Shrinking integer lattices II

Robin J. Chapman

Department of Mathematics, University of Exeter, Exeter EX4 4QE, United Kingdom

Communicated by K.W. Gruenberg
Received 7 June 1991

Abstract


Given a sublattice \( \Lambda \) of rank \( k \), of the integer lattice \( \mathbb{Z}^k \) in Euclidean \( k \)-space, we ask the following question. What is the largest integer \( r \) such that there is a sublattice \( \Lambda' \) of \( \mathbb{Z}^r \) isometric to \( r^{-1/2} \Lambda \)? In this paper I give a complete solution if \( k \leq 7 \), and if \( k = 8 \), I determine \( r \) to within a factor of 2.

1. Introduction

This paper considers the following problem: Given a full sublattice \( \Lambda \) of the integer lattice \( \mathbb{Z}^k \) in Euclidean space, i.e. a sublattice of full rank \( k \), can we find a lattice \( \Lambda' \subseteq \mathbb{Z}^k \) which is similar to \( \Lambda \) and has a fundamental region of smaller volume? In particular, can we find the least such volume that the fundamental region of such a lattice can have?

This problem has been considered by Cremona and Landau [5] for \( k \leq 4 \) and by the present author [2] for \( k = 5 \). If the lattice \( \Lambda' \) is isometric to \( \lambda^{-1/2} \Lambda \), Cremona and Landau give an upper bound for the possible \( \lambda \) and show that it is attained for \( k \leq 4 \). In [2] the present author shows that the Cremona–Landau bound is attained when \( k = 5 \) but not for \( k = 6 \) or \( k \geq 8 \). In this paper, by using the theory of rational quadratic forms we obtain an improved bound for \( \lambda \) and prove that it is attained for \( k \leq 7 \) and that it is attained except possibly for a factor of 2 when \( k = 8 \). We use the classification of unimodular integral lattices in an essential way. Our methods, unlike the constructive approach of [2] and [5], are existential in character and the question of finding an algorithm to find the best \( \Lambda' \) for \( k > 5 \) remains open.
2. Preliminary results

Let \( \mathbb{R}^k \) be \( k \)-dimensional Euclidean space with the standard inner product \( (x, y) \mapsto x \cdot y \). A linear transformation \( T : \mathbb{R}^k \to \mathbb{R}^k \) is a similarity with scale factor \( \mu > 0 \) if \( Tx \cdot Ty = \mu^2 x \cdot y \) for all \( x, y \in \mathbb{R}^k \). If \( T \) is represented by the matrix \( M \) with respect to the standard basis, this condition is equivalent to \( M'M = \mu^2 I \). A similarity with scale factor 1 is called an isometry.

Consider a full sublattice \( \Lambda \) of \( \mathbb{Z}^k \) and a similarity \( T \) of scale factor \( \mu \) with \( TA \subseteq \mathbb{Z}^k \). The elements of \( \Lambda \) span all of \( \mathbb{Q}^k \) over \( \mathbb{Q} \) and so we see that \( T(\mathbb{Q}^k) = T(\mathbb{Q}\Lambda) = \mathbb{Q}TA \subseteq \mathbb{Q}^k \). Hence \( T \) is represented by a matrix \( M \in M_k(\mathbb{Q}) \) and so \( \mu^2 \in \mathbb{Q} \). Also, if \( x, y \in \Lambda \), then \( Tx, Ty \in \mathbb{Z}^k \) and so \( \mu^2 x \cdot y = Tx \cdot Ty \in \mathbb{Z} \). This shows that \( \mu^2 \) is a rational number whose denominator divides \( x \cdot y \). In particular, if \( g = \gcd(\{x \cdot y \mid x, y \in \Lambda\}) \), then the denominator of \( \mu^2 \) divides \( g \) and in particular \( \mu^2 \geq 1/g \). We have thus proved the following:

**Lemma 1.** Let \( \Lambda \) be a full sublattice of \( \mathbb{Z}^k \) and \( T \) a similarity of \( \mathbb{R}^k \) of scale factor \( \mu \) with \( TA \subseteq \mathbb{Z}^k \). Then \( \mu^2 \) is a rational number whose denominator divides \( g \).

3. Rational quadratic forms

To find a better bound than \( \mu^2 \geq 1/g \) we use the theory of rational quadratic forms (see [7] for definitions and notation). Let \( M = (a_{ij}) \subseteq M_k(\mathbb{Q}) \) satisfy \( M'M = \mu^2 I \) with \( \mu > 0 \). Clearly \( M \) is nonsingular. We now introduce indeterminates \( X_1, X_2, \ldots, X_k \) and put \( Y_i = \sum_j a_{ij}X_j \). It immediately follows that \( \sum_i Y_i^2 = \mu^2 \sum_i X_i^2 \) and so the quadratic forms \( Q(X_1, X_2, \ldots, X_k) = X_1^2 + X_2^2 + \cdots + X_k^2 \) and \( \mu^2 Q \) are equivalent over \( \mathbb{Q} \). Using the theory of rational quadratic forms we can characterize all \( t \in \mathbb{Q} \) for which \( Q \) and \( tQ \) are equivalent over \( \mathbb{Q} \).

**Proposition 2.** Let \( t \in \mathbb{Q} \). Then \( Q \) is equivalent to \( tQ \) over \( \mathbb{Q} \) if and only if the following conditions hold:

(i) If \( k \) is odd, then \( t \) is the square of a nonzero rational.

(ii) If \( k \) is even but not divisible by 4, then \( t > 0 \) and \( \text{ord}_p(t) \) is even for all primes \( p \equiv 3 \pmod{4} \).

(iii) If \( 4 \mid k \), then \( t > 0 \).

**Proof.** We use the Corollary to Theorem 9 in Chapter IV of [7]. This states that two rational quadratic forms are equivalent over \( \mathbb{Q} \) if and only if their ranks, signatures, discriminants and Hasse invariants at each prime are equal. In all cases as \( Q \) is positive definite \( tQ \) will have the same rank and signature as \( Q \) if and only if \( t > 0 \).
Now the discriminants are \( d(Q) = 1 \) and \( d(tQ) = t^k \). Note that these have to be interpreted as elements of \( \mathbb{Q}^*/\mathbb{Q}^{*2} \). If \( k \) is odd, then \( d(tQ) = t \) and this equals \( d(Q) \) modulo squares if and only if \( t \) is a square. Conversely, if \( t \) is a square, then \( Q \) and \( tQ \) are clearly equivalent over \( \mathbb{Q} \) and so (i) follows. If \( k \) is even, then \( d(tQ) = 1 \) and the discriminants are automatically equal.

Suppose then that \( k \) is even and \( t > 0 \). The Hasse invariants are
\[
\varepsilon_p(Q) = 1 \quad \text{and} \quad \varepsilon_p(tQ) = (t, t)^{k(k-1)/2}_p,
\]
where \((,)_p\) denotes the Hilbert symbol at the prime \( p \). If \( k \) is divisible by 4, then \( k(k-1)/2 \) is even and so \( \varepsilon_p(tQ) = 1 \) for all \( p \). Hence all the invariants of \( Q \) and \( tQ \) are equal and so \( Q \) and \( tQ \) are equivalent and (iii) follows.

If now \( k \equiv 2 \pmod{4} \), then \( k(k-1)/2 \) is odd and \( \varepsilon_p(tQ) = (t, t)_p \). By standard properties of the Hilbert symbol, \((t, t)_p = (-1, t)_p\). We now use Theorem 1 in Chapter III of [7] to evaluate \((t, t)_p\). If \( p \) is odd, the formula gives us
\[
(-1, t)_p = \left( -\frac{1}{p} \right)^{\text{ord}_p(t)}
\]
and so by quadratic reciprocity \( \varepsilon_p(tQ) = 1 \) if \( p = 1 \pmod{4} \) and \( \varepsilon_p(tQ) = (-1)^{\text{ord}_p(t)} \) if \( p = 3 \pmod{4} \). Hence if \( Q \) and \( tQ \) are equivalent, then \( \text{ord}_p(t) \) is even for all \( p = 3 \pmod{4} \). Conversely, if \( \text{ord}_p(t) \) is even for all \( p = 3 \pmod{4} \), then \((t, t)_p = 1 \) for all odd \( p \) and also \((t, t)_p = 1 \) for all \( p = 3 \pmod{4} \). Now the product formula (Theorem 3 in chapter III of [7]) gives us
\[
(t, t)_p \prod_{p \text{ prime}} (t, t)_p = 1
\]
so \( \varepsilon_2(tQ) = (t, t)_2 = 1 = \varepsilon_2(Q) \). Hence all the invariants of \( Q \) and \( tQ \) are equal and so \( Q \) and \( tQ \) are equivalent and (ii) is proved. \( \square \)

We thus define a rational number \( t \) to be admissible if \( Q \) is equivalent to \( tQ \) over \( \mathbb{Q} \). Note that admissibility of \( t \) depends on \( k \) as well as \( t \) and that \( t \) is admissible if and only if its numerator and denominator are. Hence we have proved the following:

**Lemma 3.** Let \( \Lambda \) be a full sublattice of \( \mathbb{Z}^k \) and \( T \) a similarity of \( \mathbb{R}^k \) of scale factor \( \mu \). Then \( \mu^2 \) is an admissible rational number whose denominator divides
\[
g = \gcd(\{x, y \mid x, y \in \Lambda\})
\]
In particular, \( \mu^2 \geq 1/h \), where \( h \) is the largest admissible integer dividing \( g \). \( \square \)

We can now state our main theorem.

**Theorem 4.** Let \( \Lambda \), \( g \) and \( h \) be as in the previous lemma. If \( k \leq 7 \), then there is a
similarity $T$ of $\mathbb{R}^k$ with scale factor $\mu$ such that $TA \subseteq \mathbb{Z}^k$ and $\mu^{-2} = h$. If $k = 8$, then there is such a $T$ with $TA \subseteq \mathbb{Z}^k$ and $\mu^{-2} = h$ or (only if $h$ is even) $\mu^{-2} = h/2$.

4. Proof of the main theorem

We attack the problem by working a prime at a time. Let $q$ either be an admissible prime or the square of a prime and suppose $q | g$. We can embed $\Lambda$ in a lattice $\Omega$ such that $\Lambda \subseteq \Omega \subseteq \mathbb{Z}^k$ and $q | x, y$ for all $x, y \in \Omega$ and $\Omega$ is maximal with respect to this condition. If we can prove Theorem 4 for this $\Omega$, it will follow that there is a similarity $T$ of scale factor $q^{-1/2}$ with $TA \subseteq \mathbb{Z}^k$.

Define a full sublattice $\Lambda$ of $\mathbb{Z}^k$ to be $q$-divisible if $q | x, y$ for all $x, y \in \Lambda$. Also define $\Lambda$ to be maximal $q$-divisible if it is properly contained in no other $q$-divisible sublattice of $\mathbb{Z}^k$. If $\Lambda$ is a full $q$-divisible sublattice of $\mathbb{Z}^k$, then, as the index $|\mathbb{Z}^k : \Lambda|$ is finite, there exists a maximal $q$-divisible lattice $\Omega \subseteq \mathbb{Z}^k$ with $\Lambda \subseteq \Omega$.

**Theorem 5.** Let $q$ be an admissible prime number or the square of a prime number. Suppose $\Omega \subseteq \mathbb{Z}^k$ is a maximal $q$-divisible lattice. Then $|\mathbb{Z}^k : \Omega| = q^{k/2}$.

**Proof.** 1. claim that $\Omega \supseteq q\mathbb{Z}^k$. For $\Omega + q\mathbb{Z}^k$ is a $q$-divisible lattice containing $\Omega$ and so by maximality of $\Omega$, $\Omega = \Omega + q\mathbb{Z}^k \supseteq q\mathbb{Z}^k$. Let $\tilde{\Omega}$ be the image of $\Omega$ in the quotient $\mathbb{Z}^k/q\mathbb{Z}^k$. As $\Omega \supseteq q\mathbb{Z}^k$ it follows that $|\mathbb{Z}^k : \Omega| = |\mathbb{Z}^k/q\mathbb{Z}^k : \tilde{\Omega}|$. Now the inner product on $\mathbb{Z}^k$ induces a nonsingular pairing $\mathbb{Z}^k/q\mathbb{Z}^k \times \mathbb{Z}^k/q\mathbb{Z}^k \rightarrow \mathbb{Z}/q\mathbb{Z}$ which we shall also denote by the dot notation. The $q$-divisibility of $\Omega$ implies that $\tilde{\Omega} \cdot \tilde{\Omega} = 0$. Also if $V$ is a subgroup of $\mathbb{Z}^k/q\mathbb{Z}^k$ which is isotropic in the sense that $V \cdot V = 0$, then $\Lambda = \{x \in \mathbb{Z}^k | \bar{x} \in V\}$ is a $q$-divisible lattice containing $q\mathbb{Z}^k$, where $\bar{x}$ denotes the reduction of $x$ modulo $q$. Hence $\tilde{\Lambda}$ is a maximal isotropic subgroup of $\mathbb{Z}^k/q\mathbb{Z}^k$ and it suffices to show that all such subgroups have index $q^{k/2}$, or equivalently have order $q^{k/2}$.

**Case (i):** $q = 2$. For 2 to be admissible $k$ must be even. Let $V$ be a maximal isotropic subgroup of $U = \mathbb{Z}^n/2\mathbb{Z}^k$, a vector space of dimension $k$ over $\mathbb{F}_2$. If $v \in V$, then $v, v = 0$ and so an even number of the coordinates of $v$ equal 1, and so $V \subseteq U^0 = \{u \in U | \sum u_i = 0\}$. Also by isotropy $V \subseteq V^\perp = \{u \in U | u \cdot V = 0\}$. Let $w \in U^0 \cap V^\perp \supseteq V$. As $w \in U^0$, $w$ has an even number of coordinates equal to 1 and so $w \cdot w = 0$. Also as $w \in V^\perp$, $w \cdot v = 0$ for all $v \in V$. Hence the group $\langle w \rangle + V$ is isotropic and so by maximality $w \in V$. We conclude that $V = U^0 \cap V^\perp$. Now we count dimensions of vector spaces over $\mathbb{F}_2$. Note that every subgroup of $U$ is an $\mathbb{F}_2$-vector space. Let $d$ be the dimension of $V$ over $\mathbb{F}_2$. As the inner product is nonsingular the dimension of $V^\perp$ is $k - d$ and clearly the dimension of $U^0$ is $k - 1$. Hence $k - d \geq \dim_{\mathbb{F}_2}(U^0 \cap V^\perp) \geq k - d - 1$ and as $V = U^0 \cap V^\perp$, $k - d \geq d \geq k - d - 1$ and so $k \geq 2d \geq k - 1$ and as $k$ is even we conclude that $d = k/2$. Hence $|V| = 2^{k/2}$ as required.
Case (ii): \( q \) is an odd prime. We use the theory of quadratic forms over a field of characteristic \( \neq 2 \), in particular that of the Witt ring. (For definitions and notation see [3].) Let \( U = \mathbb{Z}^k/p\mathbb{Z}^k \) and note that \( U \) and all of its subgroups are \( \mathbb{F}_q \)-vector spaces. The space \( U \) has the inner product derived from the quadratic form \( Q(u_1, u_2, \ldots, u_k) = u_1^2 + u_2^2 + \cdots + u_k^2 \). It suffices to show that every maximal isotropic subspace of \( U \) has dimension \( k/2 \). By Theorem 4 in Section 8.3 of [3] this follows if \( U \) is a direct sum of hyperbolic planes. But this is true if and only if \( [U] = 0 \) in the Witt ring \( W(\mathbb{F}_q) \). Now \( [U] = k\langle 1 \rangle \) and by the Corollary to Lemma 5.8 in Chapter 2 of [1], \( |W(\mathbb{F}_q)| = 4 \) and is noncyclic if \( q = 1 \) (mod \( 4 \)). If \( q = 1 \) (mod \( 4 \)), then, as \( q \) is admissible, \( k \) is even and \( k\langle 1 \rangle = 0 \), and if \( q = 3 \) (mod \( 4 \)), then, as \( q \) is admissible, \( k \) is divisible by 4 and \( k\langle 1 \rangle = 0 \) again. This concludes the proof in this case.

Case (iii): \( q = p^2 \) with \( p \) prime. Let \( V \) be a maximal isotropic subgroup of \( U = \mathbb{Z}^k/p^i\mathbb{Z}^k \) and let \( W = V \cap p\mathbb{Z}^i/p^2\mathbb{Z}^k \). Now if we let \( V_1 \) be the image of \( V \) in \( \mathbb{Z}^k/p\mathbb{Z}^k \) and \( V_2 = \{ v \in \mathbb{Z}^k/p\mathbb{Z}^k \mid pv \in W \} \), then \( |V : W| = |V_1| \) and \( |W| = |V_2| \) and so \( |V| = |V_1||V_2| \). Now consider \( V_1 \) and \( V_2 \) as subspaces of the inner product space \( U' = \mathbb{Z}^k/p\mathbb{Z}^k \) over \( \mathbb{F}_p \). If \( x \in V_1 \) and \( y \in V_2 \), then \( x' \) and \( py \) are in \( V \), where \( x' \) is any lift of \( x \) to \( V \) and so \( x'.py = 0 \) in \( \mathbb{Z}/p^2\mathbb{Z} \) and \( x.y = 0 \) in \( \mathbb{F}_p \). Hence \( V_1 \), \( V_2 \) = 0 and so \( V_2 \subseteq V_1 \subseteq \{ u \in U' \mid u.V_1 = 0 \} \). Now I claim that \( V_2 = V_1^\perp \). If \( u \in V_1^\perp \), then consider \( pu \in U \). Trivially \( pu.pu = 0 \) and if \( x \in V \), then \( x.pu = p(x.u) = 0 \) because \( x.u = 0 \) in \( \mathbb{F}_p \) as the image of \( x \) in \( U' \) lies in \( V_1 \) and \( u \in V_1^\perp \). Clearly then \( \langle py \rangle + V \) is an isotropic subgroup of \( U \) containing \( V \) and so by maximality \( pu \in U \) and so \( u \in V_2 \) as required. Now as the inner product on \( U' \) is nonsingular, \( |V| = |V_1||V_2| = |V_1^\perp| = |U'| = p^k = q^{k/2} \) and the theorem is thus proved.

We recall that a rank \( k \) lattice \( \Lambda \) in \( \mathbb{R}^k \) is unimodular if it is integral, that is, \( x.y \in \mathbb{Z} \) for all \( x, y \in \Lambda \) and its fundamental region has volume 1. The integer lattice \( \mathbb{Z}^k \) is clearly a unimodular lattice which is odd, that is, it contains \( x \) with \( x.x \) an odd integer. Another important example is the \( E_8 \) root lattice

\[
E_8 = \left\{ (x_1, x_2, \ldots, x_8) \in \mathbb{Z}^8 \cup (\mathbb{Z} + 1/2)^8 \mid \sum_{i=1}^{8} x_i \in 2\mathbb{Z} \right\},
\]

which is an even unimodular lattice, that is, \( x.x \) is even for all \( x \in E_8 \). We have the classification theorem in dimensions \( k \leq 8 \):

**Theorem 6.** If \( \Lambda \) is a unimodular lattice in \( \mathbb{R}^k \) for \( k \leq 8 \), then there is an isometry \( T \) of \( \mathbb{R}^k \) such that \( TA = \mathbb{Z}^k \) if \( \Lambda \) is odd or \( TA = E_8 \) if \( \Lambda \) is even (and so \( k = 8 \)).

**Proof.** This is part of Theorem 106:13 in [6].

Theorem 5 has the following corollary:

**Lemma 7.** Let \( q \) be an admissible prime or the square of a prime. If \( \Omega \) is a
maximal $q$-divisible lattice, then the lattice $q^{-1/2} \Omega$ is unimodular. Also if $q$ is odd then $q^{-1/2} \Omega$ is an odd unimodular lattice.

**Proof.** By Theorem 5, $|Z^k : A| = q^{k/2}$ and so the fundamental region of $\Omega$ has volume $q^{k/2}$. Hence the fundamental region of $q^{-1/2} \Omega$ has volume 1. As $\Omega$ is $q$-divisible, $x, y \in qZ$ for all $x, y \in \Omega$ and so $q^{-1/2} x, q^{-1/2} y \in \mathbb{Z}$ and $q^{-1/2} \Omega$ is integral. Hence the lattice $q^{-1/2} \Omega$ is unimodular.

If $q$ is odd, then $x = (q, 0, 0, \ldots, 0) \in \Omega$ as $qZ^k \subseteq \Omega$. Now $y = q^{-1/2} x \in q^{-1/2} \Omega$ has $y \cdot y = q$ odd. Hence $q^{-1/2} \Omega$ is an odd unimodular lattice as claimed.

We now proceed to the proof of the main theorem. Let $A \subseteq \mathbb{Z}^k$ be a full sublattice, $g = \gcd \{ x, y \mid x, y \in A \}$ and $h$ be the largest admissible integer factor of $g$. If $h = 1$, then there is nothing to prove. If $h > 1$, then there is a $q|h$ which is either an admissible prime or the square of a prime. As $A$ is $q$-divisible we can embed $A \subseteq \Omega$ which is maximal $q$-divisible. By Lemma 3 the lattice $q^{-1/2} \Omega$ is unimodular and also odd if $q$ is odd. So unless $k = 8$ and $q$ is even then by Theorem 3 there is an isometry $T$ with $T(q^{-1/2} \Omega) = \mathbb{Z}^k$. Now the map $S : x \mapsto q^{-1/2} T x$ is a similarity of scale factor $q^{-1/2}$ with $A' = SA \subseteq \mathbb{Z}^k$. Also $g' = \gcd \{ x', y' \mid x', y' \in A' \} = g/q$ and $h' = h/q$ is the largest admissible integer factor of $g'$. Repeating this process yields a similarity $R$ of scale factor $\mu$ with $RA \subseteq \mathbb{Z}^k$ and $\mu^{-2} = h$ for $k \leq 7$ and $\mu^{-2} = l$ for $k = 8$, where $l$ is the largest odd factor of $g = h$. Hence the theorem is proved for $k \leq 7$.

Now let $k = 8$. We may assume that $g = h$ is even and by the above we may reduce to the case where $g = h$ is a power of 2. If $g \leq 2$, we are done, so suppose that 4 divides $g$. As $A$ is 4-divisible, we can embed $A \subseteq \Omega$ with $\Omega$ maximal 4-divisible. By Lemma 3 the lattice $2^{-1} \Omega$ is unimodular and so isometric to either $\mathbb{Z}^8$ or $\mathbb{E}_8$. In the former case we argue as above and reduce $h$ by a factor of 4. Now I claim that there is a sublattice $L$ of $\mathbb{Z}^8$ isometric to $\sqrt{2} \mathbb{E}_8$. Given this claim choose an isometry $T$ with $T(2^{-1/2} \Omega) = L$. The map $S : x \mapsto 2^{-1/2} T x$ is a similarity of scale factor $2^{-1/2}$ with $SA \subseteq \mathbb{Z}^k$. Hence we can reduce $g$ by a factor of 2. Repeating we can reduce $g$ to 1 or 2 and the theorem is proved.

Finally the lattice $L$ generated by the rows of the matrix

$$
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2
\end{pmatrix}
$$

is isometric to $\sqrt{2} \mathbb{E}_8$ as claimed (see p. 233 of [4]).

\[\Box\]
Acknowledgment

I would like to thank Dr. John Cremona for bringing this problem to my attention.

References