Math. J. Okayama Univ. **58** (2016), 141–158

ALTERNATIVE APPROACH FOR SIEGEL'S LEMMA

Makoto Nagata

Abstract. In this article, we present an alternative approach to show a generalization of Siegel's lemma which is an essential tool in Diophantine problems. Our main statement contains the so-called analytic Siegel's lemma as well as the Bombieri-Vaaler lemma. Our proof avoids relying on the ordinary geometry of numbers.

1. Introduction

Let T be a linear subspace of the n-dimensional Euclidean space $\mathbb{R}^n$. When T is defined over the rational number field $\mathbb{Q}$ or over an algebraic number field, the original Siegel's lemma [8] states that there exists a nontrivial integral point in T whose norm is bounded. Bombieri and Vaaler [2] established a generalization of Siegel's lemma where they introduced the notion of height of the linear subspace T. An analytic version of Siegel's lemma due to Philippon and Waldschmidt [5] is also known, where the assumption does not include algebraicity, namely it is not needed that T is defined over $\mathbb{Q}$ or an algebraic number field. Instead, it is only required that the defining equation of T has coefficients which are sufficiently near by rational numbers or algebraic numbers.

In this article, we present an alternative approach aimed to a generalization of Siegel's lemma which essentially contains both the statement by Bombieri-Vaaler and that by Philippon-Waldschmidt.

Siegel's lemma is characterized by three keywords: vector space, linear equation, and restriction of solutions. Our proof seems to rely on the same objects; however, our approach is different from the original one towards Siegel's lemma. Indeed, we first introduce an *infinite*-dimensional vector space with an inner product. Next, we consider *linear equations* whose coefficients are obtained from T, and then, we restrict our attention to solutions in a *sphere* in the vector space.

The following simple proposition plays a crucial role in introducing an infinite-dimensional vector space to prove a finiteness argument. Let V be a vector space over $\mathbb{R}$ and let $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$ be an inner product of V. For a fixed nonzero $u \in V$, we set $S(u) := \{x \in V \mid \langle x, u - x\rangle = 0\}$.

Proposition 1. *Let N be a positive integer and let $x_1, \ldots, x_N \in S(u)$ with $\langle x_i, x_j\rangle = 0$ for $1 \le i < j \le N$. Then there exists an element $w \in S(u)$ such*

Mathematics Subject Classification. Primary 11D04; Secondary 11J13.

Key words and phrases. Siegel's lemma, geometry of numbers, height.

that

$$\langle u, u\rangle = \langle w, w\rangle + \sum_{i=1}^{N}\langle x_i, x_i\rangle.$$

Here the set $S(u)$ is a sphere whose zero vector and u are the north and south poles, respectively. We assume that the inner product $\langle\ ,\ \rangle$ is positive definite. In this case, even if the dimension of V is not finite, Proposition 1 provides a finite bound.

This article is organized as follows: In section 1.1, we specify the infinite-dimensional vector space V and the sphere. We introduce a symbol $\tilde{H}_\epsilon^{m,n}$ which plays the role of height. In section 1.2, we present our main result, i.e., Theorem 1 (our version of Siegel's lemma) and the first application supplying information concerning the base field of T (Theorem 2). In section 1.3, we deduce from our Theorem 1 both the above-mentioned analytic Siegel's lemma (Corollary 1) and Bombieri-Vaaler lemma (Corollary 2). In section 2.1, we introduce our basic tool to avoid using the ordinary geometry of numbers. This section is devoted to an estimation so as to cover the role of Minkowski's theorem related to successive minima which was employed in [2, 9]. In section 2.2, we collect some lemmas that we need in later sections, and we also give a simple proof of Proposition 1. In section 3.1, we give a proof of Theorem 1, and in section 3.2 that of Corollary 1. In section 3.3, a proof of Theorem 2 is presented. In section 3.4, we show Corollary 2.

1.1. **Settings.** Let $E = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ be a fixed orthonormal basis of $\mathbb{R}^n$ and let $\mathbb{Z}^n$ be the lattice group by E; $\mathbb{Z}^n := \mathbb{Z}\mathbf{e}_1 + \cdots + \mathbb{Z}\mathbf{e}_n$. We use the symbol $|\ \ |_\infty$ for the L^∞-norm on E; $\big|\sum_{i=1}^{n}\alpha_i\mathbf{e}_i\big|_\infty = \max_{i=1,\ldots,n}|\alpha_i|$. We consider the canonical n-dimensional torus group $\Omega := \mathbb{R}^n/\mathbb{Z}^n$ with the usual topology. We put $\pi : \mathbb{R}^n \to \Omega$ as the standard projection such that $\mathrm{Ker}(\pi) = \mathbb{Z}^n$. Let P be the Haar measure of the Hausdorff compact topological abelian group Ω with $P(\Omega) = 1$, that is, the usual one induced by the Lebesgue measure.

Let V be the linear space over $\mathbb{R}$ of bounded measurable functions on Ω:

$$V = \{X : \Omega \to \mathbb{R} \mid X \text{ is a bounded measurable function}\}.$$

In other words, $X \in V$ is a random variable on Ω with the probability measure P. We also define a natural inner product on the linear space V to $\mathbb{R}$ by

$$\langle X, Y\rangle = \int_\Omega XY\,dP$$

for $X, Y \in V$.

Let $\mathbf{1} \in V$ be the function identically 1 on Ω, i.e., $\mathbf{1}(\omega) = 1$ for all $\omega \in \Omega$, and let $S(\mathbf{1}) = \{Y \in V \mid \langle Y, \mathbf{1} - Y\rangle = 0\}$ be the sphere.

For $Y \in S(\mathbf{1})$, $m, n \in \mathbb{Z}_{\geq 0}$, and a real $\epsilon > 0$, we put

$$\tilde{H}_{\epsilon}^{m,n}(Y) := \frac{1 - \langle Y, Y\rangle}{\epsilon^{n-m}} + \epsilon^{m}.$$

This value will play the role of height in our results.

To state our results, we need a few notations. For a real ϵ with $0 < \epsilon < 1/2$, $A(\epsilon) = \big\{\mathbf{x} \in \mathbb{R}^n \bigm| |\mathbf{x}|_\infty < \epsilon/2\big\}$ denotes the ϵ-cube. For $\mathbf{p} \in \mathbb{R}^n$, let $X_\epsilon^{\mathbf{p}} \in V$ be the characteristic function of the image of π of the $\mathbf{p}$-translation of $A(\epsilon)$, that is,

$$X_\epsilon^{\mathbf{p}}(\omega) = \begin{cases} 1 & \text{if } \omega \in \pi(A(\epsilon) + \mathbf{p}), \\ 0 & \text{otherwise} \end{cases}$$

where $A(\epsilon) + \mathbf{p} = \{\mathbf{a} + \mathbf{p} \mid \mathbf{a} \in A(\epsilon)\}$. Let $Z(\epsilon) = \{\mathbf{a} + \mathbf{b} \mid \mathbf{a} \in A(2\epsilon), \mathbf{b} \in \mathbb{Z}^n, \mathbf{b} \neq 0\}$.

1.2. **Results.** Theorems 1 and 2 stated below are our main results. We note that they are *analytic*, that is, we do not assume that the linear subspace T is defined over an algebraic number field.

Theorem 1. *Let l, m, n be integers with $1 \leq l \leq m < n$, and let ϵ be a real number with $0 < \epsilon < 1/2$. Let T be a linear subspace of $\mathbb{R}^n$ with $m = \dim_{\mathbb{R}} T$. Suppose that $Y \in S(\mathbf{1})$ satisfies $\langle X_\epsilon^{\mathbf{p}}, Y\rangle = 0$ for all $\mathbf{p} \in T$, where Y may depend on ϵ. Then the following hold:*

(i) There exist l points $\mathbf{z}_1(\epsilon), \dots, \mathbf{z}_l(\epsilon)$ in $\mathbb{R}^n$ with

$$\sum_{i=1}^{l} \log |\mathbf{z}_i(\epsilon)|_\infty \leq \frac{l}{m} \log \tilde{H}_{\epsilon}^{m,n}(Y) + C_{l,m,n}$$

such that $\mathbf{z}_i(\epsilon) \in T \cap Z(\epsilon)$ for $i = 1, \dots, l$, where $C_{l,m,n}$ is a constant independent of ϵ, T, Y, and $\mathbf{z}_1(\epsilon), \dots, \mathbf{z}_l(\epsilon)$.

(ii) Consider the case $l = m$. Let $\epsilon_1 > \epsilon_2 > \epsilon_3 > \dots \searrow 0$ be a decreasing sequence converging to 0 with $\epsilon_1 < 1/2$, and let $\mathfrak{S}$ be the set of all m-tuples $(\mathbf{z}_i(\epsilon_k))_{i=1,\dots,m}$ in (i);

$$\mathfrak{S} := \{(\mathbf{z}_1(\epsilon_k), \dots, \mathbf{z}_m(\epsilon_k)) \mid k = 1, 2, \dots\} \subset \mathbb{R}^{n\times m}.$$

Assume that

$$\limsup_{\epsilon \to +0} \inf_{Y \in S(\mathbf{1})} \{\tilde{H}_{\epsilon}^{m,n}(Y) \mid \langle X_\epsilon^{\mathbf{p}}, Y\rangle = 0 \textit{ for all } \mathbf{p} \in T\}$$

is finite. Then there exists an accumulating point $(\boldsymbol{\zeta}_i)_{i=1,\dots,m}$ of $\mathfrak{S}$ such that $\boldsymbol{\zeta}_1, \dots, \boldsymbol{\zeta}_m$ are linearly independent over $\mathbb{R}$.

Theorem 2. *Let T be a linear subspace of $\mathbb{R}^n$ with $m = \dim_{\mathbb{R}} T$ for $1 \leq m < n$. Then the following are equivalent.*

(I) $\limsup_{\epsilon \to +0} \inf_{Y \in S(\mathbf{1})} \{\tilde{H}_\epsilon^{m,n}(Y) \mid \langle X_\epsilon^{\mathbf{p}}, Y\rangle = 0$ *for all* $\mathbf{p} \in T\} < \infty$

(II) T is defined over $\mathbb{Q}$.

As mentioned in the Introduction, if we call " $\langle X_\epsilon^{\mathbf{p}}, Y\rangle = 0$ for all $\mathbf{p} \in T$ " a system of linear equations whose coefficients are obtained from T, we can say that $Y \in V$ is a solution of this system. Then we restrict our attention to solutions in the sphere $S(\mathbf{1})$. This is our approach for Siegel's lemma.

Remark 1. For only Part (i) of Theorem 1, one can choose the constant as

$$C_{l,m,n} = \begin{cases} l \log n & \text{if } l = 1, 2, \\ l \log n + \dfrac{(l-1)l(l+3)}{2m} \log(l-1) & \text{if } l = 3, \ldots, m. \end{cases} \tag{1}$$

However in order to validate Part (ii), we need another constant $C_{l,m,n}$, denoted by C' in our proof below, which is slightly larger than (1) for technical reasons.

1.3. **Siegel's lemma and the geometry of numbers.** The geometry of numbers, namely, the *ordinary* geometry of numbers (e.g., the Euclidean geometry of numbers and the adelic geometry of numbers, which utilize the volume of convex bodies), is an essential tool for the height type in [2, 9]. The height of a linear subspace defined over an algebraic number field is the volume of a certain convex body, and this fact allows the best use of the geometry of numbers. Philippon and Waldschmidt [5] used the pigeonhole principle; however, it is not difficult to imagine that their analytic type can be also proved by means of the geometry of numbers. For the relation between Siegel's lemma and the geometry of numbers, one can refer to [6]. There is no doubt that the geometry of numbers is an important principle underlying Siegel's lemma.

In this article, we introduce a tool (Lemma 1 below) instead of the ordinary geometry of numbers. No volume appears, that is, Lemma 1 requires only discrete conditions. Our proof of Theorem 1 relies on this tool. Furthermore Theorem 1, a hybrid of the analytic and the height type, leads to both types as the following Corollaries 1 and 2. Our approach needs the Lebesgue measure; however, our proof avoids relying on the ordinary geometry of numbers.

Now let $(\ ,\ )$ be the standard inner product on $\mathbb{R}^n$.

Corollary 1. (see [5]) *Let m and n be integers with $1 \leq m < n$ and let $\mathbf{a}_1, \ldots, \mathbf{a}_{n-m} \in \mathbb{R}^n$ be linearly independent over $\mathbb{R}$ with absolute values $M := \max_{i=1,\ldots,n-m} |\mathbf{a}_i|_\infty$. Then for a given real $\epsilon_0 > 0$, there exists a nontrivial* *lattice point* $\mathbf{z} \in \mathbb{Z}^n$ *with*

$$\log |\mathbf{z}|_\infty \leq \frac{n-m}{m} \log \frac{M}{\epsilon_0} + C_1$$

such that $|(\mathbf{a}_i, \mathbf{z})| < \epsilon_0$ *for* $i = 1, \ldots, n-m$. *Here* $C_1 = (n \log n)/m + ((m+1)\log 2)/m$.

Corollary 2. ([2] see also [9]) *With the same hypotheses as in Corollary 1, assume that* $\mathbf{a}_1, \ldots, \mathbf{a}_{n-m} \in \mathbb{Z}^n \subset \mathbb{R}^n$. *Let*

$$T_{\mathbb{Q}} = \{\mathbf{x} \in \mathbb{Q}^n \mid (\mathbf{a}_i, \mathbf{x}) = 0 \ \ for \ \ i = 1, \ldots, n-m\}.$$

Suppose that the rank of $T_{\mathbb{Q}} \cap \mathbb{Z}^n$ *over* $\mathbb{Z}$ *is* m. *Then there exist* m *linearly independent lattice points* $\mathbf{z}_1, \ldots, \mathbf{z}_m \in \mathbb{Z}^n$ *with*

$$\sum_{i=1}^{m} \log |\mathbf{z}_i|_\infty \leq \log H(T_{\mathbb{Q}}) + C_2.$$

Here $H(T_{\mathbb{Q}})$ *is the height of the linear subspace* $T_{\mathbb{Q}}$ *and the constant* C_2 *is independent of the height and* $\mathbf{z}_1, \ldots, \mathbf{z}_m$.

Remark 2. Part (i) of Theorem 1 holds even for the trivial solution $Y = 0$ (identically 0). It leads to Corollary 1. Note that the analytic Siegel's lemma in [5] was considered over the complex number field. If ϵ_0 tends to 1, Corollary 1 immediately gives the original Siegel's lemma (see [8] and [1]). In this case, it is known that C_1 is improved as $((n-m)\log n)/m$ in [1]. Our estimation of the error term $C_{l,m,n}$ in Theorem 1 is not sharp, and therefore neither C_1 nor C_2 is. It is important to note that Bombieri and Vaaler [2] obtained $C_2 = 0$. They also obtained the height type for the case of general algebraic number fields.

Some readers may be concerned that there are different versions of the definition of (the ordinary) height depending on the norm chosen at the Archimedean places. However this affects only the constant term C_2. We use the usual L^2-norm at the Archimedean places. See [2], [6] and [7] for the definition of height. In this article, we follow Schmidt in Ch. 3 of [7]; essentially, it is the same as that given as in [2].

2. Preliminaries

2.1. **Alternative tool and its estimation.** Here we introduce our tool instead of the ordinary geometry of numbers.

Let G be an abelian group and let Q be a subset of G. We call Q symmetric if $\sigma \in Q$ implies that $-\sigma \in Q$. For a nonempty subset H of G, we write $H - H = \{\sigma - \sigma' \mid \sigma, \sigma' \in H\}$. For a given real number γ, inevitably greater than 1, we will consider a subset Q of G satisfying the following:

(Condition A)
For arbitrary finite subset H of G, if $\#H \geq \gamma$ then $(H-H) \cap Q \neq \{0\}$.

Here $\#H$ denotes the cardinality of H. We always assume that $0 \in Q$.

The following Lemma 1 is our alternative tool. Only discrete conditions appear.

Lemma 1. *Let l and m be integers with $1 \leq l \leq m$. Suppose that a symmetric subset Q of the abelian group $G = \mathbb{Z}^m$ satisfies Condition A with a given real γ. Then there exist l elements $\boldsymbol{\rho}_1, \dots, \boldsymbol{\rho}_l \in Q$ which are linearly independent over $\mathbb{Z}$ such that*

$$\sum_{i=1}^{l} \log |\boldsymbol{\rho}_i|_\infty \leq \frac{l}{m} \left(\log \gamma + C(l) \right),$$

where $|\boldsymbol{\rho}|_\infty := \max_{i=1,\dots,m} |a_i|$ for $\boldsymbol{\rho} = (a_1, \dots, a_m) \in \mathbb{Z}^m$ and $C(l)$ is a constant dependent only on l. More precisely, $C(1) = C(2) = 0$ and $C(l) = ((l-1)(l+3)\log(l-1))/2$ for $l \geq 3$.

To show Lemma 1 we use the following:

Lemma 2. *Let l be an integer with $l \geq 2$. Let $r_1, \dots, r_l$, $\delta_2, \dots, \delta_l$ be real numbers with $0 < r_1 \leq r_2 \leq \cdots \leq r_l$ and with $0 < \delta_i \leq 1$ for $i = 2, \dots, l$. Suppose that a real $l \times l$ matrix $B = (a_{i,j})_{i,j=1,\dots,l}$ satisfies $|a_{i,i}| = r_i$ for $i = 1, \dots, l$ and*

$$|a_{i,j}| \leq \begin{cases} r_i \delta_j & \text{if } i < j, \\ r_j & \text{if } i > j. \end{cases}$$

If $\sum_{i=2}^{l} \delta_i (i-1)^{(i+1)/2} < 1$, then $\det B \neq 0$.

Proof of Lemma 2. We write $B_m = (a_{i,j})_{i,j=1,\dots,m}$ for $m = 1, \dots, l$. Let D_i be the (i,l)-cofactor of $B = B_l$, that is, the submatrix obtained by deleting the i-th row and the l-th column of B. By the assumptions, the absolute values of elements in the k-th column do not exceed r_k. By Hadamard's inequality we have

$$|\det D_i| \leq \sqrt{l-1}\, r_1 \cdots \sqrt{l-1}\, r_{l-1} = (l-1)^{(l-1)/2} r_1 \cdots r_{l-1}.$$

The cofactor expansion of $\det B_l$ gives that

$$\begin{aligned} |\det B_l| &= \left| r_l \det B_{l-1} + \sum_{i=1}^{l-1} (-1)^{l+i} a_{i,l} \det D_i \right| \\ &\geq r_l \, |\det B_{l-1}| - \sum_{i=1}^{l-1} r_i \delta_l \, |\det D_i| \\ &\geq |\det B_{l-1}| \, r_l - \delta_l (l-1)^{(l-1)/2} r_1 \cdots r_{l-1} \sum_{i=1}^{l-1} r_i. \end{aligned}$$

Now for $i = 2, \ldots, l$, put

$$\epsilon_i = \delta_i (i-1)^{(i-1)/2} \sum_{j=1}^{i-1} \frac{r_j}{r_i}, \quad b_i = |\det B_i| \, (r_1 \cdots r_i)^{-1}.$$

Then $b_l \geq b_{l-1} - \epsilon_l$. Similarly, $b_i \geq b_{i-1} - \epsilon_i$ for $i = 2, \ldots, l$. Consequently, if $l \geq 3$, we obtain

$$b_l \geq b_{l-1} - \epsilon_l \geq b_{l-2} - \epsilon_{l-1} - \epsilon_l \geq \cdots \geq b_2 - \sum_{i=3}^{l} \epsilon_i.$$

Since $\epsilon_2 = \delta_2 r_1 / r_2$ and since $r_1 r_2 b_2 = |\det B_2| \geq r_1 r_2 - \delta_2 r_1^2 = r_1 r_2 (1 - \epsilon_2)$, it follows that

$$b_l \geq 1 - \sum_{i=2}^{l} \epsilon_i$$

for $l = 2, 3, \ldots$. The assumption $r_i \leq r_{i+1}$ implies $\sum_{j=1}^{i-1} r_j / r_i \leq i - 1$. Therefore we have $\epsilon_i \leq \delta_i (i-1)^{(i-1)/2} (i-1)$ and

$$b_l \geq 1 - \sum_{i=2}^{l} \delta_i (i-1)^{(i+1)/2}.$$

This proves the lemma. □

Proof of Lemma 1. For $i = 1, \ldots, m$, we denote $\pi_i : \mathbb{R}^m \to \mathbb{R}$ by the standard projections, i.e., for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{R}^m$, $\pi_i(\boldsymbol{\alpha}) = \alpha_i$. Let $\mathbb{Z}^m$ be the canonical full-rank lattice group in $\mathbb{R}^m$.

Let $\mathbb{R}^m_{\geq 0}$ be the set of non-negative real coordinates vectors. For a vector $\boldsymbol{\beta} \in \mathbb{R}^m_{\geq 0}$, we write

$$C(\boldsymbol{\beta}) = \{ \mathbf{a} \in \mathbb{Z}^m \mid 0 \leq \pi_i(\mathbf{a}) \leq \pi_i(\boldsymbol{\beta}) \ \text{ for } \ i = 1, \ldots, m \}.$$

Then $\#C(\boldsymbol{\beta}) = \prod_{i=1}^{m}(\lfloor \pi_i(\boldsymbol{\beta}) \rfloor + 1) \geq \prod_{i=1}^{m} \pi_i(\boldsymbol{\beta})$, where $\lfloor \pi_i(\boldsymbol{\beta}) \rfloor$ denotes the integer not exceed $\pi_i(\boldsymbol{\beta})$. Moreover, for $\mathbf{a}$, $\mathbf{b} \in C(\boldsymbol{\beta})$ and for $i = 1, \dots, m$, we have $|\pi_i(\mathbf{a} - \mathbf{b})| \leq \pi_i(\boldsymbol{\beta})$ since $0 - \pi_i(\boldsymbol{\beta}) \leq \pi_i(\mathbf{a} - \mathbf{b}) \leq \pi_i(\boldsymbol{\beta}) - 0$.

Now let $\boldsymbol{\beta}^{(1)}$ be in $\mathbb{R}^m_{\geq 0}$ with $\pi_i(\boldsymbol{\beta}^{(1)}) = \gamma^{1/m}$ for $i = 1, \dots, m$. We first consider $C(\boldsymbol{\beta}^{(1)})$. Since $\#C(\boldsymbol{\beta}^{(1)}) \geq \prod_{i=1}^{m} \pi_i(\boldsymbol{\beta}^{(1)}) = \gamma$, there exist $\mathbf{a}$, $\mathbf{b} \in C(\boldsymbol{\beta}^{(1)}) \subset G = \mathbb{Z}^m$ with $0 \neq \mathbf{a} - \mathbf{b} \in Q$ by the assumptions. That is, the set $D_1 := \{\boldsymbol{\rho} \in Q \setminus \{0\} \mid |\pi_i(\boldsymbol{\rho})| \leq \pi_i(\boldsymbol{\beta}^{(1)}) = \gamma^{1/m} \text{ for } i = 1, \dots, m\}$ is not empty. We choose an element in D_1 such that the value of $|\ \ |_\infty$ is minimum, and we denote it by $\boldsymbol{\rho}_1$. Set $r_1 = |\boldsymbol{\rho}_1|_\infty$. Since it is in D_1, $1 \leq r_1 \leq \gamma^{1/m}$. We can assume, by exchanging coordinates of $\mathbb{R}^m$ if necessary, that $|\pi_1(\boldsymbol{\rho}_1)| = r_1$. Furthermore we can assume that $\pi_1(\boldsymbol{\rho}_1) = r_1$ since Q is symmetric. We thus conclude that Lemma 1 holds for $l = 1$ with $C(1) = 0$.

For $l = 2, \dots, m$, we now consider real numbers $\delta_2, \dots, \delta_l$ satisfying

$$0 < \delta_l \leq \cdots \leq \delta_2 < 1 \text{ and } \sum_{i=2}^{l} \delta_i (i-1)^{(i+1)/2} < 1. \tag{2}$$

Here let $\boldsymbol{\beta}^{(2)}$ be in $\mathbb{R}^m_{\geq 0}$ with $\pi_1(\boldsymbol{\beta}^{(2)}) = r_1\delta_2$ and with $\pi_i(\boldsymbol{\beta}^{(2)}) = (\gamma/(r_1\delta_2))^{1/(m-1)}$ for $i = 2, \dots, m$. We next consider $C(\boldsymbol{\beta}^{(2)})$. Again, since $\#C(\boldsymbol{\beta}^{(2)}) \geq \prod_{i=1}^{m} \pi_i(\boldsymbol{\beta}^{(2)}) = \gamma$, there exist $\mathbf{a}$, $\mathbf{b} \in C(\boldsymbol{\beta}^{(2)})$ with $0 \neq \mathbf{a} - \mathbf{b} \in Q$. That is $D_2 := \{\boldsymbol{\rho} \in Q \setminus \{0\} \mid |\pi_i(\boldsymbol{\rho})| \leq \pi_i(\boldsymbol{\beta}^{(2)}) \text{ for } i = 1, \dots, m\}$ is not empty. We choose an element in D_2 such that the value of $|\ \ |_\infty$ is minimum, and we denote it by $\boldsymbol{\rho}_2$. Set $r_2 = |\boldsymbol{\rho}_2|_\infty$. If $r_2 < r_1$, then $r_2 \leq \gamma^{1/m}$ by $r_1 \leq \gamma^{1/m}$. It follows that $\boldsymbol{\rho}_2 \in D_1$. This contradicts the minimality of $|\boldsymbol{\rho}_1|_\infty$. Therefore $r_1 \leq r_2$. Here we have $r_2 = |\boldsymbol{\rho}_2|_\infty \leq \max(r_1\delta_2, (\gamma/(r_1\delta_2))^{1/(m-1)})$. By $r_1 \leq r_2$ and by $\delta_2 < 1$, it follows that $r_1\delta_2 < r_2$. Thus $r_2 \leq (\gamma/(r_1\delta_2))^{1/(m-1)}$, that is,

$$\delta_2 r_1 r_2^{m-1} \leq \gamma.$$

Since Q is symmetric, we can assume, by exchanging coordinates of $\mathbb{R}^m$ except the first index if necessary, that $|\pi_1(\boldsymbol{\rho}_2)| \leq r_1\delta_2$, $\pi_2(\boldsymbol{\rho}_2) = r_2$ and that $|\pi_i(\boldsymbol{\rho}_2)| \leq r_2$ for $i = 3, \dots, m$.

Now we consider the case of $l = 2$. For any $0 < \delta_2 < 1$, the rank of the matrix formed from $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$ is 2 by Lemma 2; hence they are linearly independent over $\mathbb{R}$.

Since the values of r_1 and r_2 are discrete on δ_2, one sees that there exist $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$ such that $r_1 r_2^{m-1} \leq \gamma$ in the case of $\delta_2 = 1 - \delta$ for sufficiently small positive $\delta > 0$.

By $(\log r_1 + \log r_2) + (m-2)\log r_2 \leq \log\gamma$ and by $\log r_1 + \log r_2 \leq 2\log r_2$, it follows that $(1+\frac{m-2}{2})(\log r_1+\log r_2)\le \log\gamma$. That is

$$\log r_1+\log r_2\le \frac{2}{m}\log\gamma.$$

This shows that Lemma 1 holds for $l=2$ with $C(2)=0$.

We now proceed by induction. For a natural number k with $3\le k\le l$, we define $\boldsymbol{\beta}^{(k-1)}\in\mathbb{R}^m_{\ge 0}$ by $\pi_1(\boldsymbol{\beta}^{(k-1)})=r_1\delta_{k-1}$, $\pi_2(\boldsymbol{\beta}^{(k-1)})=r_2\delta_{k-1}$, …, $\pi_{k-2}(\boldsymbol{\beta}^{(k-1)})=r_{k-2}\delta_{k-1}$ and by

$$\pi_i(\boldsymbol{\beta}^{(k-1)})=(\gamma/(r_1r_2\cdots r_{k-2}\delta_{k-1}^{k-2}))^{1/(m-(k-2))}$$

for $i=k-1,\dots,m$. We now assume the following (1-i)–(1-iii):

(1-i) the set $D_{k-1}:=\{\boldsymbol{\rho}\in Q\setminus\{0\}\mid |\pi_i(\boldsymbol{\rho})|\le\pi_i(\boldsymbol{\beta}^{(k-1)})\ \text{ for }\ i=1,\dots,m\}$ is not empty.

(1-ii) we can choose an element in D_{k-1} such that the value of $|\cdot|_\infty$ is minimum, and we denote it by $\boldsymbol{\rho}_{k-1}$. Set $r_{k-1}=|\boldsymbol{\rho}_{k-1}|_\infty$. Then $r_{k-1}=\pi_{k-1}(\boldsymbol{\rho}^{(k-1)})$ and $r_1\le r_2\le\cdots\le r_{k-1}$ hold.

(1-iii) the inequality $\delta_{k-1}^{k-2}r_1r_2\cdots r_{k-2}r_{k-1}^{m-(k-2)}\le\gamma$ holds.

One sees that these three assumptions hold for $k=3$. Note that the last inequality is equivalent to

$$r_{k-1}\le\pi_{k-1}(\boldsymbol{\beta}^{(k-1)}).\tag{3}$$

Now we define $\boldsymbol{\beta}^{(k)}\in\mathbb{R}^m_{\ge 0}$ by $\pi_1(\boldsymbol{\beta}^{(k)})=r_1\delta_k$, $\pi_2(\boldsymbol{\beta}^{(k)})=r_2\delta_k$, …, $\pi_{k-1}(\boldsymbol{\beta}^{(k)})=r_{k-1}\delta_k$ and by $\pi_i(\boldsymbol{\beta}^{(k)})=(\gamma/(r_1r_2\cdots r_{k-1}\delta_k^{k-1}))^{1/(m-(k-1))}$ for $i=k,\dots,m$. We consider the set $C(\boldsymbol{\beta}^{(k)})$. Since $\#C(\boldsymbol{\beta}^{(k)})\ge\prod_{i=1}^m\pi_i(\boldsymbol{\beta}^{(k)})$ $=\gamma$, there exist $\mathbf{a}$, $\mathbf{b}\in C(\boldsymbol{\beta}^{(k)})$ with $0\ne\mathbf{a}-\mathbf{b}\in Q$. That is, the set $D_k:=\{\boldsymbol{\rho}\in Q\setminus\{0\}\mid|\pi_i(\boldsymbol{\rho})|\le\pi_i(\boldsymbol{\beta}^{(k)})\ \text{ for }\ i=1,\dots,m\}$ is not empty. We choose an element in D_k such that the value of $|\cdot|_\infty$ is minimum, and we denote it by $\boldsymbol{\rho}_k$, set $r_k=|\boldsymbol{\rho}_k|_\infty$. We now show that $r_{k-1}\le r_k$. Assume the negation: $r_k<r_{k-1}$. By $\boldsymbol{\rho}_k\in D_k$, we have $|\pi_i(\boldsymbol{\rho}_k)|\le r_i\delta_k\le r_i\delta_{k-1}=\pi_i(\boldsymbol{\beta}^{(k-1)})$ for $i=1,\dots,k-2$. Noting the assumption (3) we have $|\pi_{k-1}(\boldsymbol{\rho}_k)|\le r_k<r_{k-1}\le\pi_{k-1}(\boldsymbol{\beta}^{(k-1)})$ for $i=k-1$. Moreover one sees that $|\pi_i(\boldsymbol{\rho}_k)|\le r_k<r_{k-1}\le\pi_{k-1}(\boldsymbol{\beta}^{(k-1)})=\pi_i(\boldsymbol{\beta}^{(k-1)})$ holds for $i=k,k+1,\dots,m$. That is, $\boldsymbol{\rho}_k\in D_{k-1}$, which contradicts the minimality of $|\rho_{k-1}|_\infty$. Therefore $r_{k-1}\le r_k$, i.e., $r_1\le r_2\le\cdots\le r_{k-1}\le r_k$.

We can assume, by changing the $k,\dots,m$-th coordinates of $\mathbb{R}^m$ if necessary, that $r_k=\pi_k(\boldsymbol{\rho}_k)$. Since $r_k=|\boldsymbol{\rho}_k|_\infty\le\max(r_1\delta_k,r_2\delta_k,\dots,r_{k-1}\delta_k,$ $(\gamma/(r_1r_2\cdots r_{k-1}\delta_k^{k-1}))^{1/(m-(k-1))})$, the conditions $r_1\le r_2\le\cdots\le r_k$ and $\delta_k\le\cdots\le\delta_2<1$ give that $r_k\le(\gamma/(r_1r_2\cdots r_{k-1}\delta_k^{k-1}))^{1/(m-(k-1))}$, i.e., $\delta_k^{k-1}r_1r_2\cdots r_{k-1}r_k^{m-(k-1)}\le\gamma$.

By induction on k, we obtain $r_1 \le r_2 \le \cdots \le r_{l-1} \le r_l$ and

$$\delta_l^{l-1} r_1 r_2 \cdots r_{l-1} r_l^{m-(l-1)} \le \gamma. \tag{4}$$

Lemma 2 and the condition (2) show that the matrix formed from $\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_l$ has the full rank, hence $\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_l$ are linearly independent over $\mathbb{R}$. Note that $\sum_{i=1}^{l} \log r_i \le l \log r_l$. Again by (4) and since

$$(l-1)\log\delta_l + \sum_{i=1}^{l} \log r_i + (m-l)\log r_l \le \log\gamma,$$

we have

$$(l-1)\log\delta_l + \left(1 + \frac{m-l}{l}\right) \sum_{i=1}^{l} \log r_i \le \log\gamma.$$

Therefore

$$\sum_{i=1}^{l} \log r_i \le \frac{l}{m}\left(\log\gamma + (l-1)\log(1/\delta_l)\right) \tag{5}$$

holds. Recall that the condition (2) about $\delta_2, \ldots, \delta_l$. So for any sufficient small positive $\delta > 0$, the inequality (5) holds in the case of

$$\delta_l = \delta_{l-1} = \cdots = \delta_2 = \left(\sum_{i=2}^{l} (i-1)^{(i+1)/2}\right)^{-1} - \delta.$$

Furthermore, since the left-hand side in the inequality (5) is discrete on δ, one sees that the estimation in Lemma 1

$$\sum_{i=1}^{l} \log r_i \le \frac{l}{m}\left(\log\gamma + (l-1)\log\sum_{i=2}^{l}(i-1)^{(i+1)/2}\right)$$

holds for sufficiently small $\delta > 0$. Finally, we have $\sum_{i=2}^{l}(i-1)^{(i+1)/2} \le (l-1)\cdot(l-1)^{(l+1)/2} = (l-1)^{(l+3)/2}$ since the value $(i-1)^{(i+1)/2}$ is increasing on $i = 2, 3, \ldots$. Therefore we conclude that Lemma 1 holds for $l = 3, \ldots, m$ with $C(l)$. □

2.2. **Some lemmas.** We now give a proof of Proposition 1 as Lemma 3 below in a slightly generalized form. By abuse of notation, we use the same letters employed in the preceding sections. Let V and K be abelian groups and let $\langle\ ,\ \rangle : V \times V \to K$ be a bilinear mapping as $\mathbb{Z}$-modules. We will use the symbols $+, -$ and 0 in the usual sense. For a fixed nonzero $u \in V$, we put $S(u) = \{x \in V \mid \langle x, u-x\rangle = \langle u-x, x\rangle = 0\}$.

Lemma 3. *Let N be a positive integer and let $x_1, \dots, x_N$ be in $S(u)$ with $\langle x_i, x_j\rangle = 0$ for $i, j = 1, \dots, N$, $i \neq j$. Then there exists an element $w \in S(u)$ such that*

$$\langle u, u\rangle = \langle w, w\rangle + \sum_{i=1}^{N} \langle x_i, x_i\rangle.$$

Proof. For $x \in V$, we abbreviate $\langle x, x\rangle$ to $\langle x\rangle$. Put $w = u - \sum_{i=1}^{N} x_i$. We claim that $w \in S(u)$ and that $\langle u\rangle = \langle w\rangle + \sum_{i=1}^{N}\langle x_i\rangle$. Since $\langle x_i, x_j\rangle = 0$ for $i \neq j$, we have

$$\langle w, u - w\rangle = \langle u, \sum_{i=1}^{N} x_i\rangle - \langle \sum_{i=1}^{N} x_i, \sum_{j=1}^{N} x_j\rangle = \sum_{i=1}^{N}\langle u - x_i, x_i\rangle = 0.$$

Similarly, $\langle u - w, w\rangle = 0$. Thus $w \in S(u)$. Since $\langle x_i\rangle = \langle u, x_i\rangle$ for $i = 1, \dots, N$ and since $0 = \langle w, u - w\rangle$,

$$\langle w\rangle = \langle w, u\rangle = \langle u - \sum_{i=1}^{N} x_i, u\rangle = \langle u\rangle - \sum_{i=1}^{N}\langle x_i, u\rangle = \langle u\rangle - \sum_{i=1}^{N}\langle x_i\rangle.$$

□

The following Lemma 4 is a simple corollary of Proposition 1 for such our situation. We follow here the notation of Theorem 1. For $\mathbf{p} \in \mathbb{R}^n$, we write $W_\epsilon(\mathbf{p}) = \{Y \in V \mid \langle X_\epsilon^{\mathbf{p}}, Y\rangle = 0\}$. For a finite index set $I = \{1, 2, \dots, N\}$ we consider $\{\mathbf{p}_i\}_{i\in I}$ which is a finite subset of $\mathbb{R}^n$. We denote $\langle X, X\rangle$ briefly by $\langle X\rangle$ for $X \in V$.

Lemma 4. *Suppose that*

$$\#I > \frac{1 - \langle Y\rangle}{\langle X_\epsilon^0\rangle}$$

for $Y \in S(\mathbf{1}) \cap \bigcap_{i\in I} W_\epsilon(\mathbf{p}_i)$. Then there exist $i, j \in I$ with $i \neq j$ such that $\langle X_\epsilon^{\mathbf{p}_i}, X_\epsilon^{\mathbf{p}_j}\rangle \neq 0$. Here $X_\epsilon^0 \in V$ is defined by

$$X_\epsilon^0(\omega) = \begin{cases} 1 & \text{if } \omega \in \pi(A(\epsilon)), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Assume that $\langle X_\epsilon^{\mathbf{p}_i}, X_\epsilon^{\mathbf{p}_j}\rangle = 0$ for any $i \neq j$. Equalities $\langle X_\epsilon^{\mathbf{p}_i}\rangle = P(\pi(A(\epsilon))) = \langle X_\epsilon^{\mathbf{p}_i}, \mathbf{1}\rangle$ gives $X_\epsilon^{\mathbf{p}_i} \in S(\mathbf{1})$. Since $\langle X_\epsilon^{\mathbf{p}_i}, Y\rangle = 0$ for any $i \in I$, Proposition 1 now shows that there exists $Z \in S(\mathbf{1})$ such that

$$\langle \mathbf{1}\rangle = \langle Z\rangle + \langle Y\rangle + \sum_{i\in I}\langle X_\epsilon^{\mathbf{p}_i}\rangle.$$

By $\langle \mathbf{1}\rangle = 1$, $\langle X_\epsilon^{\mathbf{p}_i}\rangle = P(\pi(A(\epsilon))) = \langle X_\epsilon^0\rangle$ and by $\langle Z\rangle \geq 0$, we have $1 - \langle Y\rangle \geq \#I \times \langle X_\epsilon^0\rangle$, a contradiction. □

Lemma 5. *For* $\mathbf{p}, \mathbf{q} \in \mathbb{R}^n$*, if* $\langle X_\epsilon^{\mathbf{p}}, X_\epsilon^{\mathbf{q}} \rangle \neq 0$*, then* $\mathbf{p} - \mathbf{q} \in \mathbb{Z}^n + A(2\epsilon)$*.*

Proof. By the definition of $\langle\ ,\ \rangle$ and the assumption $\langle X_\epsilon^{\mathbf{p}}, X_\epsilon^{\mathbf{q}} \rangle \neq 0$, we have $\pi(A(\epsilon) + \mathbf{p}) \cap \pi(A(\epsilon) + \mathbf{q}) \neq \varnothing$. Then there exist $\boldsymbol{\alpha}, \boldsymbol{\beta} \in A(\epsilon)$ such that $\pi(\boldsymbol{\alpha} + \mathbf{p}) = \pi(\boldsymbol{\beta} + \mathbf{q})$, that is , $(\boldsymbol{\alpha} + \mathbf{p}) - (\boldsymbol{\beta} + \mathbf{q}) \in \mathrm{Ker}(\pi) = \mathbb{Z}^n$. Therefore $\mathbf{p} - \mathbf{q} \in \mathbb{Z}^n + A(2\epsilon)$. □

Lemma 6. *Consider two orthonormal bases of* $\mathbb{R}^n$*,* $E := \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ *and* $F := \{\mathbf{f}_1, \dots, \mathbf{f}_n\}$*. For* $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{R}$*, let*

$$|\sum_{i=1}^n \alpha_i \mathbf{e}_i|_\infty^E = \max_{i=1,\dots,n} |\alpha_i|, \quad |\sum_{i=1}^n \beta_i \mathbf{f}_i|_\infty^F = \max_{i=1,\dots,n} |\beta_i|.$$

Then for arbitrary $\mathbf{x} \in \mathbb{R}^n$*, the inequality* $|\mathbf{x}|_\infty^E \leq \sqrt{n}|\mathbf{x}|_\infty^F$ *holds.*

Proof. The proof is standard, left to the reader. □

3. Proofs

3.1. **Proof of Theorem 1.** *Part (i)*: According to the preceding section, we fix an orthonormal basis $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ and an inner product $(\ ,\ )$. Let T be an m-dimensional linear subspace of $\mathbb{R}^n$ in Theorem 1. Now let $F = \{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ be another orthonormal basis of $\mathbb{R}^n$ with $(\ ,\ )$ such that

$$T = \{\sum_{i=1}^m \alpha_i \mathbf{f}_i \mid \alpha_1, \dots, \alpha_m \in \mathbb{R}\}.$$

Let $B = \{\mathbf{x} \in \mathbb{R}^n \mid (\mathbf{x}, \mathbf{x}) < n\epsilon^2\}$ denote the ball centered at the origin with radius $\sqrt{n}\epsilon$. Then B contains the cube $A(2\epsilon)$. We now consider a subgroup of T,

$$G := \{\sum_{i=1}^m a_i \sqrt{n}\epsilon \mathbf{f}_i \mid a_1, \dots, a_m \in \mathbb{Z}\}.$$

Let $H \subset G$ be a finite subset of G. For any H, Y in Theorem 1 satisfies

$$Y \in S(\mathbf{1}) \cap \bigcap_{\mathbf{p} \in H} W_\epsilon(\mathbf{p}).$$

Here we set

$$Q = G \cap (\mathbb{Z}^n + A(2\epsilon)) \quad \text{and} \quad \gamma = \left\lfloor \frac{1 - \langle Y \rangle}{\epsilon^n} \right\rfloor + 1.$$

Replacing I in Lemma 4 by H, there exist $\mathbf{p}$, $\mathbf{q} \in H$ with $\mathbf{p} \neq \mathbf{q}$ such that $\langle X_\epsilon^{\mathbf{p}}, X_\epsilon^{\mathbf{q}} \rangle \neq 0$ for any $H \subset G$ with $\#H \geq \gamma$ since $\langle X_\epsilon^0 \rangle = \epsilon^n$. Lemma 5 thus implies that $\mathbf{p} - \mathbf{q} \in Q \setminus \{0\}$. Furthermore we find that $\mathbf{p} - \mathbf{q} \notin A(2\epsilon)$. Because any $\mathbf{r} \in G$ with $\mathbf{r} \neq 0$ satisfies $(\mathbf{r}, \mathbf{r}) \geq n\epsilon^2$, we have $\mathbf{r} \notin B$, i.e., $\mathbf{r} \notin A(2\epsilon)$. It is clear that Q is symmetric and that $0 \in Q$. Thus Q, which is a subset of G, satisfies Condition A with γ. Now we consider an isomorphism $\phi : G \simeq \mathbb{Z}^m$ by $\sum_{i=1}^m a_i \sqrt{n}\epsilon \mathbf{f}_i \mapsto (a_1, \ldots, a_m)$. For $\boldsymbol{\rho} = \sum_{i=1}^m a_i \sqrt{n}\epsilon \mathbf{f}_i$ with $a_1, \ldots, a_m \in \mathbb{Z}$, write $|\phi(\boldsymbol{\rho})|_\infty^F = \max_{i=1,\ldots,m} |a_i| =: R$. Then $|\boldsymbol{\rho}|_\infty^F = R\sqrt{n}\epsilon$ and $|\boldsymbol{\rho}|_\infty^E \leq n\epsilon R$ by Lemma 6. Lemma 1 shows that there exist $\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_l \in Q \subset G$ such that they are linearly independent over $\mathbb{R}$ and such that

$$\sum_{i=1}^l \log |\phi(\boldsymbol{\rho}_i)|_\infty^F \leq \frac{l}{m} \left(\log \gamma + C(l)\right),$$

that is,

$$\sum_{i=1}^l \log |\boldsymbol{\rho}_i|_\infty^E \leq \frac{l}{m} \left(\log \gamma + C(l)\right) + l \log \epsilon + l \log n.$$

Here $\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_l$ are in $G \cap (\mathbb{Z}^n + A(2\epsilon)) \subset T \cap (\mathbb{Z}^n + A(2\epsilon))$ and they are not in $A(2\epsilon)$. Since

$$\gamma \epsilon^m \leq \frac{1 - \langle Y \rangle}{\epsilon^{n-m}} + \epsilon^m,$$

we obtain Part (i) of Theorem 1 with

$$C_{l,m,n} = \frac{l}{m} C(l) + l \log n,$$

where $C(l)$ is in Lemma 1. This completes the proof of Part (i).

Remark 3. Let $r_1, \ldots, r_l$ be as in the proof of Lemma 2. Then $r_i = |\phi(\boldsymbol{\rho}_i)|_\infty^F$, i.e., $r_i \sqrt{n}\epsilon = |\boldsymbol{\rho}_i|_\infty^F$ holds.

Part (ii): By the assumptions, there exists a constant C, independent of ϵ, satisfying the following: there exists $Y \in S(\mathbf{1})$ (which depends on ϵ) with $\tilde{H}_\epsilon^{m,n}(Y) \leq C$ with $\langle X_\epsilon^{\mathbf{p}}, Y \rangle = 0$ for all $\mathbf{p} \in T$ for arbitrary small $\epsilon > 0$. Now suppose that δ in our proof of Lemma 1 is fixed. Here δ is a sufficiently small positive real number depending on only l, m, n (and independent of ϵ). Replacing $C(l)$ by "a constant depending on l and δ", one can check that Lemma 1 is still true. Thus Part (i) holds with a constant depending on δ instead of (1). From the condition of Part (ii), we then have the following: for any ϵ, $0 < \epsilon < 1/2$, there exist m linearly independent points $\mathbf{z}_1(\epsilon), \ldots, \mathbf{z}_m(\epsilon) \in \mathbb{R}^n$ with

$$\sum_{i=1}^m \log |\mathbf{z}_i(\epsilon)|_\infty \leq \log(C + \epsilon^m) + C' \tag{6}$$

such that $\mathbf{z}_i(\epsilon) \in T \cap Z(\epsilon)$ for $i = 1, \ldots, m$. Here C' depends on m, n, δ and is independent of ϵ. Moreover we can choose C' such that $C' \to C_{m,m,n}$ in (1) as $\delta \to +0$.

We now consider the set $\mathfrak{S}$ in Theorem 1, $\mathfrak{S} = \{(\mathbf{z}_1(\epsilon_k), \ldots, \mathbf{z}_m(\epsilon_k)) \mid k = 1, 2, \ldots\} \subset \mathbb{R}^{n \times m}$, where $\mathbf{z}_1(\epsilon_k), \ldots, \mathbf{z}_m(\epsilon_k)$ are linearly independent points in $T \cap Z(\epsilon_k)$ in (6). Note that they are not in $A(2\epsilon_k)$ and that $\mathfrak{S}$ is bounded in $\mathbb{R}^{n\times m}$. Thus there exists an accumulating point $\{\boldsymbol{\zeta}_1, \dots, \boldsymbol{\zeta}_m\}$ of $\mathfrak{S}$. Since each $\boldsymbol{\zeta}_i$ is in $T \cap Z(\epsilon_k)$ for infinitely many $\epsilon_k \to +0$, it must be in $T \cap (\mathbb{Z}^n \setminus \{0\})$. We now show that $\boldsymbol{\zeta}_1, \dots, \boldsymbol{\zeta}_m$ are linearly independent over $\mathbb{R}$. We look back on our proof of Part (i). In the later part of the proof, for any $\epsilon > 0$ let us now consider $D_1 = |\det((a_{k,i}\sqrt{n}\epsilon)_{k,i=1,\dots,m})| = |\det((a_{k,i})_{k,i=1,\dots,m})|(\sqrt{n}\epsilon)^m$ formed by m linearly independent elements in Q, $\boldsymbol{\rho}_k(\epsilon) := \boldsymbol{\rho}_k := \sum_{i=1}^m a_{k,i}\sqrt{n}\epsilon\mathbf{f}_i$ for $k = 1, \dots, m$ where $a_{k,i}$ depends on ϵ. From the proofs of Lemma 1 and Lemma 2, one can see that

$$\frac{|\det((a_{k,i})_{k,i=1,\dots,m})|}{r_1 \cdots r_m} \geq 1 - \sum_{i=2}^{m} \delta_i (i-1)^{(i+1)/2},$$

where $r_1, \dots, r_m$ are in our proof of Lemma 1. Let D_2 be the right-hand side of the last inequality. Suppose that δ in the proof of Lemma 2 is a sufficiently small positive constant depending only on l, m, n. Then D_2 does not vanish, and it is independent of ϵ. From the proof of Lemma 2, each $\boldsymbol{\rho}_k(\epsilon) = \boldsymbol{\rho}_k = \sum_{i=1}^m a_{k,i}\sqrt{n}\epsilon\mathbf{f}_i$ for $k = 1, \dots, m$ in the proof of Part (i) satisfies that $|\boldsymbol{\rho}_k|_\infty^F = r_k\sqrt{n}\epsilon$ by Remark 3. We thus obtain

$$D_1 \geq |\boldsymbol{\rho}_1|_\infty^F \cdots |\boldsymbol{\rho}_m|_\infty^F D_2 \geq |\boldsymbol{\rho}_1|_\infty^E \cdots |\boldsymbol{\rho}_m|_\infty^E (\sqrt{n})^{-m} D_2 \geq (1-2\epsilon)^m (\sqrt{n})^{-m} D_2$$

by Lemma 6 and by $|\boldsymbol{\rho}_k|_\infty^E \geq 1 - 2\epsilon$. Hence D_1 is bigger than a positive constant independent of ϵ when ϵ is sufficiently small. This shows that the determinant formed by $\boldsymbol{\zeta}_1, \dots, \boldsymbol{\zeta}_m$ is not 0 and that they are linearly independent over $\mathbb{R}$. Therefore T has m linearly independent $\boldsymbol{\zeta}_1, \dots, \boldsymbol{\zeta}_m \in \mathbb{Z}^n$ and we conclude that T is defined over $\mathbb{Q}$. The proof is complete. □

3.2. **Proof of Corollary 1.** First note that the following inequality holds: let ϵ, $a_1, \dots, a_n$ be real numbers with $a_i \geq 1$ for $i = 1, \dots, n$. Then

$$\sum_{i=1}^{n} \log(a_i + \epsilon) \leq n \log(1+\epsilon) + \sum_{i=1}^{n} \log a_i \tag{7}$$

because $a_i + \epsilon \leq a_i(1+\epsilon)$.

Proof of Corollary 1. Let T, M and ϵ_0 be as in Corollary 1 and let ϵ in Theorem 1 be given by $\epsilon_0 = nM\epsilon$. To deduce Corollary 1 from Part (i), take the trivial solution, $Y = 0$, which is in $S(\mathbf{1})$. Then Part (i) of Theorem 1 says that there exist l linearly independent $\mathbf{z}_1, \dots, \mathbf{z}_l \in T \cap (\mathbb{Z}^n \setminus \{0\} + Z(\epsilon))$ such that

$$\sum_{i=1}^{l} \log|\mathbf{z}_i|_\infty \leq \frac{l}{m} \log\left(\epsilon^{m-n} + \epsilon^m\right) + C_{l,m,n}.$$

For any $j = 1, \dots, l$ and for $\mathbf{z}_j$, there exist $\mathbf{b}_j \in \mathbb{Z}^n \setminus \{0\}$ and $\mathbf{d}_j \in A(2\epsilon)$ such that $\mathbf{z}_j = \mathbf{b}_j + \mathbf{d}_j$. By $\mathbf{z}_j \in T$, we have $(\mathbf{a}_i, \mathbf{z}_j) = 0$ for $i = 1, \dots, n-m$.

Then $|(\mathbf{a}_i, \mathbf{b}_j)| = |(\mathbf{a}_i, \mathbf{z}_j) - (\mathbf{a}_i, \mathbf{d}_j)| = |(\mathbf{a}_i, \mathbf{d}_j)| < nM\epsilon = \epsilon_0$. Moreover we see that $1 \leq |\mathbf{b}_j|_\infty = |\mathbf{z}_j - \mathbf{d}_j|_\infty \leq |\mathbf{z}_j|_\infty + |\mathbf{d}_j|_\infty \leq |\mathbf{z}_j|_\infty + \epsilon$, namely $1 - \epsilon \leq |\mathbf{z}_j|_\infty$. Then the inequality (7) gives

$$\sum_{j=1}^{l} \log\left(\frac{|\mathbf{z}_j|_\infty}{1-\epsilon} + \frac{\epsilon}{1-\epsilon}\right) \leq l \log\left(1 + \frac{\epsilon}{1-\epsilon}\right) + \sum_{j=1}^{l} \log \frac{|\mathbf{z}_j|_\infty}{1-\epsilon}.$$

That is,

$$\sum_{j=1}^{l} \log\left(|\mathbf{z}_j|_\infty + \epsilon\right) \leq l \log\left(1 + \frac{\epsilon}{1-\epsilon}\right) + \sum_{j=1}^{l} \log |\mathbf{z}_j|_\infty.$$

Thus

$$\begin{aligned} \sum_{j=1}^{l} \log |\mathbf{b}_j|_\infty &\leq \sum_{j=1}^{l} \log(|\mathbf{z}_j|_\infty + \epsilon) \\ &\leq \frac{l}{m} \log\left(\epsilon^{m-n} + \epsilon^{m}\right) + l \log\left(1 + \frac{\epsilon}{1-\epsilon}\right) + C_{l,m,n}. \end{aligned}$$

Again, by $\epsilon = \epsilon_0/(nM) < 1$ and by $m < n$, (7) gives $\log(\epsilon^{m-n} + \epsilon^n) \leq \log(1 + \epsilon^n) + \log \epsilon^{m-n}$. Since $n \geq 2$ and since $M \geq 1$ one sees that $\epsilon < 1/2$ for $\epsilon_0 < 1$. Therefore we obtain

$$\sum_{j=1}^{l} \log |\mathbf{b}_j|_\infty \leq \frac{l(n-m)}{m} \log \frac{M}{\epsilon_0} + \frac{l(n-m)}{m} \log n + \left(\frac{l}{m} + l\right) \log 2 + C_{l,m,n}.$$

The case of $l = 1$ completes the proof. □

3.3. **Proof of Theorem 2.** The definition of height of a linear subspace and detailed discussions can be found in [2] and [7]. We follow Schmidt [7, Ch. 3].

Let T be a linear subspace of $\mathbb{R}^n$ defined over $\mathbb{Q}$ with $\dim_{\mathbb{R}} T = m$. Then there exist $\mathbf{g}_1, \ldots, \mathbf{g}_m \in \mathbb{Z}^n$ such that

$$T \cap \mathbb{Z}^n = \{\sum_{i=1}^{m} b_i \mathbf{g}_i \mid b_1, \ldots, b_m \in \mathbb{Z}\}.$$

Throughout this section, we write

$$\mathfrak{F} = \{\sum_{i=1}^{m} \beta_i \mathbf{g}_i \mid 0 \leq \beta_i < 1 \text{ for } i = 1, \ldots, m\}$$

for a fundamental domain of the lattice group $T \cap \mathbb{Z}^n$. According to Schmidt [7, Theorem 1], the height of $T \cap \mathbb{Q}^n$ equals the volume of $\mathfrak{F}$ in our proof of Lemma 7 below; $H(T \cap \mathbb{Q}^n) = \mu_1(\mathfrak{F})$. We denote it briefly by $H(T_{\mathbb{Q}})$.

Let ϵ, $A(\epsilon)$, π and P be as in above.

Lemma 7. *Let T be a linear subspace of $\mathbb{R}^n$ with $\dim_{\mathbb{R}} T = m$. Suppose that T is defined over $\mathbb{Q}$. That is, there exist $\mathbf{a}_1, \ldots, \mathbf{a}_{n-m} \in \mathbb{Z}^n$ such that*

$$T = \{\mathbf{x} \in \mathbb{R}^n \mid (\mathbf{a}_i, \mathbf{x}) = 0 \textit{ for } i = 1, \ldots, n-m\}.$$

Then the inequality

$$P\left(\bigcup_{\mathbf{p}\in T} \pi(A(\epsilon) + \mathbf{p})\right) \leq D_{n-m}\epsilon^{n-m} H(T_{\mathbb{Q}})$$

holds. Here D_{n-m} is the volume of the $(n-m)$-dimensional ball with radius $\sqrt{n}/2$: $D_{n-m} = \pi^{(n-m)/2}\left(\sqrt{n}/2\right)^{n-m}/\Gamma((n-m+2)/2)$.

Proof. Let $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ be the orthonormal basis of $\mathbb{R}^n$ in our proof of Theorem 1. Let $T^{\perp}$ be the orthogonal complement of T. For $x = \sum_{i=1}^{n} \alpha_i \mathbf{f}_i \in \mathbb{R}^n$, we define the natural projections, $\phi_1 : \mathbb{R}^n \to T$ by $\phi_1(x) = \sum_{i=1}^{m} \alpha_i \mathbf{f}_i$ and $\phi_2 : \mathbb{R}^n \to T^{\perp}$ by $\phi_2(x) = x - \phi_1(x)$. Moreover we denote the natural inclusions $T \hookrightarrow \mathbb{R}^n$ by ι_1, and $T^{\perp} \hookrightarrow \mathbb{R}^n$ by ι_2. For $\mathbf{x} \in T$, $\mathbf{y} \in T^{\perp}$, we write $\mathbf{x} \oplus \mathbf{y} = \iota_1(\mathbf{x}) + \iota_2(\mathbf{y}) \in \mathbb{R}^n$. Moreover we set $A \times B = \{\mathbf{x} \oplus \mathbf{y} \mid \mathbf{x} \in A,\ \mathbf{y} \in B\}$ for $A \subset T$, $B \subset T^{\perp}$.

Let $E = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ be the orthonormal basis of $\mathbb{R}^n$ in the preceding section. Then $A(\epsilon) = \{\mathbf{x} \in \mathbb{R}^n \mid |\mathbf{x}|_{\infty}^{E} < \epsilon/2\}$. Let $B_0 = \{\mathbf{x} \in \mathbb{R}^n \mid (\mathbf{x}, \mathbf{x}) < n(\epsilon/2)^2\}$ be the ball centered the origin with radius $\sqrt{n}\epsilon/2$ in $\mathbb{R}^n$. Then $A(\epsilon) \subset B_0$. Since $\phi_1(\mathbf{a} + \mathbf{p}) = \phi_1(\mathbf{a}) + \phi_1(\mathbf{p}) = \phi_1(\mathbf{a}) + \mathbf{p} \in T$ and since $\phi_2(\mathbf{a} + \mathbf{p}) = \phi_2(\mathbf{a}) \in \phi_2(A(\epsilon)) \subset \phi_2(B_0)$ for $\mathbf{a} \in A(\epsilon)$, $\mathbf{p} \in T$, we have $\mathbf{a} + \mathbf{p} = \phi_1(\mathbf{a}) + \mathbf{p} + \phi_2(\mathbf{a}) \in T \times \phi_2(B_0)$. Thus we have

$$\bigcup_{\mathbf{p}\in T} A(\epsilon) + \mathbf{p} \subset T \times \phi_2(B_0).$$

Next, for any subset D of $T^{\perp}$, we show that $\pi(T \times D) \subset \pi(\mathfrak{F} \times D)$. Note that

$$T = \{\mathbf{y} + \sum_{i=1}^{m} b_i \mathbf{g}_i \mid \mathbf{y} \in \mathfrak{F},\ b_1, \ldots, b_m \in \mathbb{Z}\}.$$

Then $(\mathbf{y} + \sum_{i=1}^{m} b_i \mathbf{g}_i) \oplus \mathbf{d} = \iota_1(\mathbf{y} + \sum_{i=1}^{m} b_i \mathbf{g}_i) + \iota_2(\mathbf{d}) = \iota_1(\mathbf{y}) + \iota_2(\mathbf{d}) + \sum_{i=1}^{m} b_i \mathbf{g}_i$ for $\mathbf{d} \in D$. Since $\pi(\sum_{i=1}^{m} b_i \mathbf{g}_i) = 0$ we have $\pi((\mathbf{y} + \sum_{i=1}^{m} b_i \mathbf{g}_i) \oplus \mathbf{d}) \in \pi(\mathfrak{F} \times D)$. Therefore we obtain

$$\pi\left(\bigcup_{\mathbf{p}\in T} A(\epsilon) + \mathbf{p}\right) \subset \pi(\mathfrak{F} \times \phi_2(B_0)).$$

Let μ be the Lebesgue measure on $\mathbb{R}^n$. In general, the inequality $P(\pi(S)) \leq \mu(S)$ holds for any measurable set S of $\mathbb{R}^n$. Then $P(\pi(\mathfrak{F} \times \phi_2(B_0))) \leq \mu(\mathfrak{F} \times \phi_2(B_0)) = \mu_1(\mathfrak{F}) \times \mu_2(\phi_2(B_0))$ where μ_1 is the Lebesgue measure on $\mathbb{R}^m$ via $T \simeq \mathbb{R}^n$ by $\sum_{i=1}^m \alpha_i \mathbf{f}_i \mapsto (\alpha_1, \ldots, \alpha_m)$, and μ_2 is the Lebesgue measure on $\mathbb{R}^{n-m}$ via $T^\perp \simeq \mathbb{R}^{n-m}$ by $\sum_{i=m+1}^n \alpha_i \mathbf{f}_i \mapsto (\alpha_{m+1}, \ldots, \alpha_n)$.

We now write $\mathbf{g}_i = \sum_{j=1}^m \alpha_{i,j} \mathbf{f}_j$ for $i = 1, \ldots, m$. Then $\mu_1(\mathfrak{F}) = |\det(\alpha_{i,j})_{i,j=1,\ldots,m}|$ and this equals $H(T_\mathbb{Q})$, the height of T (see [7, Ch. 3]). Since $\phi_2(B_0)$ is the ball centered the origin with radius $\sqrt{n}\epsilon/2$ in $T^\perp \simeq \mathbb{R}^{n-m}$, $\mu_2(\phi_2(B_0)) = D_{m-n}\epsilon^{n-m}$. This completes the proof. □

Here we give our proof of Theorem 2. It also shows that we can take $C = H(T_\mathbb{Q})D_{n-m}$ where C is the constant in our proof of Part (ii) of Theorem 1. Here $H(T_\mathbb{Q})$ is the height of T and D_{n-m} is in Lemma 7. This is why we say that $\tilde{H}_\epsilon^{m,n}(Y)$ plays a role of height.

Proof of Theorem 2. We only need to show that (II) implies (I). We show here that there exists a constant C in our proof of Part (ii) of Theorem 1. The set $\bigcup_{\mathbf{p}\in T} \pi(A(\epsilon)+\mathbf{p})$ is open. Let D be the complement of it. Let Y be the indicator random variable of the measurable set D. That is, for $\omega \in \Omega$, $Y(\omega) = 1$ if $\omega \in D$, $Y(\omega) = 0$ if not. By definition, we have $\langle Y, \mathbf{1}\rangle = \langle Y, Y\rangle$. Then $Y \in S(\mathbf{1})$. One can see that $X_\epsilon^\mathbf{p}(\omega)Y(\omega) = 0$ for $\omega \in \Omega$ and for $\mathbf{p} \in T$. Thus $\langle X_\epsilon^\mathbf{p}, Y\rangle = 0$. Under the condition (II), we have

$$\langle Y\rangle = P(D) = 1 - P\left(\bigcup_{\mathbf{p}\in T} \pi(A(\epsilon)+\mathbf{p})\right) \geq 1 - D_{n-m}\epsilon^{n-m}H(T_\mathbb{Q})$$

by Lemma 7. Let $C = D_{n-m}H(T_\mathbb{Q})$. It follows that there exists $Y \in S(\mathbf{1})$ (which depends on ϵ) with $\tilde{H}_\epsilon^{m,n}(Y) \leq C$ with $\langle X_\epsilon^\mathbf{p}, Y\rangle = 0$ for all $\mathbf{p} \in T$ for arbitrary small $\epsilon > 0$. □

3.4. **Proof of Corollary 2.** Let T be in Corollary 2. Then Theorem 2 shows that we can use the accumulating point $(\boldsymbol{\zeta}_i)_{i=1,\ldots,m}$ of $\mathfrak{S}$ in Theorem 1. Let $\epsilon \to +0$ in our proof of Part (ii). Since one can choose δ in the proof of Part (ii) to be arbitrary small (but δ must be independent of ϵ), one can check that the following holds by Theorem 1 and by (6): there exist m linearly independent points $\boldsymbol{\zeta}_1, \ldots, \boldsymbol{\zeta}_m \in T \cap (\mathbb{Z}^n \setminus \{0\})$ with

$$\sum_{i=1}^m \log|\boldsymbol{\zeta}_i|_\infty \leq \log(D_{n-m}H(T_\mathbb{Q})) + C_{m,m,n}.$$

Since D_{n-m} and $C_{m,m,n}$ in (1) are independent of $H(T_\mathbb{Q})$, the last inequality shows Corollary 2. □

Acknowledgements

The author is deeply indebted to Professor Noriko Hirata-Kohno, who provided valuable information, advice, and encouragement. He would also like to thank Professors Masaaki Amou, Mamoru Asada and Yoshinori Takei, who made significant contributions to this work through their insightful comments.

References

[1] A. Baker, Transcendental Number Theory Cambridge University Press, 1975.

[2] E. Bombieri and J. Vaaler, *On Siegel's lemma* Invent Math. 7 (1983) 11–32.

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

[4] M. Nagata, *On Siegel's lemma and linear spaces of random variables* Diophantine analysis and related fields 2010, AIP Conf. Proc., 1264, Amer. Inst. Phys., Melville, NY (2010) 62–70.

[5] P. Philippon et M. Waldschmidt, *Formes lineaires de logarithmes sur les groupes algebraiques comutatifs* Illinois J. of Math. 32, Num. 2, (1988) 281–314.

[6] W. M. Schmidt, Diophantine Approximations and Diophantine Equations, LNM 1467, Springer-Verlag, Berlin Heidelberg, 1991.

[7] W. M. Schmidt, *On heights of algebraic subspaces and Diophantine approximations* Annals of Math. 85 (1967), 430–472.

[8] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen* (1929), Carl Ludwig Siegel Gesammelte Abhandlungen Band I, Springer-Verlag (1966) 209–266.

[9] J. L. Thunder, *Remarks on Adelic Geometry of Numbers* Number Theory for the Millennium III, (2000) 253–259.

Osaka University of Pharmaceutical Sciences
Osaka, 569-1094, Japan
e-mail address: nagata@gly.oups.ac.jp

(*Received September 25, 2013*)
(*Accepted April 10, 2014*)