Claremont Colleges
Scholarship @ Claremont

CMC Faculty Publications and Research | CMC Faculty Scholarship

1-1-2006

Integral Points of Small Height Outside of a Hypersurface

Lenny Fukshansky
Claremont McKenna College

Recommended Citation
Fukshansky, Lenny. "Integral points of small height outside of a hypersurface." Monatshefte für Mathematik 147.1 (2006): 25-41.

This Article is brought to you for free and open access by the CMC Faculty Scholarship at Scholarship @ Claremont. It has been accepted for inclusion in CMC Faculty Publications and Research by an authorized administrator of Scholarship @ Claremont. For more information, please contact scholarship@cuc.claremont.edu.

INTEGRAL POINTS OF SMALL HEIGHT OUTSIDE OF A HYPERSURFACE

LENNY FUKSHANSKY

Abstract. Let F be a non-zero polynomial with integer coefficients in N variables of degree M. We prove the existence of an integral point of small height at which F does not vanish. Our basic bound depends on N and M only. We separately investigate the case when F is decomposable into a product of linear forms, and provide a more sophisticated bound. We also relate this problem to a certain extension of Siegel's Lemma as well as to Faltings' version of it. Finally we exhibit an application of our results to a discrete version of the Tarski plank problem.

1. Introduction and notation

Let

$$F(\boldsymbol{X}) = F(X_1, ..., X_N) \in \mathbb{Z}[X_1, ..., X_N]$$

be a polynomial in $N \geq 1$ variables of degree $M \geq 1$ with integer coefficients. If F is not identically zero, there must exist a point with integer coordinates at which F does not vanish, in other words an integral point that lies outside of the hypersurface defined by F over $\mathbb{Q}$. How does one find such a point?

For a point $\boldsymbol{x} = (x_1, ..., x_N) \in \mathbb{Z}^N$, define its *height* and *length* respectively by

$$H(\boldsymbol{x}) = \max_{1 \leq i \leq N} |x_i|, \quad \mathcal{L}(\boldsymbol{x}) = \sum_{i=1}^{N} |x_i|.$$

It is easy to see that a set of points with height or length bounded by some fixed constant is finite. In fact, for a positive real number R,

$$\big|\{\boldsymbol{x} \in \mathbb{Z}^N : H(\boldsymbol{x}) \leq R\}\big| = (2[R]+1)^N, \tag{1}$$

and

$$\big|\{\boldsymbol{x} \in \mathbb{Z}^N : \mathcal{L}(\boldsymbol{x}) \leq R\}\big| = \sum_{k=0}^{\min([R],N)} 2^k \binom{N}{k}\binom{[R]}{k}, \tag{2}$$

where (1) is obvious and (2) follows from Theorem 6 of [4]; we write $[R]$ for the integer part of R. Therefore if we were able to prove the existence of a point $\boldsymbol{x} \in \mathbb{Z}^N$ with $H(\boldsymbol{x}) \leq R$ or $\mathcal{L}(\boldsymbol{x}) \leq R$ for some explicitly determined value of R, then the problem of finding this point would reduce to a finite search. Thus we will consider the following problem.

1991 *Mathematics Subject Classification.* Primary 11C08, 11H06; Secondary 11D04, 11H46.
Key words and phrases. polynomials, lattices, linear forms, height.

Problem 1. *Given a polynomial $F(X_1, ..., X_N) \in \mathbb{Z}[X_1, ..., X_N]$ in $N \geq 1$ variables of degree $M \geq 1$, prove the existence of a point $\boldsymbol{x} \in \mathbb{Z}^N$ of small height (length) such that $F(\boldsymbol{x}) \neq 0$ with an explicit upper bound on the height (length).*

This problem, although of independent interest, is also closely related to an important trend in Diophantine approximations. Consider the special case when $F(\boldsymbol{X})$ is homogeneous in $N \geq 2$ variables and decomposable into a product of integral linear forms, i.e. suppose that

$$F(X_1, ..., X_N) = \prod_{i=1}^{M} L_i(X_1, ..., X_M),$$

where $L_i(X_1, ..., X_N) \in \mathbb{Z}[X_1, ..., X_N]$ is a linear form for each $1 \leq i \leq M$. Write

$$\Lambda_i = \{\boldsymbol{y} \in \mathbb{Z}^N : L_i(\boldsymbol{y}) = 0\},$$

for each $1 \leq i \leq M$. Then each such Λ_i is a lattice of rank $N-1$ in $\mathbb{R}^N$, and the statement that $F(\boldsymbol{x}) \neq 0$ for some $\boldsymbol{x} \in \mathbb{Z}^N$ is equivalent to the statement that $\boldsymbol{x} \in \mathbb{Z}^N \setminus \bigcup_{i=1}^{M} \Lambda_i$. In this case Problem 1 can be restated as follows.

Problem 2. *Let $\Lambda_1, ..., \Lambda_M$ be sublattices of $\mathbb{Z}^N$ of rank $N-1$. Prove the existence of a point $\boldsymbol{x} \in \mathbb{Z}^N \setminus \bigcup_{i=1}^{M} \Lambda_i$ of small height with an explicit bound on height.*

More generally, suppose that $\Omega \subseteq \mathbb{Z}^N$ is a lattice of rank J, $2 \leq J \leq N$, and let $\Lambda_1, ..., \Lambda_M$ be proper sublattices of Ω of respective ranks $l_1, ..., l_M$, $1 \leq l_i \leq J-1$ for each $1 \leq i \leq M$. We can state the following generalization of Problem 2.

Problem 3. *Prove the existence of a point $\boldsymbol{x} \in \Omega \setminus \bigcup_{i=1}^{M} \Lambda_i$ of small height with an explicit bound on the height.*

Notice that this can be viewed as a certain extension of a classical Siegel's Lemma (see for instance [3], [16], and [19]), which guarantees the existence of a non-zero point of small height in Ω. Then Problem 3 is a version of Siegel's Lemma with additional linear conditions, and Problem 2 can be thought of as a problem inverse to Siegel's Lemma. Here is the main result of this paper.

Theorem 1.1. *Let $\Omega \subseteq \mathbb{Z}^N$ be a sublattice of rank J, $1 \leq J \leq N$. Let $\Lambda_1, ..., \Lambda_M$ be proper non-zero sublattices of Ω. Then there exists $\boldsymbol{x} \in \Omega \setminus \bigcup_{i=1}^{M} \Lambda_i$ such that*

$$H(\boldsymbol{x}) \leq \left(\left(\frac{3}{2}\right)^{J-1} J^J \left\{ \sum_{i=1}^{M} \frac{1}{H(\Lambda_i)} + \sqrt{M} \right\} + J \right) H(\Omega). \tag{3}$$

A generalization of this theorem to the number field case is presented in the companion paper [9]. The paper is organized as follows. In section 2 we treat Problem 1 for a general polynomial in N variables of degree M with integer coefficients and produce some basic results. The bounds on height and length depend on N and M only. In fact, we produce simple bounds on both, height and length, that depend only on M. In sections 3 and 4 we prove some technical lemmas on counting lattice points in simple convex bodies in a Euclidean space. These lemmas are then used in section 5 to treat Problem 2 and Problem 3, proving Theorem 1.1. The bounds on height of the points in question in section 5 depend on M, N, and heights of corresponding lattices. We also derive a sharper bound for Faltings' version of Siegel's Lemma (see Proposition 2.18, [8]) in our context as a corollary of

the main result. Finally in section 6 we exhibit a simple application of our results to a discrete version of the Tarski plank problem.

Before we can proceed we need to introduce some additional notation. We can extend height to polynomials by evaluating height of their coefficient vectors. We also define a height function on lattices. Let $\Lambda \subseteq \mathbb{Z}^N$ be a lattice of rank J, $1 \leq J \leq N$. Choose a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$ for Λ, and write $X = (\boldsymbol{x}_1 \ ... \ \boldsymbol{x}_J)$ for the corresponding $N \times J$ basis matrix. Then

$$\Lambda = \{X\boldsymbol{t} : \boldsymbol{t} \in \mathbb{Z}^J\}.$$

On the other hand, there exists an $(N-J) \times N$ matrix A with integer relatively prime entries so that

$$\Lambda \subseteq \{\boldsymbol{x} \in \mathbb{Z}^N : A\boldsymbol{x} = 0\}.$$

Let $\mathcal{I}$ be the collection of all subsets I of $\{1, ..., N\}$ of cardinality J. For each $I \in \mathcal{I}$ let I' be its complement, i.e. $I' = \{1, ..., N\} \setminus I$, and let $\mathcal{I}' = \{I' : I \in \mathcal{I}\}$. Then

$$|\mathcal{I}| = \binom{N}{J} = \binom{N}{N-J} = |\mathcal{I}'|.$$

For each $I \in \mathcal{I}$, write X_I for the $J \times J$ submatrix of X consisting of all those rows of X which are indexed by I, and ${}_{I'}A$ for the $(N-J) \times (N-J)$ submatrix of A consisting of all those columns of A which are indexed by I'. By the duality principle of Brill-Gordan [12] (also see Theorem 1 on p. 294 of [14])

$$|\det(X_I)| = \gamma |\det({}_{I'}A)|, \tag{4}$$

for an appropriate $\gamma \in \mathbb{Q}$. Then define the vectors of *Grassmann coordinates* of X and A respectively to be

$$Gr(X) = (\det(X_I))_{I \in \mathcal{I}} \in \mathbb{Z}^{|I|}, \quad Gr(A) = (\det({}_{I'}A))_{I' \in \mathcal{I}'} \in \mathbb{Z}^{|I'|},$$

and so by (4)

$$H(Gr(X)) = \gamma H(Gr(A)).$$

Define height of Λ denoted by $H(\Lambda)$ to be $H(Gr(X))$. This definition is legitimate, since it does not depend on the choice of the basis for Λ. In particular, notice that if $N \geq 2$ and

$$L(X_1, ..., X_N) = \sum_{i=1}^{N} q_i X_i \in \mathbb{Z}[X_1, ..., X_N]$$

is a linear form with a non-zero coefficient vector $\boldsymbol{q}$ having relatively prime coordinates, and $\Lambda = \{\boldsymbol{x} \in \mathbb{Z}^N : L(\boldsymbol{x}) = 0\}$ is a sublattice of $\mathbb{Z}^N$ of rank $N-1$, then

$$H(\Lambda) = H(L) = H(\boldsymbol{q}). \tag{5}$$

We are now ready to proceed. Results of this paper also appear as a part of [11].

2. Basic bounds

In this section we prove the existence of integral points of small height and length at which a given polynomial in N variables of degree M does not vanish. Our bounds on height depend on M and N only. An application of results of this section is exhibited in [10].

First let

$$\mathcal{M}' = \mathcal{M}'(N, M) = \{\boldsymbol{m} \in \mathbb{Z}_{\geq 0}^N : m_1 + ... + m_N \leq M\}.$$

Then let

$$F(X_1, ..., X_N) = \sum_{\boldsymbol{m} \in \mathcal{M}'} f_{\boldsymbol{m}} X_1^{m_1} ... X_N^{m_N} \in \mathbb{Z}[X_1, ..., X_N],$$

be a polynomial (not necessarily homogeneous) in $N \geq 1$ variables of degree $M \geq 1$ with coefficients in $\mathbb{Z}$. We write $\deg_{X_i}(F)$ for degree of F in the variable X_i for each $1 \leq i \leq N$, and $\deg(F)$ for the total degree of F. Let

$$m(F) = \max_{1 \leq i \leq N} \deg_{X_i}(F),$$

then $m(F) \leq \deg(F) = M$.

Lemma 2.1. *Suppose $F(\boldsymbol{X})$ is not identically 0. Let $S \subset \mathbb{C}$ be a finite set of cardinality at least $m(F) + 1$. Then there exists $\boldsymbol{x} \in S^N$ such that $F(\boldsymbol{x}) \neq 0$.*

This is an immediate corollary of Lemma 1 on p. 261 of [5]. Notice that the assertion of Lemma 2.1 is best possible (i.e. $|S|$ *must* be at least $m(F) + 1$) as seen on the following example. Let $S = \{\alpha_1, ..., \alpha_M\} \subset \mathbb{Z}$, and let

$$F(X_1, ..., X_N) = \sum_{i=1}^{N} \prod_{j=1}^{M} (X_i - \alpha_j).$$

Then for each $\boldsymbol{x} \in S^N$ we have $F(\boldsymbol{x}) = 0$, where $m(F) = M = |S|$.

Lemma 2.2. *Let F be as in Lemma 2.1. There exists $\boldsymbol{x} \in \mathbb{Z}^N$ with $\boldsymbol{x}_i \neq 0$ for all $1 \leq i \leq N$, $F(\boldsymbol{x}) \neq 0$, and*

$$H(\boldsymbol{x}) \leq \frac{M+2}{2}. \tag{6}$$

Moreover, if F is homogeneous, then the upper bound of (6) can be replaced with $\frac{M+1}{2}$.

Proof. Recall that $M \geq m(F)$, and let

$$S = \left\{ -\left[\frac{M}{2}\right] - 1, ..., -1, 1, ..., \left[\frac{M}{2}\right] + 1 \right\},$$

then $|S| = 2\left(\left[\frac{M}{2}\right] + 1\right) \geq M + 1$. Hence, by Lemma 2.1, there must exist $\boldsymbol{x} \in S^N$ such that $F(\boldsymbol{x}) \neq 0$.

Now assume that F is homogeneous and $M \geq 1$. Notice that if for any $1 \leq i \leq N$ the "diagonal" coefficient $f_{M\boldsymbol{e}_i} \neq 0$, then $F(\boldsymbol{e}_i) = f_{M\boldsymbol{e}_i} \neq 0$, and we are done. Hence assume $f_{M\boldsymbol{e}_i} = 0$ for all $1 \leq i \leq N$. Then each monomial of F has degree M and is a product of powers of at least two variables. Therefore $m(F) \leq M - 1$, and so we can take

$$S = \left\{ -\left[\frac{M-1}{2}\right] - 1, ..., -1, 1, ..., \left[\frac{M-1}{2}\right] + 1 \right\},$$

then $|S| = 2\left(\left[\frac{M-1}{2}\right]+1\right) \geq M \geq m(F)+1$. Hence, by Lemma 2.1, there must exist $\boldsymbol{x} \in S^N$ such that $F(\boldsymbol{x}) \neq 0$. This completes the proof. □

Next we want to produce a bound on length of an integral point at which F does not vanish. Consider $\boldsymbol{x}$ of Lemma 2.2. Notice that

$$\mathcal{L}(\boldsymbol{x}) \leq NH(\boldsymbol{x}) \leq \frac{N(M+2)}{2}. \tag{7}$$

This is a trivial bound. We will produce a non-trivial bound on $\mathcal{L}(\boldsymbol{x})$ in a slightly more restrictive situation. Let $N \geq 2$, $M \geq 1$ be integers, and write

$$\mathcal{M} = \mathcal{M}(N, M) = \left\{\boldsymbol{m} \in \mathbb{Z}_+^N : m_1 + ... + m_N = M\right\}.$$

For the rest of this section, let

$$F(X_1, ..., X_N) = \sum_{\boldsymbol{m} \in \mathcal{M}} f_{\boldsymbol{m}} X_1^{m_1} ... X^{m_N} \in \mathbb{Z}[X_1, ..., X_N],$$

be a non-zero homogeneous polynomial in N variables of degree M with coefficients in $\mathbb{Z}$.

Lemma 2.3. *Let F be as above. There exists a point $\boldsymbol{x} \in \mathbb{Z}^N$ such that $F(\boldsymbol{x}) \neq 0$, and $\mathcal{L}(\boldsymbol{x}) \leq \frac{(M+2)^2}{8}$.*

Proof. If $M = 1$, then F is just a linear form in $N \geq 2$ variables. Its nullspace has dimension $N-1$, and so cannot contain all the standard basis vectors. Therefore there exists $\boldsymbol{x} \in \mathbb{Z}^N$ with $\mathcal{L}(\boldsymbol{x}) = 1$ and $F(\boldsymbol{x}) \neq 0$. From now on assume that $M \geq 2$. We can also assume that for each $1 \leq i \leq N$, the coefficient $f_{M\boldsymbol{e}_i} = 0$, where $\boldsymbol{e}_1, ..., \boldsymbol{e}_N$ are the standard basis vectors, since if for some $1 \leq i \leq N$, $f_{M\boldsymbol{e}_i} \neq 0$, then $F(\boldsymbol{e}_i) = f_{M\boldsymbol{e}_i} \neq 0$.

We argue by induction on N. First suppose that $N = 2$, then we can write

$$F(X_1, X_2) = \sum_{i=1}^{M-1} f_i X_1^i X_2^{M-i} = X_1 X_2 \sum_{i=1}^{M-1} f_i X_1^{i-1} X_2^{M-i-1},$$

and so $\frac{1}{X_1} F(X_1, 1) = \sum_{i=1}^{M-1} f_i X_1^{i-1}$ is a polynomial in one variable of degree at most $M-2$, therefore it can have at most $M-2$ nonzero roots, and so there must exist an integer β with $|\beta| \leq \frac{M-2}{2} + 1$ such that $F(\beta, 1) \neq 0$. Then $\boldsymbol{x} = (\beta, 1)$ is the required point with

$$\mathcal{L}(\boldsymbol{x}) \leq \frac{M+2}{2} \leq \frac{(M+2)^2}{8},$$

since $M \geq 2$.

Next assume $N > 2$. For each $1 \leq i \leq N$, define F_i, *i-th section of F*, to be the homogeneous polynomial in $N-1$ variables of degree M obtained from F by setting i-th variable equal to 0. First suppose that all sections of F are identically zero, then

$$F(X_1, ..., X_N) = X_1 ... X_N G(X_1, ..., X_N),$$

where G is a homogeneous polynomial of degree $M - N$ (this is only possible if $N \leq M$). By Lemma 2.2 and (7), there exists $\boldsymbol{x} \in \mathbb{Z}^N$ such that $x_j \neq 0$ for all $1 \leq j \leq N$, $G(\boldsymbol{x}) \neq 0$, and

$$\mathcal{L}(\boldsymbol{x}) \leq \frac{N}{2}(M - N + 2).$$

Then $F(\boldsymbol{x}) \neq 0$. Let

$$f(z) = \frac{z}{2}(M - z + 2) = -\frac{1}{2}z^2 + \frac{(M+2)}{2}z,$$

then f achieves its maximum when $z = \frac{M+2}{2}$, and this maximum value is $\frac{(M+2)^2}{8}$. Hence

$$\mathcal{L}(\boldsymbol{x}) \leq \frac{(M+2)^2}{8}. \tag{8}$$

Next assume that for some $1 \leq i \leq N$, F_i is not identically zero. Then we are done by the inductive hypothesis. This completes the proof. □

Notice that observations of (7) and Lemma 2.3 can be summarized as follows.

Proposition 2.4. *Let F be as above. There exists a point $\boldsymbol{x} \in \mathbb{Z}^N$ such that $F(\boldsymbol{x}) \neq 0$, and*

$$\mathcal{L}(\boldsymbol{x}) \leq \left[\frac{(M+2)}{2} \ \min\left\{N, \frac{M+2}{4}\right\}\right], \tag{9}$$

where [ ], as above, stands for the integer part function.

Notice that if F is irreducible, then the bound of Proposition 2.4 can be trivially improved by replacing N with $N-1$ in the upper bound, since we can set any one variable equal to zero without making an irreducible polynomial identically zero.

3. Lattice points in an aligned box

In the next two sections we produce estimates for the number of points of a sublattice of the integer lattice in a closed cube in $\mathbb{R}^N$. These estimates are later used to prove our main theorem.

Let $A = (a_{mn})$ be an $N \times N$, uppertriangular, nonsingular matrix with real entries. Let $u_m < v_m$ for $m = 1, 2, \ldots, N$ and write

$$B(\boldsymbol{u}, \boldsymbol{v}) = \{\boldsymbol{x} \in \mathbb{R}^N : u_m < x_m \leq v_m\}.$$

We will be interested in estimating the number of points $\boldsymbol{\xi}$ in $\mathbb{Z}^N$ such that $A\boldsymbol{\xi}$ belongs to the aligned box $B(\boldsymbol{u}, \boldsymbol{v})$. To begin with we have the following special result.

Lemma 3.1. *Assume that $a_{11} = a_{22} = \cdots = a_{NN} = 1$ and $v_m - u_m$ is a positive integer for each $m = 1, 2, \ldots, N$. Then*

$$|\{\boldsymbol{\xi} \in \mathbb{Z}^N : A\boldsymbol{\xi} \in B(\boldsymbol{u}, \boldsymbol{v})\}| = \prod_{m=1}^{N} (v_m - u_m). \tag{10}$$

Proof. We argue by induction on N. If $N = 1$ the result is trivial because one easily checks that the number of integer points ξ_1 such that $u_1 < \xi_1 \leq v_1$ is equal to $[v_1] - [u_1]$. As $v_1 - u_1$ is an integer we find that $[v_1] - [u_1] = v_1 - u_1$.

Now assume that $N \geq 2$. Let $\boldsymbol{\eta}$ be a point in $\mathbb{Z}^{N-1}$ with coordinates indexed by $n = 2, 3, \ldots, N$. Then define

$$I_{N-1} = \{\boldsymbol{\eta} \in \mathbb{Z}^{N-1} : u_m < \sum_{n=m}^{N} a_{mn}\eta_n \leq v_m \text{ for } m = 2, 3, \ldots, N\}.$$

By the inductive hypothesis we have

$$|I_{N-1}| = \prod_{m=2}^{N} (v_m - u_m). \tag{11}$$

If $\boldsymbol{\eta}$ is a point in I_{N-1} then the number of integer points ξ_1 such that

$$u_1 < \xi_1 + a_{12}\eta_2 + a_{13}\eta_3 + \cdots + a_{1N}\eta_N \le v_1, \tag{12}$$

is $v_1 - u_1$. Clearly a point

$$\boldsymbol{\xi} = \begin{pmatrix} \xi_1 \\ \eta_2 \\ \vdots \\ \eta_N \end{pmatrix}$$

satisfies the condition $A\boldsymbol{\xi} \in B(\boldsymbol{u}, \boldsymbol{v})$ if and only if $\boldsymbol{\eta} \in I_{N-1}$ and ξ_1 satisfies (12). We have shown that the number of such points is

$$(v_1 - u_1)|I_{N-1}|,$$

and this proves the lemma. □

If we drop the condition that each edge length $v_m - u_m$ is an integer then we get the following estimates.

Lemma 3.2. *Assume that $a_{11} = a_{22} = \cdots = a_{NN} = 1$, then*

$$\prod_{m=1}^{N} [v_m - u_m] \le |\{\boldsymbol{\xi} \in \mathbb{Z}^N : A\boldsymbol{\xi} \in B(\boldsymbol{u}, \boldsymbol{v})\}| \le \prod_{m=1}^{N} ([v_m - u_m] + 1). \tag{13}$$

Proof. When proving the lower bound on the left of (13) we can assume that $1 \le v_m - u_m$ for each $m = 1, 2, \ldots, N$. Now select real numbers u'_m and v'_m so that

$$u_m \le u'_m < v'_m \le v_m \quad \text{and} \quad v'_m - u'_m = [v_m - u_m], \quad \text{for} \quad m = 1, 2, \ldots, N.$$

As $B(\boldsymbol{u}', \boldsymbol{v}') \subseteq B(\boldsymbol{u}, \boldsymbol{v})$ the inequality follows from Lemma 3.1. To obtain the upper bound on the right of (13) we argue in essentially the same way. Select real numbers u''_m and v''_m so that

$$u''_m \le u_m < v_m \le v''_m \quad \text{and} \quad v''_m - u''_m = [v_m - u_m] + 1, \quad \text{for} \quad m = 1, 2, \ldots, N.$$

Then $B(\boldsymbol{u}, \boldsymbol{v}) \subseteq B(\boldsymbol{u}'', \boldsymbol{v}'')$, and again the inequality follows from Lemma 3.1. □

Next we drop the condition that the diagonal entries of the matrix A are all equal to 1.

Corollary 3.3. *Assume that the diagonal entries $a_{11}, a_{22}, \ldots, a_{NN}$ are all positive. Then we have*

$$\prod_{m=1}^{N} \Big[\frac{v_m - u_m}{a_{mm}}\Big] \le |\{\boldsymbol{\xi} \in \mathbb{Z}^N : A\boldsymbol{\xi} \in B(\boldsymbol{u}, \boldsymbol{v})\}| \le \prod_{m=1}^{N} \Big(\Big[\frac{v_m - u_m}{a_{mm}}\Big] + 1\Big). \tag{14}$$

4. Lattice points in cubes

In this section we focus on the case when the box of section 3 is actually a cube, and in this case extend the estimate of section 3 to lattices of not full rank.

For the rest of this section, let $R \geq 1$, and define

$$C_R^N = \{\boldsymbol{x} \in \mathbb{R}^N : \max_{1 \leq i \leq N} |x_i| \leq R\},$$

to be a cube in $\mathbb{R}^N$ centered at the origin with sidelength $2R$. Given a lattice $\Lambda \subseteq \mathbb{Z}^N$ of rank $N-l$ for $0 \leq l \leq N-1$ and determinant Δ, we want to estimate the number of points of Λ in C_R^N. First notice that if $\Lambda = A\mathbb{Z}^N$ has full rank, and matrix A as in section 3 has fixed determinant Δ, then the right hand side of (14) takes its maximum value when $a_{mm} = 1$ for $N-1$ distinct values of m. This leads to the following corollary.

Corollary 4.1. *Let $\Lambda \subseteq \mathbb{Z}^N$ be a lattice of full rank in $\mathbb{R}^N$ of determinant Δ. Then for each point $\boldsymbol{z}$ in $\mathbb{R}^N$ we have*

$$|\Lambda \cap (C_R^N + \boldsymbol{z})| \leq \left(\frac{2R}{\Delta} + 1\right)(2R+1)^{N-1}. \tag{15}$$

Moreover, if R is a positive integer multiple of Δ, we have

$$\frac{(2R)^N}{\Delta} \leq |\Lambda \cap (C_R^N + \boldsymbol{z})|. \tag{16}$$

Now suppose that Λ of Corollary 4.1 is not of full rank. The bounds we produce next, as well as the bound of Corollary 4.1, depend only on the lattice, not on the choice of the basis as in (14).

Theorem 4.2. *Suppose that $\Lambda \subseteq \mathbb{Z}^N$ is a lattice of rank $N-l$, where $1 \leq l \leq N-1$. Let Δ be the maximum of absolute values of Grassmann coordinates of Λ, that is $\Delta = H(\Lambda)$. Then for each point $\boldsymbol{z}$ in $\mathbb{R}^N$ we have*

$$|\Lambda \cap (C_R^N + \boldsymbol{z})| \leq \left(\frac{2R}{\Delta} + 1\right)(2R+1)^{N-l-1}. \tag{17}$$

Proof. Pick $\boldsymbol{e}_{k_1}, ..., \boldsymbol{e}_{k_l}$ such that the lattice

$$\mathrm{span}_{\mathbb{Z}}\{\Lambda, \boldsymbol{e}_{k_1}, ..., \boldsymbol{e}_{k_l}\} \subseteq \mathbb{Z}^N$$

has rank N. Write $X = (\boldsymbol{x}_1 \dots \boldsymbol{x}_{N-l})$ for the $N \times (N-l)$ basis matrix of Λ. Let $\boldsymbol{k} = (k_1, ..., k_l)$, and let $\Delta_{\boldsymbol{k}}$ be absolute value of the $\boldsymbol{k}$-th Grassmann coordinate of X and so of Λ (i.e. $\Delta_{\boldsymbol{k}}$ is absolute value of the $(N-l) \times (N-l)$ subdeterminant of X obtained by removing the rows numbered $k_1, ..., k_l$; this is an invariant of the lattice). Let $L_{k_1}, ..., L_{k_l}$ be distinct prime numbers so that $L_{k_i} \nmid \Delta_{\boldsymbol{k}}$ for each $1 \leq i \leq l$. Define

$$\Omega_{\boldsymbol{k}} = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, ..., \boldsymbol{x}_{N-1}, L_{k_1}\boldsymbol{e}_{k_1}, ..., L_{k_l}\boldsymbol{e}_{k_l}\}. \tag{18}$$

Then $\Lambda \subset \Omega_{\boldsymbol{k}} \subseteq \mathbb{Z}^N$, $\Lambda \neq \Omega_{\boldsymbol{k}}$, and $\Omega_{\boldsymbol{k}}$ is a lattice of rank N. Notice that $\boldsymbol{e}_{k_1}, ..., \boldsymbol{e}_{k_l} \notin \Omega_{\boldsymbol{k}}$.

Choose an integer basis $\boldsymbol{\alpha}_1, ..., \boldsymbol{\alpha}_N$ for $\Omega_{\boldsymbol{k}}$ so that the $N \times N$ basis matrix $A = (\boldsymbol{\alpha}_1 \dots \boldsymbol{\alpha}_N)$ is upper triangular, and

$$0 \leq a_{nj} < a_{nn} \ \ \forall\, 1 \leq n \leq N,\ 1 \leq j \leq N,\ j \neq n. \tag{19}$$

Such a basis for $\Omega_{\boldsymbol{k}}$ exists uniquely by Corollary 1 on p. 13 of [5]. Notice that

$$\det(\Omega_{\boldsymbol{k}}) = \Delta_{\boldsymbol{k}} \prod_{i=1}^{l} L_{k_i} = |\det(A)| = \prod_{n=1}^{N} a_{nn}.$$

Fix an s, $1 \leq s \leq l$. Since L_{k_s} is prime, $L_{k_s} | a_{nn}$ for some $1 \leq n \leq N$, and since $L_{k_s} \nmid \Delta_{\boldsymbol{k}}$ this is the only a_{nn} that L_{k_s} divides. Since $L_{k_s} \boldsymbol{e}_{k_s} \in \Omega_{\boldsymbol{k}}$ and A is upper triangular, there must exist integers $\alpha_{s1}, ..., \alpha_{sN}$ such that

$$L_{k_s} = \sum_{i=k_s}^{N} \alpha_{si} a_{ik_s}, \quad 0 = \sum_{i=j}^{N} \alpha_{si} a_{ij}, \ \forall\, j \neq k_s.$$

Case 1. Suppose $k_s = N$. Then $L_N = \alpha_{sN} a_{NN}$, which implies that either $\alpha_{sN} = L_N,\ a_{NN} = 1$, or $\alpha_{sN} = 1,\ a_{NN} = L_N$. However, if $a_{NN} = 1$, then by (19) $a_{Ni} = 0$ for all $1 \leq i \leq N-1$, and so $\boldsymbol{\alpha}_N = \boldsymbol{e}_N \in \Omega_{\boldsymbol{k}}$, which is a contradiction. Therefore $a_{NN} = L_N$.

Case 2. Suppose $k_s < N$. Then $\alpha_{sN} a_{NN} = 0$, and so $\alpha_{sN} = 0$. Then

$$\alpha_{s(N-1)} a_{(N-1)(N-1)} + \alpha_{sN} a_{N(N-1)} = 0,$$

which means that $\alpha_{s(N-1)} = 0$. Continuing in the same manner, we see that $\alpha_{si} = 0$ for each $i > k_s$. Hence $L_{k_s} = \sum_{i=k_s}^{N} \alpha_{si} a_{ik_s} = \alpha_{sk} a_{k_s k_s}$. By the same argument as in case 1, this means that $a_{k_s k_s} = L_{k_s}$.

Therefore we proved that $a_{k_s k_s} = L_{k_s}$ for all $1 \leq s \leq l$, and each L_{k_s} does not divide any other a_{nn}, hence

$$\prod_{n=1, n \neq k_1, ..., k_l}^{N} a_{nn} = \Delta_{\boldsymbol{k}}. \tag{20}$$

Applying Corollary 4.1, we see that for any $\boldsymbol{z} \in \mathbb{R}^N$,

$$\begin{aligned} |\Lambda \cap (C_R^N + \boldsymbol{z})| &\leq |\Omega_{\boldsymbol{k}} \cap (C_R^N + \boldsymbol{z})| \\ &\leq \prod_{s=1}^{l} \left(\frac{2R}{L_{k_s}} + 1 \right) \prod_{n=1, n \neq k_1, ..., k_l}^{N} \left(\frac{2R}{a_{nn}} + 1 \right). \end{aligned} \tag{21}$$

Since our choice of $L_{k_1}, ..., L_{k_l}$ was arbitrary, we will now let $L_{k_s} \to \infty$ for all $1 \leq s \leq l$, and so

$$\begin{aligned} |\Lambda \cap (C_R^N + \boldsymbol{z})| &\leq \prod_{n=1, n \neq k_1, ..., k_l}^{N} \left(\frac{2R}{a_{nn}} + 1 \right) \prod_{s=1}^{l} \lim_{L_{k_s} \to \infty} \left(\frac{2R}{L_{k_s}} + 1 \right) \\ &= \prod_{n=1, n \neq k_1, ..., k_l}^{N} \left(\frac{2R}{a_{nn}} + 1 \right). \end{aligned} \tag{22}$$

The right hand side of (22) takes its maximum value when $a_{nn} = 1$ for $N - l - 1$ distinct values of n. Therefore, applying (20) we obtain

$$|\Lambda \cap (C_R^N + \boldsymbol{z})| \leq \left(\frac{2R}{\Delta_{\boldsymbol{k}}} + 1 \right) (2R+1)^{N-l-1}. \tag{23}$$

We can now specify how we select $\boldsymbol{k}$. We want to do it so that the upper bound in (23) is minimized. For this, let $\boldsymbol{k}$ be such that $\Delta_{\boldsymbol{k}}$ is the maximal among all the Grassmann coordinates of Λ, and call this maximum value Δ (notice that if

$\Delta_k \neq 0$, then the lattice $\mathrm{span}_{\mathbb{Z}}\{\Lambda, \boldsymbol{e}_{k_1}, ..., \boldsymbol{e}_{k_l}\} \subseteq \mathbb{Z}^N$ has rank N). This completes the proof. □

The upper bounds in (15) and (17) are best possible as seen on the example of

$$\Lambda = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{e}_1, ..., \boldsymbol{e}_{N-l-1}, \Delta \boldsymbol{e}_{N-l}\},$$

where $0 \leq l \leq N-1$.

Theorem 4.3. *Suppose that $\Lambda \subseteq \mathbb{Z}^N$ is a lattice of rank $N-l$, where $1 \leq l \leq N-1$. Let Δ be the maximum of absolute values of Grassmann coordinates of Λ. Then for every R that is a positive integer multiple of $(N-l)\Delta$, we have*

$$\frac{(2R)^{N-l}}{(N-l)^{N-l}\Delta} \leq |\Lambda \cap C_R^N|. \tag{24}$$

Proof. Pick a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_{N-l}$ for Λ and write $X = (\boldsymbol{x}_1 \ ... \ \boldsymbol{x}_{N-l})$ for the corresponding $N \times (N-l)$ basis matrix. Let A be an $l \times N$ matrix such that $A\boldsymbol{x} = \boldsymbol{0}$ for each $\boldsymbol{x} \in \Lambda$. Write $\Delta_{i_1 \dots i_{N-l}}$ for the Grassmann coordinate of X, which is the determinant of the submatrix of X whose rows are indexed by $i_1, ..., i_{N-l} \in \{1, ..., N\}$. Write $\delta^{j_1 \dots j_l}$ for the Grassmann coordinate of A, which is the determinant of the submatrix of A whose columns are indexed by $j_1, ..., j_l \in \{1, ..., N\}$. By the duality principle of Brill-Gordan [12] (also see Theorem 1 on p. 294 of [14]) we have

$$\Delta_{i_1 \dots i_{N-l}} = (-1)^{i_1 + \dots + i_{N-l}} \ \gamma \ \delta^{i_{N-l+1} \dots i_N}, \tag{25}$$

for an appropriate $\gamma \in \mathbb{R}$, where $\{i_1, ..., i_{N-l}, i_{N-l+1}, ..., i_N\} = \{1, ..., N\}$. We can assume without loss of generality that

$$\Delta = |\Delta_{1 \dots (N-l)}| = |\gamma||\delta^{(N-l+1) \dots N}|. \tag{26}$$

Let X' be the $(N-l) \times (N-l)$ submatrix of X whose rows are indexed by $1, ..., (N-l)$, and let Λ' be a lattice of full rank in $\mathbb{R}^{N-l}$ generated by the column vectors of X'. Then $\det(\Lambda') = \det(X') = \Delta$, and so, by the lower bound of Corollary 4.1

$$|\Lambda' \cap C_R^{N-l}| \geq \frac{(2R)^{N-l}}{\Delta}. \tag{27}$$

Suppose that $\boldsymbol{y} = (y_1, ..., y_{N-l}) \in \Lambda' \cap C_R^{N-l}$, then $|\boldsymbol{y}| \leq R$, where $R \geq 1$. There exists $\boldsymbol{z} = (z_1, ..., z_l) \in \mathbb{R}^l$ such that $(\boldsymbol{y}, \boldsymbol{z}) = (y_1, ..., y_{N-l}, z_1, ..., z_l) \in \Lambda$. We want to establish an upper bound on $|\boldsymbol{z}|$. By equation (4) on page 293 of [14], every point $\boldsymbol{x} \in \Lambda$ must satisfy the following system of linear equations:

$$\sum_{j=1}^{N} \delta^{i_1 \dots i_{l-1} j} x_j = 0, \tag{28}$$

where $i_1, ..., i_{l-1}$ assume all possible values; only $N-l$ of these equations are linearly independent. It is easy to see that the sum on the left side of each equation like (28) has only $N-l+1$ terms: there are only $N-l+1$ possibilities for j since the $l-1$ values $i_1, ..., i_{l-1}$ have been preassigned. For each $N-l+1 \leq i \leq N$ let $I_i = \{N-l+1, ..., N\} \setminus \{i\}$, then the following l equations form a subset of equations in (28):

$$\sum_{j=1}^{N-l} \delta^{I_i j} x_j + \delta^{(N-l+1) \dots N} x_i = 0. \tag{29}$$

Substitute the coordinates of the point $(\boldsymbol{y}, \boldsymbol{z})$ into (29), then we see that for each $1 \leq i \leq l$

$$z_i = -\sum_{j=1}^{N-l} \frac{\delta^{I_{(N-l+i)}j}}{\delta^{(N-l+1)\ldots N}} y_j, \tag{30}$$

and so

$$|z_i| \leq \sum_{j=1}^{N-l} \left| \frac{\delta^{I_{(N-l+i)}j}}{\delta^{(N-l+1)\ldots N}} \right| |y_j| \leq (N-l)R, \tag{31}$$

since each $\left| \frac{\delta^{I_{(N-l+i)}j}}{\delta^{(N-l+1)\ldots N}} \right| \leq 1$ by construction, since $\delta^{(N-l+1)\ldots N}$ is the biggest in absolute value among all the Grassmann coordinates of A, and $|\boldsymbol{y}| \leq R$. Therefore for each $\boldsymbol{y} \in \Lambda' \cap C_R^{N-l}$ there exists $\boldsymbol{z} \in \mathbb{R}^l$ such that $(\boldsymbol{y}, \boldsymbol{z}) \in \Lambda \cap C_{(N-l)R}^N$, hence

$$|\Lambda \cap C_R^N| \geq |\Lambda' \cap C_{\frac{R}{N-l}}^{N-l}| \geq \frac{(2R)^{N-l}}{(N-l)^{N-l}\Delta}. \tag{32}$$

This completes the proof. □

Notice that the entire argument in the proof of Theorem 4.2, except for (27), holds even if we drop the assumptions that $\Lambda \subseteq \mathbb{Z}^N$ and that R is a positive integer multiple of $(N-l)\Delta$. In particular, this is true for (32).

Remark. The problem of counting lattice points in compact domains has been studied extensively. A long list of contributions on this subject can, for instance, be found in the supplement iv of Chapter 2 (pages 140 - 147) of [13]. The vast majority of such results is asymptotic in nature, which is not sufficient for our purposes. Explicit bounds on the number of lattice points in convex bodies can be found for instance in [17] and [20], however these bounds are, although quite general in the choice of the convex body, depend on parameters which are hard to compute. The advantage of bounds developed here in sections 3 and 4 is that they are reasonably sharp and easy to use in the particular case needed for our main result.

5. Points outside of a collection of sublattices

In this section we consider Problem 2 and Problem 3. Throughout this section $N \geq 2$. Given a sublattice Ω of $\mathbb{Z}^N$ and a collection of proper sublattices $\Lambda_1, ..., \Lambda_M$ of Ω we want to prove the existence of a non-zero integral point of small height in $\Omega \setminus \bigcup_{i=1}^M \Lambda_i$.

We start with a discussion of Problem 2, namely the case when $\Omega = \mathbb{Z}^N$ and $\Lambda_1, ..., \Lambda_M$ are sublattices of $\mathbb{Z}^N$ of rank $N-1$. If these sublattices are maximal, there exist uniquely (up to $\pm$ sign) non-zero linear forms $L_1(\boldsymbol{X}), ..., L(\boldsymbol{X})$ in N variables with integer relatively prime coeffcients such that

$$\Lambda_i = \{\boldsymbol{y} \in \mathbb{Z}^N : L_i(\boldsymbol{y}) = 0\}.$$

Then, given such a collection of linear forms, we want to prove the existence of an integer lattice point at which none of these linear forms would vanish.

A basic bound that depends only on the number of linear forms follows from results of section 2. Take $F(\boldsymbol{X}) = L_1(\boldsymbol{X}) \cdots L_M(\boldsymbol{X})$. By Lemma 2.2, there exists

an integer lattice point $\boldsymbol{x}$ such that $F(\boldsymbol{x}) \neq 0$, and so $L_i(\boldsymbol{x}) \neq 0$ for all $1 \leq i \leq N$, with

$$H(\boldsymbol{x}) \leq \frac{M+1}{2}. \tag{33}$$

Moreover, a bound of the form $H(\boldsymbol{x}) \ll_N M^{(N-1)/N}$ follows from [2], however the constant there is not explicit.

We want to produce a result that depends on the actual linear forms, not just on their number. We will obtain such a result as a corollary of Theorem 1.1, which presents a solution to the more general Problem 3. Namely, we prove the existence of a point of small height in a sublattice of the integer lattice outside of a collection of its proper sublattices. We will now relate this problem to the lattice point counting problem of sections 3 and 4 to prove our main theorem.

Proof of Theorem 1.1. For each $1 \leq i \leq M$ let l_i be the rank of lattice Λ_i, then $0 < l_i < J$. Define a counting function of a variable R, which is a positive integer multiple of $JH(\Omega)$, by

$$f_\Omega(R) = |\Omega \cap C_R^N| - \left|\bigcup_{i=1}^M \Lambda_i \cap C_R^N\right|, \tag{34}$$

then

$$\begin{aligned} f_\Omega(R) &\geq |\Omega \cap C_R^N| - \sum_{i=1}^M |\Lambda_i \cap C_R^N| \\ &\geq \frac{(2R)^J}{J^J H(\Omega)} - \sum_{i=1}^M \left(\frac{2R}{H(\Lambda_i)} + 1\right)(2R+1)^{l_i - 1}, \end{aligned} \tag{35}$$

where the last inequality follows by Corollary 4.1, Theorem 4.2, and Theorem 4.3. Notice that $f_\Omega(R) > 0$ if and only if there exists a point $\boldsymbol{x} \in \Omega \setminus \bigcup_{i=1}^M \Lambda_i$ with $H(\boldsymbol{x}) \leq R$. Hence ideally we want to find R, the smallest positive integer multiple of $JH(\Omega)$, so that $f_\Omega(R) > 0$. Recall that $l_i \leq J-1$ for each i. Then using (35), we have

$$f_\Omega(R) \geq R^{J-2}\left\{\left(\frac{2^J}{J^J H(\Omega)}\right)R^2 - 3^{J-1}\left(\sum_{i=1}^M \frac{1}{H(\Lambda_i)}\right)R - 3^{J-2}M\right\}.$$

Therefore we want to solve for R a quadratic inequality

$$\left(\frac{2^J}{J^J H(\Omega)}\right)R^2 - 3^{J-1}\left(\sum_{i=1}^M \frac{1}{H(\Lambda_i)}\right)R - 3^{J-2}M > 0. \tag{36}$$

It is not difficult to deduce from (36) that we can take R to be a positive integer multiple of $JH(\Omega)$ such that

$$R \geq \left(\frac{3}{2}\right)^{J-1} J^J \left\{\sum_{i=1}^M \frac{1}{H(\Lambda_i)} + \sqrt{M}\right\} H(\Omega). \tag{37}$$

This completes the proof. □

The dependence on $H(\Omega)$, $H(\Lambda_i)$ for each i, and on M in the upper bound of Theorem 1.1 seems to be best possible. Let $M = 1$, and take Λ_1 to be a sublattice of Ω of rank $J-1$ generated by the vectors corresponding to the first $J-1$ successive

minima of Ω with respect to a unit cube. Then the smallest vector in $\Omega \setminus \Lambda_1$ will be the one corresponding to the J-th successive minimum, and its height can be approximated by $H(\Omega)$. The dependence on $H(\Lambda_i)$ is sharp because it comes from the upper bounds on the number of lattice points in a cube (see (15) and (17)), which are best possible. Finally, the proof of Theorem 1.1 (specifically see (36)) suggests that dependence on M is essentially sharp.

Also notice that since Problem 2 is a special case of Problem 3, a solution to it follows from Theorem 1.1 when $J = N$, i.e. $\Omega = \mathbb{Z}^N$, and $l_i = N - 1$ for all $1 \le i \le M$. In this case we obtain a point $\boldsymbol{x} \in \mathbb{Z}^N$ such that $\boldsymbol{x} \notin \bigcup_{i=1}^M \Lambda_i$ and

$$H(\boldsymbol{x}) \le \left(\frac{3}{2}\right)^{N-1} N^N \left\{ \sum_{i=1}^M \frac{1}{H(\Lambda_i)} + \sqrt{M} \right\} + N.$$

Hence Theorem 1.1 can be thought of as a combination of Siegel's Lemma and its inverse problem of finding points of small height outside of a collection of sublattices.

In fact, a slightly better bound for the point in question in Problem 2 can be obtained from the proof of Theorem 1.1. Notice that if $\Omega = \mathbb{Z}^N$ then in the lower bound of (35) the quantity $\frac{(2R)^J}{J^J H(\Omega)} = \left(\frac{2R}{N}\right)^N$ can be replaced with the slightly larger $(2R+1)^N$, since $|\mathbb{Z}^N \cap C_R^N| = (2R+1)^N$ for positive integer values of R. This leads to the following slightly sharper bound.

Corollary 5.1. *Let $L_1(\boldsymbol{X}), ..., L_M(\boldsymbol{X}) \in \mathbb{Z}[X_1, ..., X_N]$ be non-zero linear forms with relatively prime coordinates. Then there exists $\boldsymbol{x} \in \mathbb{Z}^N$ such that $L_i(\boldsymbol{x}) \neq 0$ for every $i = 1, ..., M$ and*

$$H(\boldsymbol{x}) \le \sum_{i=1}^M \frac{1}{H(L_i)} + \sqrt{M}. \tag{38}$$

Corollary 5.1 produces a better bound than (33) for linear forms with suffciently large heights. Also, suppose that N is fixed and M grows. Then our collection must contain linear forms with relatively large heights, since there are only finitely many vectors of height $\le C$ in $\mathbb{Z}^N$ for each C. This is definitely the more interesting situation, since if $M < N$ or if the two are comparable, there must exist integer lattice points of height $\ll N$ at which the linear forms do not vanish.

Another immediate corollary of Theorem 1.1 in case when $M = 1$ is a sharper bound for a special case of Faltings' version of Siegel's Lemma (see [8], [15], and [7]).

Corollary 5.2. *Let V and W be real vector spaces of respective dimensions d_1 and d_2. Let $\Omega_1 = V \cap \mathbb{Z}^{d_1}$ and $\Omega_2 = W \cap \mathbb{Z}^{d_2}$. Let $\rho : V \longrightarrow W$ be a linear map such that $\rho(\Omega_1) \subseteq \Omega_2$. Let $U = \ker(\rho)$, and let $\Omega = U \cap \Omega_1$. Let J be the rank of Ω. Then for any subspace U_0 of U which does not contain Ω there exists a point $\boldsymbol{x} \in \Omega \setminus U_0$ such that*

$$H(\boldsymbol{x}) \le \left\{ 2J^J \left(\frac{3}{2}\right)^{J-1} + J \right\} H(\Omega). \tag{39}$$

Faltings' lemma is more general: it works with Ω_1, Ω_2, and Ω being any lattices in V, W, and U respectively, as well as any choice of norms on V and W (our height

is the sup-norm). However, the upper bound on $H(\boldsymbol{x})$ which follows from Faltings' lemma is

$$H(\boldsymbol{x}) \leq d_1^{\frac{1}{d-d_0}} H(\Omega)^{\frac{3d_1}{d-d_0}}, \tag{40}$$

where $d = \dim_{\mathbb{R}}(U)$ and $d_0 = \dim_{\mathbb{R}}(U_0)$, so that $d_1 > d > d_0$ and $d \geq J$. Faltings' method of proof is different from ours: it relies on Minkowski's theorem about successive minima.

6. Tarski plank problem

We now consider a simple application of our results to a certain analogue of the discrete version of the Tarski plank problem. First we provide some background. By a *plank* of width h in $\mathbb{R}^N$ we mean a strip of space of width h between two parallel $(N-1)$-dimensional hyperplanes. Let C be a convex body of minimal width w in $\mathbb{R}^N$. If C is covered by p planks of widths $h_1, ..., h_p$ respectively, is it true that $h_1 + ... + h_p \geq w$? This question was originally asked by Tarski in [18]. It was answered affirmitively by Bang in [1]. One can also ask for the minimal number of planks with prescribed widths that would cover C. The discrete version of this problem (see for instance [6]) asks for the minimal number of $(N-1)$-dimensional hyperplanes that would cover a convex set of lattice points in $\mathbb{R}^N$. We ask a somewhat different, but analogous question. Consider the set of all integer lattice points in $\mathbb{R}^N$ that are contained in the closed cube C_R^N, where R is a positive integer as above. This set has cardinality $(2R+1)^N$. What is the minimal number of sublattices of $\mathbb{Z}^N$ of rank $N-1$ required to cover this set? Let M be this number. Then the inequality

$$M \geq 2R - 1 \tag{41}$$

follows immediately from (33). For such a sublattice Λ let $L(\boldsymbol{X}) \in \mathbb{Z}[X_1, ..., X_N]$ be the linear form with relatively prime coefficients such that $\Lambda = \{\boldsymbol{y} \in \mathbb{Z}^N : L(\boldsymbol{y}) = 0\}$. An analogue of width of a plank in this case would be the quantity $H(L)^{-1} = H(\Lambda)^{-1}$, and the sidelength of the cube C_R^N which is equal to $2R$ is an analogue of the width of a convex body. Then we can state the following result, which is an immediate corollary of Corollary 5.1.

Corollary 6.1. *Let $\Lambda_1, ..., \Lambda_M$ be sublattices of $\mathbb{Z}^N$ of rank $N-1$ each, such that $C_R^N \cap \mathbb{Z}^N \subset \bigcup_{i=1}^M \Lambda_i$. Then*

$$\sum_{i=1}^{M} \frac{1}{H(\Lambda_i)} \geq R - \sqrt{M}. \tag{42}$$

A similar problem is treated in [2]. Let C be a compact convex body, which is symmetric with respect to the origin in $\mathbb{R}^N$. Suppose that C can be inscribed into a cube C_R^N as above. How many $(N-1)$-dimensional subspaces of $\mathbb{R}^N$ does it take to cover $C \cap \mathbb{Z}^N$, the set of integer lattice points contained in C? Call this number M. Theorem 2 of [2] provides an upper bound for M in terms of the successive minima of C with respect to $\mathbb{Z}^N$, which implies that M is of the order of magnitude $O(R^{N/(N-1)})$, which is better than (41). However, the actual constants

in the inequalities of [2] are not effectively computable, since they rely on successive minima. More precisely, Theorem 2 of [2] states that

$$M \leq c2^N N^2 \log N \min_{0<m<N} (\lambda_m \cdots \lambda_N)^{-\frac{1}{N-m}}, \tag{43}$$

where $0 < \lambda_1 \leq ... \leq \lambda_N \leq 1$ are the successive minima of C with respect to $\mathbb{Z}^N$ (the case $\lambda_N > 1$ is trivial: $M = 1$), and c is an absolute constant.

Aknowledgements. I would like to express my deep gratitude to Professor Jeffrey D. Vaaler for his valuable advice and numerous helpful conversations on the subject of this paper. In particular, the argument of section 3 was suggested by him. I would also like to thank Dr. Iskander Aliev and Professor Preda Mihailescu for their very helpful remarks.

References

[1] T. Bang. A solution of the "Plank Problem". *Amer. Math. Soc. Proceedings*, 2:990–993, 1951.
[2] I. Bárány, G. Harcos, J. Pach, and G. Tardos. Covering lattice points by subspaces. *Period. Math. Hungar.*, 43:93–103, 2001.
[3] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.
[4] D. Bump, K. K. Choi, P. Kurlberg, and J. D. Vaaler. A local Riemann hypothesis. I. *Math. Z.*, 233(1):1–19, 2000.
[5] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1959.
[6] C. Corzatt. Covering convex sets of lattice points with straight lines. *Proceedings of the Sundance conference on combinatorics and related topics. Congr. Numer.*, 150:129–135, 1985.
[7] B. Edixhoven. Arithmetic part of Faltings's proof. *Diophantine approximation and abelian varieties (Soesterberg, 1992)*, Lecture Notes in Math.(1566):97–110, 1993.
[8] G. Faltings. Diophantine approximation on abelian varieties. *Ann. of Math.*, 133(2):549–576, 1991.
[9] L. Fukshansky. Siegel's lemma with additional conditions. *submitted for publication*.
[10] L. Fukshansky. Small zeros of quadratic forms with linear conditions. *to appear in J. Number Theory*.
[11] L. Fukshansky. *Algebraic points of small height with additional arithmetic conditions*. PhD thesis, University of Texas at Austin, 2004.
[12] P. Gordan. Uber den grossten gemeinsamen factor. *Math. Ann.*, 7:443–448, 1873.
[13] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland Publishing Co., 1987.
[14] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume 1*. Cambridge Univ. Press, 1947.
[15] R. J. Kooman. Faltings's version of Siegel's lemma. *Diophantine approximation and abelian varieties (Soesterberg, 1992)*, Lecture Notes in Math.(1566):93–96, 1993.
[16] C. L. Siegel. Uber einige Anwendungen diophantischer Approximationen. *Abh. der Preuss. Akad. der Wissenschaften Phys.-math Kl.*, Nr. 1:209–266, 1929.
[17] P. G. Spain. Lipschitz: a new version of an old principle. *Bull. London Math. Soc.*, 27:565–566, 1995.
[18] A. Tarski. Further remarks about the degree of equivalence of polygons (in Polish). *Odbitka Z. Parametru.*, 2:310–314, 1932.
[19] A. Thue. Uber Annaherungswerte algebraischer Zahlen. *J. Reine Angew. Math.*, 135:284–305, 1909.
[20] J. L. Thunder. The number of solutions of bounded height to a system of linear equations. *J. Number Theory*, 43:228–250, 1993.

Department of Mathematics, Texas A&M University, College Station, Texas 77843-3368
E-mail address: lenny@math.tamu.edu