A problem of Schinzel on lattice points

by

WOLFGANG M. SCHMIDT (Boulder, Colo.)

1. Theorem. Let \( A \) be a lattice of integer points in Euclidean \( E^n \) and let \( A^+ \) be the set of lattice points with nonnegative coordinates. There exists a finite set \( S \) of points of \( A^+ \) such that every point \( g \) of \( A^+ \) may be written

\[
 g = c_1 u_1 + \ldots + c_n u_n
\]

with \( u_1, \ldots, u_n \) 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 \( E^d \) for the coordinate plane consisting of points \((x_1, \ldots, x_d, 0, \ldots, 0)\) and \( E^d^+ \) for the subset of \( E^d \) when \( x_1 \geq 0, \ldots, x_d \geq 0 \). We also shall write \( E^+ = E^d^+ \). Let \( E^+ \) be the set of points \( x \in E^d^+ \) with length \( |x| = 1 \).

\[ B = (u_1, \ldots, u_n) \]

will be called a basis of \( A^+ \) if \( u_1, \ldots, u_n \) lie in \( A^+ \) and form a basis of \( A \). Given such a basis \( B \), let \( C(B) \) be the cone consisting of the points

\[
x = \lambda_1 u_1 + \ldots + \lambda_n u_n
\]

with nonnegative coefficients \( \lambda_1 \). If a lattice point \( g \) lies in \( C(B) \), 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 \( B_1, \ldots, B_m \) of \( A^+ \) such that

\[
 \bigcup_{i=1}^{m} C(B_i) = E^+.
\]

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 (1966), pp. 1-34.
By homogeneity it will suffice to find bases \( B_1, \ldots, B_n \) such that
\[
\bigcup_{i=1}^n C(B_i)
\]
covers \( K^+ \). Now \( K^+ \) is compact, and hence it will be enough to show that every \( x \) in \( K^+ \) is contained in a neighborhood \( N(x) \) in \( K^+ \) which is open with respect to \( K^+ \) and which is contained in a finite union of sets \( C(B) \).

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

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

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

Consider \( n \)-tuples of linearly independent points \( u_1, \ldots, u_n \) of \( A^+ \) such that
\[
x = \lambda_1 u_1 + \cdots + \lambda_n u_n \quad \text{with} \quad \lambda_1 > 0, \ldots, \lambda_n > 0.
\]

There do in fact exist such \( n \)-tuples: Let \( u_1, \ldots, u_n \) be points of \( A^+ \) which lie on the positive coordinate axes. Such points exist since \( A \) is a sublattice of the integer lattice. Since all the coordinates of \( x \) are positive, \( x \) has a representation as in (4) with positive coefficients.

Let \( u_1, \ldots, u_n \) be an \( n \)-tuple of this type such that the absolute value of the determinant \( |u_1, \ldots, u_n| \) is least possible. We claim that \( B = (u_1, \ldots, u_n) \) is a basis of \( A^* \).

Otherwise, there would be a point \( u' \neq 0 \) in \( A \) with
\[
u' = \mu_1 u_1 + \cdots + \mu_n u_n
\]
and \( 0 < \mu_i < 1 \) \((i = 1, \ldots, n)\). We may assume without loss of generality that \( \mu_1 > 0, \ldots, \mu_s > 0, \mu_{s+1} = \cdots = \mu_n = 0 \). We may further assume that
\[
\lambda_1/|u_1| \leq \lambda_2/|u_2| \leq \cdots \leq \lambda_s/|u_s|
\]
where \( \lambda_1, \ldots, \lambda_s \) are given by (4).

The points \( u', u_2, \ldots, u_n \) are linearly independent. A short computation shows that
\[
x = \lambda'_1 u' + \lambda'_2 u_2 + \cdots + \lambda'_n u_n
\]
with
\[
\lambda'_i = \lambda_i/\mu_i, \quad \lambda'_s = \mu_s (1 - \lambda_s/\mu_s) \quad (2 \leq i \leq s), \quad \lambda'_s = \lambda_s \quad (s < i \leq n).
\]

Hence the coefficients \( \lambda'_i \) are nonnegative, and since \( x \) lies in no rational subspace, they are in fact positive. Moreover, the absolute value of \( |u', u_2, \ldots, u_n| \) is smaller than the absolute value of \( |u_1, \ldots, u_n| \), and this contradicts the choice of \( u_1, \ldots, u_n \).

Hence \( B = (u_1, \ldots, u_n) \) is in fact a basis of \( A^+ \) and by (4) \( x \) lies in the interior of \( C(B) \). Hence there is a neighborhood \( N(x) \) of \( x \) which is contained in \( C(B) \).

3. Now suppose \( x \) 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 \( x \) lies in a \( k \)-dimensional rational subspace \( R^k \) but in no \((k-1)\)-dimensional such space. We have
\[
1 < k < n - 1.
\]

Let \( R^k = E^k \cap E^+ \). Since \( x \) is in the interior of \( E^+ \), there is a neighborhood \( N(x) \) of \( x \) in \( R^k \) which is contained in \( R^k \). Suppose \( R^k \) is spanned by points \( q_1, \ldots, q_k \) of \( A \). The points
\[
r = r_1 q_1 + \cdots + r_k q_k
\]
with rational coefficients \( r_i \) are dense in \( R^k \). Hence there are \( k \) linearly independent such points \( r_1, \ldots, r_k \) in \( M^1(x) \) such that
\[
x = r_1 q_1 + \cdots + r_k q_k
\]
with positive coefficients \( r_1, \ldots, r_k \). Each \( r_i \) is a positive rational multiple of a lattice point \( u_i \) in \( R^k \), and we may write
\[
x = \lambda_1 u_1 + \cdots + \lambda_k u_k
\]
with positive \( \lambda_1, \ldots, \lambda_k \). By an argument used in §2 above there are in fact points \( u_1, \ldots, u_k \) of \( R^k \) which form a basis of the lattice \( A^* = R^k \cap A \) of \( R^k \) such that (6) holds with positive \( \lambda_1, \ldots, \lambda_k \).

Since \( x \) has positive coordinates, so does
\[
y = \langle \lambda \rangle u_1 + \cdots + \langle \lambda \rangle u_k \quad (3).
\]

It is possible to choose \( v_1, \ldots, v_k \) such that
\[
(u_1, \ldots, u_k, v_1, \ldots, v_k)
\]
is a basis of \( A \). Choose the integer \( k \) so large that the \( 2(n-k) \) points
\[
\pm v_1 + y, \ldots, \pm v_k + y
\]
have positive coordinates. For each choice of sign \( \pm \), the points
\[
u_1, \ldots, u_k, \pm v_1 + y, \ldots, \pm v_k + y
\]
form a basis \( B \) of \( A^+ \). There are \( 2^{n-k} \) such bases.

(3) \( \langle \lambda \rangle \) denotes the integer \( g \) with \( a < g < a + 1 \).
An arbitrary point $\mathbf{z}$ may be written

$$\mathbf{z} = \mu_1 \mathbf{u}_1 + \cdots + \mu_n \mathbf{u}_n + \mu_{n+1} \mathbf{v}_{n+1} + \cdots + \mu_k \mathbf{v}_k.$$

An easy computation shows that

$$\mathbf{z} = \sum_{i=1}^{k} (\mu_i - 1) \mathbf{u}_i + \sum_{i=k+1}^{n} |\mu_i| \mathbf{v}_i \pm \mathbf{y},$$

with $+ \mathbf{v}_i$ if $\mu_i$ is positive and $- \mathbf{v}_i$ otherwise. Recall that $\lambda_1, \ldots, \lambda_k$ are positive. If $\mathbf{z}$ is close to $\mathbf{x}$ 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 $\mathbf{z}$ will be in a cone $C(\mathbf{B})$ where $\mathbf{B}$ is one of the bases (7).

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

4. Finally we consider the case when $\mathbf{z}$ lies in a coordinate plane. We may assume that $\mathbf{z}$ lies in $E^t$ where

$$1 \leq t \leq n - 1,$$

but in no $(t-1)$-dimensional plane. Hence $\mathbf{x} = (x_1, \ldots, x_t, 0, \ldots, 0)$ 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

$$\mathbf{z} = \mathbf{x} + \varepsilon \mathbf{e}_t$$

with $x_t e^F$, $x_t e^F$ and with $|\mathbf{z} - \mathbf{x}| < \varepsilon$, $|\mathbf{z}| < \varepsilon$ form a neighborhood $N(\mathbf{x})$ of $\mathbf{x}$ in $E^t$.

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

$$\mathbf{B}_1, \ldots, \mathbf{B}_i$$

of $A^{t*}$ such that

$$\bigcup_{i=1}^{t} C(\mathbf{B}_i) = E^t.$$

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

$$\mathbf{B}_1, \ldots, \mathbf{B}_n$$

in $A^{t*}$ such that

$$\bigcup_{i=1}^{n} C(\mathbf{B}_i) = E^+. $$

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

$$\mathbf{B}_i = (u_1^{(i)}, \ldots, u_n^{(i)}, v_{t+1}^{(i)}, \ldots, v_n^{(i)})$$

is a basis of $A^*$.

Now suppose that $\mathbf{z}$ is of the type (10) and lies in $N(\mathbf{x})$. The vector $\mathbf{z}$ is in some cone $C(\mathbf{B}_i)$. Hence there are nonnegative reals $\lambda_1, \ldots, \lambda_n$ such that

$$\mathbf{z} = \mathbf{x} - \lambda_1 e_1^{(i)} - \cdots - \lambda_n e_n^{(i)}$$

lies in $E^t$. If $\varepsilon$ is small, then so will be $\lambda_1, \ldots, \lambda_n$, and hence $|z_n|$ will be small. For sufficiently small $\varepsilon$ and $\mathbf{z} \in N(\mathbf{x})$ we shall have

$$|z_n| < \varepsilon \min(x_1, \ldots, x_t) \quad \text{and} \quad |\mathbf{z} - \mathbf{x}| < \varepsilon \min(x_1, \ldots, x_t).$$

Therefore the first $t$ coordinates of $\mathbf{z}$ will be positive, and $\mathbf{z} \in C(\mathbf{B}^t)$ for some $\mathbf{B}^t$. Therefore

$$\mathbf{z} = \lambda_1 u_1^{(i)} + \cdots + \lambda_n u_n^{(i)}$$

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

$$\mathbf{z} = \mathbf{x} + \mathbf{z} = \lambda_1 u_1^{(i)} + \cdots + \lambda_n u_n^{(i)} + \lambda_1 v_{t+1}^{(i)} + \cdots + \lambda_n v_n^{(i)}.$$

This shows that $\mathbf{z}$ lies in $C(\mathbf{B}_i)$.

Thus for sufficiently small $\varepsilon$, the neighborhood $N(\mathbf{x})$ is contained in the union of the $\mathbf{B}_i$ cones $C(\mathbf{B}_i)$.

This finishes the proof of our theorem.

Reçu par la Rédaction le 4.6.1968.