there is a neighborhood $M^k(\boldsymbol{x})$ of $\boldsymbol{x}$ in $R^k$ which is contained in $R^{k+}$. Suppose $R^k$ is spanned by points $\boldsymbol{q}_1, \dots, \boldsymbol{q}_k$ of $\Lambda$. The points

$$\boldsymbol{r} = r_1 \boldsymbol{q}_1 + \dots + r_k \boldsymbol{q}_k$$

with rational coefficients $r_i$ are dense in $R^k$. Hence there are $k$ linearly independent such points $\boldsymbol{r}_1, \dots, \boldsymbol{r}_k$ in $M^k(\boldsymbol{x})$ such that

$$\boldsymbol{x} = \nu_1 \boldsymbol{r}_1 + \dots + \nu_k \boldsymbol{r}_k$$

with positive coefficients $\nu_1, \dots, \nu_k$. Each $\boldsymbol{r}_i$ is a positive rational multiple of a lattice point $\boldsymbol{u}_i$ in $R^{k+}$, and we may write

(6) $$\boldsymbol{x} = \lambda_1 \boldsymbol{u}_1 + \dots + \lambda_k \boldsymbol{u}_k$$

with positive $\lambda_1, \dots, \lambda_k$. By an argument used in § 2 above there are in fact points $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ of $R^{k+}$ which form a basis of the lattice $\Lambda^k = R^k \cap \Lambda$ of $R^k$ such that (6) holds with positive $\lambda_1, \dots, \lambda_k$.

Since $\boldsymbol{x}$ has positive coordinates, so does

$$\boldsymbol{y} = \langle \lambda_1 \rangle \boldsymbol{u}_1 + \dots + \langle \lambda_k \rangle \boldsymbol{u}_k \text{ (2)}.$$

It is possible to choose $\boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_n$ such that

$$(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_n)$$

is a basis of $\Lambda$. Choose the integer $t$ so large that the $2(n-k)$ points

$$\pm \boldsymbol{v}_{k+1} + t\boldsymbol{y}, \; \dots, \; \pm \boldsymbol{v}_n + t\boldsymbol{y}$$

have positive coordinates. For each choice of sign $\pm$, the points

(7) $$\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \; \pm \boldsymbol{v}_{k+1} + t\boldsymbol{y}, \dots, \; \pm \boldsymbol{v}_n + t\boldsymbol{y}$$

form a basis $\boldsymbol{B}$ of $\Lambda^+$. There are $2^{n-k}$ such bases.

(2) $\langle a \rangle$ denotes the integer $g$ with $a \leqslant g < a+1$.

An arbitrary point $z$ may be written

$$z = \mu_1 u_1 + \ldots + \mu_k u_k + \mu_{k+1} v_{k+1} + \ldots + \mu_n v_n.$$

An easy computation shows that

$$z = \sum_{i=1}^{k} \Big(\mu_i - t\langle\lambda_i\rangle \sum_{j=k+1}^{n} |\mu_j|\Big) u_i + \sum_{i=k+1}^{n} |\mu_i| (\pm v_i + ty), \tag{8}$$

with $+v_i$ if $\mu_i$ is positive and $-v_i$ otherwise. Recall that $\lambda_1, \ldots, \lambda_k$ are positive. If $z$ is close to $x$ then $\mu_1, \ldots, \mu_k$ will be close to $\lambda_1, \ldots, \lambda_k$, respectively, and $\mu_{k+1}, \ldots, \mu_n$ will be small. Therefore in this case the coefficients in (8) will be nonnegative and $z$ will be in a cone $C(B)$ where $B$ is one of the bases (7).

Hence there is a neighborhood of $x$ which is contained in the union of the $2^{n-k}$ cones $C(B)$ with $B$ of the type (7).

**4.** Finally we consider the case when $n$ lies in a coordinate plane. We may assume that $x$ lies in $E^t$ where

$$1 \leqslant t \leqslant n-1, \tag{9}$$

but in no (t—1)-dimensional plane. Hence $x = (x_1, \ldots, x_t, 0, \ldots, 0)$ with $x_1 > 0, \ldots, x_t > 0$.

Let $F$ be the orthogonal complement of $E^t$; it consists of points $y = (0, \ldots, 0, y_{t+1}, \ldots, y_n)$. Further let $F^+ = F \cap E^+$. Given $\varepsilon$ with $0 < \varepsilon < \min(x_1, \ldots, x_t)$, the points

$$z = z_1 + z_2 \tag{10}$$

with $z_1 \epsilon E^t$, $z_2 \epsilon F^+$ and with $|z_1 - x| < \varepsilon$, $|z_2| < \varepsilon$ form a neighborhood $N_\varepsilon(x)$ of $x$ in $E^+$.

Let $\Lambda^t$ be the lattice $\Lambda \cap E^t$ in $E^t$, and let $\Lambda^{t+} = \Lambda^t \cap E^+$. By the inductive assumption there are bases

$$B_1^t, \ldots, B_l^t$$

of $\Lambda^{t+}$ such that

$$\bigcup_{i=1}^{l} C(B_i^t) = E^{t+}.$$

Let $\Lambda^*$ be the orthogonal projection of $\Lambda$ on $F$; it is a lattice in $F$ consisting of integer points. Further put $\Lambda^{*+} = \Lambda^* \cap E^+$. Again by the induction there are bases

$$B_1^*, \ldots, B_m^*$$

in $\Lambda^{*+}$ such that

$$\bigcup_{j=1}^{m} C(B_j^*) = F^+.$$



Suppose $B_i^t = (u_1^{(i)}, \ldots, u_t^{(i)})$ and suppose $B_j^*$ consists of orthogonal projections of $v_{t+1}^{(j)}, \ldots, v_n^{(j)}$. Then $(u_1^{(i)}, \ldots, u_t^{(i)}, v_{t+1}^{(j)}, \ldots, v_n^{(j)})$ is a basis of $\Lambda$. The vectors $u_r^{(i)}$ lie in $\Lambda^+$, and the last $n-t$ coordinates of the vectors $v_s^{(j)}$ are nonnegative. By adding a suitable lattice point of $\Lambda^{t+}$ to each $v_s^{(j)}$ we may in fact assume that

$$B_{i,j} = (u_1^{(i)}, \ldots, u_t^{(i)}, v_{t+1}^{(j)}, \ldots, v_n^{(j)}) \tag{11}$$

is a basis of $\Lambda^+$.

Now suppose that $z$ is of the type (10) and lies in $N_\varepsilon(x)$. The vector $z_2$ is in some cone $C(B_j^*)$. Hence there are nonnegative reals $\lambda_{t+1}, \ldots, \lambda_n$ such that

$$z_0 = z_2 - \lambda_{t+1} v_{t+1}^{(j)} - \ldots - \lambda_n v_n^{(j)}$$

lies in $E^t$. If $\varepsilon$ is small, then so will be $\lambda_{t+1}, \ldots, \lambda_n$, and hence $|z_0|$ will be small. For sufficiently small $\varepsilon$ and $z \epsilon N_\varepsilon(x)$ we shall have

$$|z_0| < \tfrac{1}{2}\min(x_1, \ldots, x_t) \quad \text{and} \quad |z_1 - x| < \tfrac{1}{2}\min(x_1, \ldots, x_t).$$

Therefore the first $t$ coordinates of $z_0 + z_1$ will be positive, and $z_0 + z_1$ will lie in $C(B_i^t)$ for some $B_i^t$. Therefore

$$z_0 + z_1 = \lambda_1 u_1^{(i)} + \ldots + \lambda_t u_t^{(i)}$$

with nonnegative coefficients $\lambda_1, \ldots, \lambda_t$. We therefore get

$$z = z_1 + z_2 = \lambda_1 u_1^{(i)} + \ldots + \lambda_t u_t^{(i)} + \lambda_{t+1} v_{t+1}^{(j)} + \ldots + \lambda_n v_n^{(j)}.$$

This shows that $z$ lies in $C(B_{i,j})$.

Thus for sufficiently small $\varepsilon$, the neighborhood $N_\varepsilon(x)$ is contained in the union of the $lm$ cones $C(B_{i,j})$.

This finishes the proof of our theorem.

*Reçu par la Rédaction le 4. 5. 1968*