On the number of lattice points in a small sphere

Annika Meyer

On the number of lattice points in a small sphere

Annika Meyer

Chaire de Structures Algébriques et Géométriques
École Polytechnique Fédérale de Lausanne

Abstract. Let L be a lattice in $\mathbb{R}^n$. We upper bound the number of points of L contained in a small sphere, centered anywhere in $\mathbb{R}^n$. One way to do this is based on the observation that if the radius of the sphere is sufficiently small then the lattice points contained in that sphere give rise to a spherical code with a certain minimum angle. Another method involves Gaussian measures on L in the sense of [2]. Examples where the obtained bounds are optimal include some root lattices in small dimensions and the Leech lattice. We also present a natural decoding algorithm for lattices constructed from lattices of smaller dimension, and apply our results on the number of lattice points in a small sphere to conclude on the performance of this algorithm.

1 Introduction

A *lattice* L in $\mathbb{R}^n$ is the set of all integral linear combinations of a basis $(b_1, \ldots, b_n)$ of $\mathbb{R}^n$, i.e.

$$L = \{z_1 b_1 + \cdots + z_n b_n \mid z_1, \ldots, z_n \in \mathbb{Z}\}.$$

In this paper we give upper bounds on the number of lattice points contained in a closed ball

$$B_r(z) := \{v \in \mathbb{R}^n \mid |v - z| \leq r\}$$

where z is any vector in $\mathbb{R}^n$ and $|\ .\ |$ is the usual Euclidian length. In the special case where $L = \mathbb{Z}^2$ is the standard lattice in $\mathbb{R}^2$ and z is a lattice point, the cardinality of $B_r(z) \cap L$ is the subject of *Gauss's circle problem*, whose solution is well known (see [7], for instance). Moreover, there exist good asymptotic estimates for $|B_r(z) \cap L|$, i.e. as r goes to infinity (cf. [6, 16, 19]).

However, very little seems to be known for small values of r. To the author's knowledge, the only work that has been done so far is by Conway and Sloane, who in [10] give a *lower* bound on $|B_{\sqrt{\mu(L)}}(z) \cap L|$, provided that z is not exactly at distance $\mu(L)$ from any lattice point. Here

$$\mu(L) := \max_{v \in \mathbb{R}^n} \min_{l \in L} |v - l|^2$$

is the (squared) covering radius of L.

The first method we use to upper bound $|B_r(z) \cap L|$ resembles the one used by Conway and Sloane in [9, Ch.13] to upper bound the *kissing number* of a lattice (i.e. the number of its shortest nonzero vectors). Let

$$\min(L) := \min_{0 \neq l \in L} |l|^2$$

be the minimum of L. If $\frac{\min(L)}{4} \leq r^2 \leq \min(L)$ then Theorem 1 shows that the lattice points in $B_r(z)$ can be rearranged inside $B_r(z)$ as a *spherical code* with a certain minimum angle. Recall that a spherical code $\mathcal{C}$ with minimum angle θ is just a set of points lying on the boundary of a sphere centered anywhere, at v, say, such that the angle between $v-c$ and $v-c'$ is at least θ, for any two distinct points $c, c' \in \mathcal{C}$. This gives rise to upper bounds on $|B_r(z) \cap L|$, since there exist various methods to upper bound the cardinality of a spherical code with a given minimum angle. The most general approach uses linear programming. The key idea for the linear programming method is given in Lemma 1, but for a more detailed treatment, we refer the reader to [9, Ch.13]). Calculations using this linear programming method are summarized in Table 4 for some important lattices, such as root lattices in dimension up to 10 and the Leech lattice, for $r = \sqrt{\mu(L)}$. This choice of r is motivated by the coding theoretic application in Section 5. In some cases the upper bound on $|B_{\sqrt{\mu(L)}}(z) \cap L|$ is attained when z is a *deep hole* of L, that is, $\min_{l \in L} |z-l|^2 = \mu(L)$. This shows that in the respective cases, these bounds are optimal, and moreover, the lattice points at distance $\sqrt{\mu(L)}$ from a deep hole of L form an optimal spherical code with the respective minimum angle.

To also obtain upper bounds on $|B_r(z) \cap L|$ when $r^2 > \min(L)$, we present a different approach in Section 3, based on Gaussian-like measures on L. For each $z \in \mathbb{R}^n$ Theorem 2 gives a positive real number $\gamma_{r,L,z}$ such that $|B_r(z) \cap L| \leq \gamma_{r,L,z}$. Based on worst-case assumptions on z, we also obtain a universal upper bound, i.e. a positive real $\gamma_{r,L}$ such that

$$\sup_{z \in \mathbb{R}^n} |B_r(z) \cap L| \leq \gamma_{r,L}. \tag{1}$$

The bounds obtained for $r = \sqrt{\mu(L)}$ are also in Table 4.

The results show that in general neither of the two methods to upper bound $|B_r(L) \cap L|$ is superior to the other. Moreover, our observations let us conjecture the following.

Conjecture 1. If $\mu(L) \leq \min(L)$ then the function $\mathbb{R}^n \to \mathbb{N}, \;\; z \mapsto |B_{\sqrt{\mu(L)}}(z) \cap L|$ takes its maximum in a deep hole of L.

From our calculations, summarized in Table 4, we can verify this conjecture in some cases, as follows.

Remark 1. The lattices A_n $(n \in \{2,3,4\})$, D_n $(n \in \{3,4,5\})$, E_n $(n \in \{6,7,8\})$ and the Leech lattice Λ_{24} satisfy Conjecture 1.

In Section 5 we give a coding theoretic application of our results. Lattices are used as codebooks in important modern communication systems, like MIMO fading channels (cf. [5, 4]). In this context decoding a received signal $z \in \mathbb{R}^n$ means finding the lattice point closest to z, i.e. finding $l \in L$ such that $|z-l| \leq |z-\tilde{l}|$ for all $\tilde{l} \in L$. This problem is commonly called the *Closest Vector Problem* and is hard to solve in general (see [15] for a study of the complexity of this problem).

In this paper we give an algorithm that solves the closest vector problem *approximately* in lattices with a certain structure. Here approximately means that, given $z \in \mathbb{R}^n$, our algorithm finds a lattice point $l \in L$ such that

$$|z - l| \leq \gamma \cdot |z - \tilde{l}|$$

for all $\tilde{l} \in L$, where $\gamma > 1$ is a real number which does not depend on z.

The lattices considered in this paper are given in the following form. Given positive integers n_i for $i \in \{0, \ldots, t\}$, and lattices W_i in $\mathbb{R}^{n_i}$ as well as linear maps $f_i : \mathbb{R}^{n_0+\cdots+n_{i-1}} \to \mathbb{R}^{n_i}$, $i \in \{1, \ldots, t\}$, with $f_1 = 0$, consider the lattice L given by

$$\{(u_1, \ldots, u_t) \in \mathbb{R}^{n_1+\cdots+n_t} \mid u_i - f_i(u_0, \ldots, u_{i-1}) \in W_i,\ i \in \{1, \ldots, t\}\}.$$

For example, lattices obtained from Turyn's construction (cf. Chapter 8 of [9]) are obtained in this way (see Lemma 4). These include very well known lattices such as the Leech lattice and the recently found extremal unimodular even lattice in dimension 72 (cf. [17]).

The recursive definition of the points in L allows to approximate a vector $(z_1, \ldots, z_t) \in \mathbb{R}^{n_1+\cdots+n_t}$ by successive approximations in W_i. An algorithm to do this is given in Section 5. It is a generalisation of Babai's Nearest Plane Method (cf. [1]), using the Fincke-Pohst method (also called *sphere decoding*, cf. [12]) as a subroutine to obtain all points of W_1 in a certain small sphere B around z_1 first. The approximation factor is given in Remark 2. The additional effort to our algorithm stemming from dealing with all the points of W_1 contained in B depends of course on $|B \cap W_1|$ and can be estimated using the results in the previous sections. We then apply the algorithm to lattices obtained from Turyn's construction. In particular, we conclude on the performance of the algorithm in the case of the newly found extremal even unimodular lattice in dimension 72 (see [17]).

2 Bounds on $|B_r(z) \cap L|$ via spherical codes

Let L be a lattice in $\mathbb{R}^n$, and assume (possibly after rescaling) that L has covering radius 1. Let z be a deep hole of L. Then the lattice points in $B := B_1(z)$ all lie on the border of the unit ball B; in other words, they form a *spherical code* $\mathcal{C}$. Since any two different elements of $\mathcal{C}$ are at least $\min(L)^{\frac{1}{2}}$ apart, the angle θ between them satisfies

$$\theta \geq 2 \sin^{-1}\left(\frac{\sqrt{\min(L)}}{2}\right).$$

This observation is generalized in Theorem 1, which states that for every ball $B_r(z)$ with $r^2 \in [\frac{\min(L)}{4}, \min(L)]$ centered at *any* point $z \in \mathbb{R}^n$, the lattice points contained in that ball give rise to a spherical code with a certain minimum angle.

In what follows let $A(n, \theta)$ be the maximal cardinality of a spherical code in dimension n and with minimum angle at least θ.

Theorem 1. *Let L be a lattice in $\mathbb{R}^n$ and let r be a positive real such that $\frac{\min(L)}{4} \leq r^2 \leq \min(L)$. Then for any $z \in \mathbb{R}^n - L$, the set*

$$\{|x-z|^{-1}\,(x-z) \mid x \in B_r(z) \cap L\}$$

is a spherical code with minimum angle $\cos^{-1}(1-\frac{\min(L)}{2r})$. In particular $|B_r(z) \cap L| \leq A(n, \cos^{-1}(1-\frac{\min(L)}{2r}))$.

Proof. After rescaling L with r^{-1}, assume that $r = 1$, and hence $\min(L) \geq 1$. For any $x, y \in B_1(z) \cap L$, we aim to lower bound the angle θ between $x-z$ and $y-z$. Observe that

$$|x-z|^2 + |y-z|^2 - 2\cos(\theta)|x-z|\,|y-z| = |x-y|^2.$$

Since $|x-y|^2 \geq \min(L)$, this yields

$$\cos(\theta) \leq \frac{|x-z|^2 + |y-z|^2 - \min(L)}{2|x-z|\,|y-z|}. \tag{2}$$

Now for $a \in (0,1]$ consider the real function $f_a : t \mapsto \frac{a^2+t^2-\min(L)}{2at}$. This function is decreasing since for any real t,

$$\frac{\delta f}{\delta t}(t) = \frac{t^2 - a^2 + \min(L)}{2at^2} \geq 0.$$

For symmetry reasons, it follows that the right hand side of (2) is maximised if $|x-z| = |y-z| = 1$. In this case, equation (2) yields $\cos(\theta) \leq 1 - \frac{\min(L)}{2}$, which shows the assertion.

The lemma below follows from Theorem 1 together with [9, Ch.13]. Since the proof is analogous to the one provided in [9], we shall omit it here.

Lemma 1. *Let L be a lattice in $\mathbb{R}^n$ with $\mu(L) \leq \min(L)$ and let f be a real polynomial of degree d satisfying the following conditions:*

(i) $f(t) \leq 0$ *for* $-1 \leq t \leq 1 - 2\frac{\min(L)}{\mu(L)}$,

(ii) if $f(t) = \sum_{i=0}^{d} f_i P_i^{\alpha,\alpha}$ *is the expansion of f in terms of Jacobi polynomials, with* $\alpha = \frac{n-3}{2}$, *then* $f_0 > 0$ *and* $f_i \geq 0$ *for* $i \in \{1, \ldots, d\}$.

Then $|B_{\mu(L)}(z) \cap L| \leq \frac{f(1)}{f_0}$ *for every* $z \in \mathbb{R}^n$.

Note that a polynomial f as in Lemma 1 can be found by linear programming - again, see [9, Ch.13] for an explanation.

3 Bounds on $|B_r(z) \cap L|$ via Gaussian measures on L

Let L be a lattice in $\mathbb{R}^n$ and let

$$L^\sharp := \{v \in \mathbb{R}^n \mid (v,l) \in \mathbb{Z} \text{ for all } l \in L\}$$

be its *dual lattice*, where $(\cdot,\cdot) : \mathbb{R}^n \times \mathbb{R}^n,\ (v,w) \mapsto v_1w_1 + \cdots + v_nw_n$ is the standard scalar product on $\mathbb{R}^n$.

The main idea in this section is to use the Schwartz function $f : \mathbb{R}^n \to \mathbb{R},\ x \mapsto e^{-\pi(x,x)}$ as a kind of measure on L as well as on its translate $L - u := \{l - u \mid l \in L\}$ to upper bound $|B_r(u) \cap L|$ (see also [2]).

Theorem 2. *Let L be a lattice in $\mathbb{R}^n$ and let $z \in \mathbb{R}^n$. For every positive real r and every $\delta > (\frac{n}{2\pi})^{\frac{1}{2}}$ we have $|L \cap B_r(z)| \le \gamma_{r,L,z}$, where*

$$\gamma_{r,L,z} = e^{\pi r^2}\ \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp \cap B_\delta(0)} \cos(2\pi(z,y)) f(y)\ R_\delta.$$

Moreover, for any $z \in \mathbb{R}^n$ we have $\gamma_{r,L,z} \le \gamma_{r,L}$, where

$$\gamma_{r,L} = e^{\pi r^2} \sum_{x \in L \cap B_\delta(0)} f(x)\ R_\delta.$$

The error term is $R_\delta = (1 - (\delta(\frac{2\pi}{n})^{\frac{1}{2}})^n e^{\frac{n}{2} - \pi\delta^2})^{-1}$ and tends to 1 as δ goes to infinity.

For the proof of Theorem 2 we need the two lemmata below. The following improves [2, Lemma 1.4(ii)].

Lemma 2. *With f as above, we have*

$$\sum_{x \in L - z} f(x) = \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp} \cos(2\pi(z,y)) f(y) \le \sum_{x \in L} f(x).$$

Proof. Our proof uses the Poisson summation formula for lattices, which states for any lattice L in $\mathbb{R}^n$ and a sufficiently well-behaved function $g : \mathbb{R}^n \to \mathbb{C}$,

$$\sum_{x \in L} g(x) = \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp} \hat{g}(y),$$

where $\hat{g} : \mathbb{R}^n \to \mathbb{C},\ y \mapsto \int_{\mathbb{R}^n} e^{2\pi i(x,y)} g(x)dx$ is the Fourier transform of g.

Now the functions f and its translate $x \mapsto f(x - z)$ are sufficiently well-behaved, and f is its own Fourier transform, wheras the Fourier transform of the translate is $y \mapsto e^{2\pi i(z,y)} f(y)$. Hence Poisson summation yields

$$\begin{aligned}
\sum_{x \in L - z} f(x) = \sum_{x \in L} f(x - z) &= \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp} \exp(-2\pi i(z,y)) f(y) \\
&= \det(L)^{-\frac{1}{2}} (1 + \sum_{\substack{\{y,-y\} \subseteq L, \\ y \neq 0}} 2\cos(2\pi(z,y)) f(y) \\
&= \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp} \cos(2\pi(z,y)) f(y) \le \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp} f(y) = \sum_{x \in L} f(x).
\end{aligned}$$

Lemma 3. *[(cf. [2, Lemma 1.5(ii)])] For any lattice L in $\mathbb{R}^n$ and for each $\delta > \left(\frac{n}{2\pi}\right)^{\frac{1}{2}}$ we have*

$$\sum_{x \in L - B_\delta(0)} f(x) < (\delta(\frac{2\pi}{n})^{\frac{1}{2}})^n e^{\frac{n}{2} - \pi\delta^2} \sum_{x \in L} f(x).$$

Proof of Theorem 2. Consider the inequality chain

$$|L \cap B_r(z)|\, e^{-\pi r^2} \leq \sum_{x \in L - z} f(x) = \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp} \cos(2\pi(y,z)) f(y).$$

The first inequality simply stems from the fact that $|L \cap B_r(z)| = |L - z \cap B_r(0)|$. The second inequality follows from Lemma 2. Now take any $\delta > \left(\frac{n}{2\pi}\right)^{\frac{1}{2}}$, then the right hand side of the above is at most

$$\begin{aligned} \det(L)^{-\frac{1}{2}} \quad & \Big(\sum_{y \in L^\sharp \cap B_\delta(0)} \cos(2\pi(y,z)) f(y) \quad + \sum_{y \in L^\sharp - B_\delta(0)} f(y) \Big) \\ & \leq \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp \cap B_\delta(0)} \cos(2\pi(y,z)) f(y) R_\delta \leq \sum_{x \in L \cap B_\delta(0)} f(x) R_\delta, \end{aligned}$$

where the last two inequalities are due to Lemma 3. This proves the theorem. □

4 Results for some important lattices

The following table lists some important lattices L (see [9] for a definition of these lattices). If Theorem 1 applies with $r = \sqrt{\mu(L)}$ then the minimal angle of the obtained spherical code is denoted θ; an upper bound on $\sup_{z \in \mathbb{R}^n} |B_{\sqrt{\mu(L)}}(z) \cap L|$ is hence given by $A(n, \theta)$. To upper bound $A(n, \theta)$, the author implemented the linear programming method described in [9, Ch.13] in MAGMA ([3]), obtaining a polynomial f as in Lemma 1. The coefficients of f in the expansion in terms of Jacobi polynomials are given in the fourth column, rounded to three decimal places, as a sequence $[f_0, \ldots, f_d]$, meaning that $f(t) = f_0 P_0^{\alpha,\alpha}(t) + \cdots + f_d P_d^{\alpha,\alpha}(t)$, where α and d are as in Lemma 1.

The penultimate column gives the bound obtained by the method described in Section 3. Note that it may be convenient to rescale the lattices to obtain better results. The author observed that in many cases the best results are obtained when the lattice is rescaled as to be of minimum 1. The last column of the table gives the the maximal number $|B_{\sqrt{\mu(L)}}(u) \cap L|$ attained at a deep hole u of L.

Type	n	θ	$[f_0, \ldots, f_d]$	$A(n,\theta)$	Gaussian bound	for deep holes
A	2	$\frac{2}{3}\pi$		3	3	3
	3	$\frac{\pi}{2}$	$[1, 2.4, 2.002, 0.601]$	6	7	6
	4	$\cos^{-1}(\frac{1}{6})$	$[1, 2.226, 2.178, 1.010]$	10	12	10
	5	$\cos^{-1}(\frac{1}{3})$	$[1, 2.187, 2.659, 1.941, 0.695, 0, 0, 0.413]$	≤ 24	26	20
	6	$\cos^{-1}(\frac{5}{12})$	$[1, 1.957, 2.512, 2.376, 1.455, 0.587, 0, 0, 0, 0.685]$	≤ 54	47	35
	7	$\frac{\pi}{3}$	$[1, 2.503, 2.935, 3.185, 2.466, 1.365, 0.382, 0, 0, 0.062, 0.057]$	≤ 140	99	70
	8	-	-	-	188	126
	9	-	-	-	391	252
	10	-	-	-	758	462
D	3	$\frac{\pi}{2}$	$[1, 2.4, 2.002, 0.601]$	6	8	6
	4	$\frac{\pi}{2}$	$[1, 2.001, 1.602, 0.458]$	8	10	8
	5	$\cos^{-1}(\frac{1}{5})$	$[1, 2.143, 2.084, 1.116]$	16	20	16
	6	$\cos^{-1}(\frac{1}{3})$	$[1, 2.166, 2.589, 1.946, 0.722, 0, 0, 0.037]$	≤ 37	42	32
	7	$\cos^{-1}(\frac{3}{7})$	$[1, 1.933, 2.515, 2.457, 1.543, 0.667, 0, 0, 0, 0.082]$	≤ 88	88	64
	8	$\frac{\pi}{3}$	$2.286, 3.175, 3.602, 2.835, 1.705, 0.552$	240	183	128
	9	-	-	-	595	256
	10	-	-	-	1211	512
E	6	$\cos^{-1}(\frac{1}{4})$	$[1, 1.852, 2.029, 1.311]$	27	37	27
	7	$\cos^{-1}(\frac{1}{3})$	$[1, 1.909, 2.274, 1.832, 0.892, 0.189]$	56	84	56
	8	$\frac{\pi}{2}$	$[1, 1.485, 0.891, 0.195]$	16	77	16
Leech	24	$\frac{\pi}{2}$	$[1, 1.158, 0.322, 0.033]$	48	974	48

5 A recursive decoding algorithm for certain lattices

In this section we describe a recursive decoding algorithm for lattices obtained from lattices of smaller dimension by a procedure resembling the *gluing method* (see [9, Ch.4]). We show that among these lattices, there are those obtained from Turyn's construction. Hence in particular our algorithm applies to the Leech lattice and to the recently found extremal even unimodular lattice in dimension 72 ([17]).

The lattices considered here are of the following form: Let $n_0, \ldots, n_t$ be positive integers and let $W_1, \ldots, W_t$ be lattices in $\mathbb{R}^{n_i}$. Moreover, let

$$f_i : \mathbb{R}^{n_0+\cdots+n_{i-1}} \to \mathbb{R}^{n_i}$$

be linear maps, for $i \in \{1, \ldots, t\}$, where $f_1 = 0$. Let $n := n_1 + \cdots + n_t$. Then we define $\mathcal{L} = \mathcal{L}(W_1, \ldots, W_t, f_2, \ldots, f_t)$ as

$$\mathcal{L} := \{(u_1, \ldots, u_t) \in \mathbb{R}^n \mid u_i - f_i(u_0, \ldots, u_{i-1}) \in W_i \ (i = 1, \ldots, t)\}.$$

Clearly $\mathcal{L}$ is a lattice in $\mathbb{R}^n$. We propose the following algorithm to find a point nearby a given vector in $\mathbb{R}^n$ in a lattice $\mathcal{L}$ as above.

Algorithm $\mathcal{A}$: Input: A vector $z := (z_1, \ldots, z_t) \in \mathbb{R}^n$ (where $z_i \in \mathbb{R}^{n_i}$ for $i \in \{1, \ldots, t\}$) and a lattice $\mathcal{L}$ as above.

(1) Use sphere decoding to find all points in $W_1 \cap B_{\sqrt{\mu(W_1)}}(z_1)$.
(2) For every point w_1 found in step (1) do the following. Put $x_0 := 0$ and $x_1 := w_1$. Successively, approximate $z_i - f_i(x_0, \ldots, x_{i-1})$ by a point $w_i \in W_i$ and put $x_i := w_i + f_i(x_0, \ldots, x_{i-1})$. Then $x := (x_1, \ldots, x_t) \in \mathcal{L}$.
(3) Among all approximations found in step (2), choose the best one.

Remark 2. Let $\hat{x}$ be the approximation of z found by the above algorithm. Then

$$|\hat{x} - z|^2 < \mu(W_1)^{-1} \sum_{i=1}^{t} \mu(W_i) \, |l - z|^2$$

for all $l \in \mathcal{L}$.

Proof. If $\hat{x}$ is the closest lattice point in $\mathcal{L}$ to z then the claim follows, since the approximation factor given above is always greater than 1. So suppose that a lattice point $l \in \mathcal{L}$ nearest to z satisfies $|l - z| < |\hat{x} - z|$. On the one hand, one clearly has $|\hat{x} - z|^2 \leq \sum_{i=1}^{t} \mu(W_i)$. On the other hand, observe that every approximation $x = (x_1, \ldots, x_t)$ found in step (2) satisfies

$$|x - z| = \min\{|y - z| \mid y \in \mathcal{L} \text{ and } y_1 = x_1\},$$

which implies $|\hat{x} - z| = \min\{|y - z| \mid y \in \mathcal{L} \text{ and } |y_1 - z_1|^2 \leq \mu(W_1)\}$. Hence we must have $|l - z|^2 \geq |l_1 - z_1|^2 > \mu(W_1)$. This yields the assertion.

In [20], Turyn gave a way of constructing a lattice in dimension nk based upon a polarisation of a lattice in dimension n (where n and k are integers, with $k \geq 2$), as follows. The Leech lattice, for instance, can be constructed in this way from a polarisation of E_8 (cf. [14, Cor. 2.11]), and the extremal even unimodular lattice in dimension 72 found by Nebe (cf. [17]) is obtained by a polarisation of the Leech lattice.

Definition 1. *(cf. [18]) Let L be a lattice in $\mathbb{R}^n$ such that $\sqrt{2}L$ is even and unimodular. A* polarisation *of L is a pair of integral sublattices M, N of L such that $M + N = L$ and $M \cap N = 2L$. Given such a polarisation and an integer $k \geq 2$, one defines $\mathcal{M} = \mathcal{M}(L, M, N, k)$ by*

$$\mathcal{M} := \{(u_1, \ldots, u_k) \in \perp_{i=1}^{k} L \mid u_1 - u_i \in N \ (i = 2, \ldots, k),\ u_1 + \cdots + u_k \in M\}.$$

Then $\mathcal{M}$ is an integral unimodular lattice, which is even if and only if N is even or k is even.

Lemma 4. *With L, M, N, n and k as above, we have*

$$\mathcal{M}(L, M, N, k) = \mathcal{L}(L, N, \ldots, N, M \cap N, \iota_1, \ldots, \iota_{k-2}, f),$$

where there are $k-2$ copies of N, $\iota_i : \mathbb{R}^{n_0+n(i+1)} \to \mathbb{R}^n,\ (u_0, \ldots, u_{i+1}) \mapsto u_1$ for $u_j \in \mathbb{R}^n$ $(j \in \{1, \ldots, i+1\})$ and $i \in \{1, \ldots, k-2\}$. The map f is defined as follows: Choose a basis $(a_1 + b_1, \ldots, a_n + b_n)$ of $L = M + N$, where $a_i \in N$ and $b_i \in M$ for $i \in \{1, \ldots, n\}$. Then let the linear map $\pi_N : \mathbb{R}^n \to \mathbb{R}^n,\ a_i + b_i \mapsto b_i$, so in particular $\pi_N(l) \in N$ and $l - \pi_N(l) \in M$ for every $l \in L$. Now let

$$f : \ \mathbb{R}^{n_0} \perp \perp_{i=1}^{k-1} \mathbb{R}^n \to \mathbb{R}^n,\ \ (u_0, \ldots, u_{k-1}) \mapsto u_1 - \pi_N(2u_1 + u_2 + \cdots + u_{k-1}).$$

Since the proof of this lemma is straightforward verification, we shall omit it here. We now investigate the approximation factor obtained when decoding $\mathcal{M}$ with Algorithm $\mathcal{A}$.

Proposition 1. *Let $\hat{x}$ be the approximation of z found by Algorithm $\mathcal{A}$. Then for all $l \in L$,*

$$|z - \hat{x}| \leq (4k - 3) \cdot |z - l|.$$

Proof. According to Remark 2 and Lemma 4, the approximation factor is at most $\mu(L)^{-1}(\mu(L) + (k-2)\mu(N) + \mu(M \cap N))$. The assertion now follows from

$$\mu(N) \leq \mu(M \cap N) = \mu(2L) = 4\mu(L).$$

Example 1 (Algorithm $\mathcal{A}$ for the extremal even unimodular lattice Λ_{72} in dimension 72 ([17])). This lattice of minimum 8 is obtained from a polarisation of the Leech lattice Λ_{24} with $k = 3$.

Here Algorithm $\mathcal{A}$ yields an approximation factor of 9. The two sublattices of Λ_{24} yielding Λ_{72} are isomorphic to multiples of Λ_{24}. Hence according to Remark 1 the maximum number of times that steps (2) and (3) of Algorithm $\mathcal{A}$ must be performed to decode a point in $\mathbb{R}^{72}$ equals

$$\sup_{z \in \mathbb{R}^{24}} |B_{\sqrt{\mu(\Lambda_{24})}}(x) \cap \Lambda_{24}| = 48.$$

References

1. Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica 6, 1–13 (1986)
2. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Math. Ann. 296, 625–635 (1993)
3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24, 235–265 (1997)
4. Caire, G., Damen, M.O., El Gamal, H.: On maximum-likelihood detection and the search for the closest lattice point (English summary). IEEE Trans. Inform. Theory 49, 2389–2402 (2003)
5. Caire, G., Damen, M.O., El Gamal, H.: Lattice coding and decoding achieve the optimal diversity-multiplexing tradeoff of MIMO channels (English summary). IEEE Trans. Inform. Theory 50, 968–985 (2004)
6. Chamizo, F., Iwaniec, H.: On the sphere problem. Rev. Mat. Iberoamericana 11, 417–429 (1995)
7. Cohn-Vossen, S., Hilbert, D.: Geometry and the imagination. Chelsea Publishing Company (1999)
8. Conway, J.H., Sloane, N.J.A.: Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice. IEEE Trans. Inform. Theory 32, 41–50 (1986)
9. Conway, J.H., Sloane, N.J.A.: Sphere packings, lattices and groups. Grundlehren der mathematischen Wissenschaften 290, Springer (1988)
10. Conway, J.H., Sloane, N.J.A.: On the covering multiplicity of lattices. Discrete Comput. Geom. 8, 109–130 (1992)
11. Delsarte, P., Goethals, J.M., Seidel, J.J.: Spherical codes and designs. Geometricae Dedicata 6, 363–388 (1977)
12. Fincke, U., Pohst, M.: Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. Math. Comp. 44, 463–471 (1985)
13. Forney, G.D.: Coset Codes - Part II: Binary lattices and related codes. Coding techniques and coding theory. IEEE Trans. Inform. Theory 5, 1152–1187 (1988)
14. Griess Jr., R.L.: Rank 72 high minimum norm lattices. J. Number Theory 130, 1512–1519 (2010)
15. Guruswami, V., Micciancio, D., Regev, O.: The complexity of the covering radius problem. Comput. Complexity 14, 90–121 (2005)
16. Heath-Brown, D.R.: Lattice points in the sphere. Number theory in progress 2, 883–892 (1999)
17. Nebe, G.: An even unimodular 72-lattice with minimum 8. J. Reine und Angew. Math. (to appear)
18. Quebbemann, H.-G.: A construction of integral lattices. Mathematika 31, 137–140 (1984)
19. Tsang, K.-M.: Counting lattice points in the sphere. Bull. London Math. Soc. 32, 679–688 (2000)
20. Turyn, R.J.: Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. J. Combinatorial Theory 16, 313–333 (1974)