Des. Codes Cryptogr. (2013) 66:375–390
DOI 10.1007/s10623-012-9724-0

On the number of lattice points in a small sphere and a recursive lattice decoding algorithm

Annika Meyer

Received: 4 September 2011 / Revised: 21 February 2012 / Accepted: 23 June 2012 /
Published online: 19 July 2012

Abstract Let L be a lattice in $\mathbb{R}^n$. This paper provides two methods to obtain upper bounds on the number of points of L contained in a small sphere centered anywhere in $\mathbb{R}^n$. The first method is based on the observation that if the sphere is sufficiently small then the lattice points contained in the sphere give rise to a spherical code with a certain minimum angle. The second method involves Gaussian measures on L in the sense of Banaszczyk (Math Ann 296:625–635, 1993). 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.

Keywords Lattice · Sphere decoding · Spherical code · Kissing number · Gaussian measure · Lattice decoding

Mathematics Subject Classification (2010) 06B99 · 90C05 · 11T71

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.

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

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography".

A. Meyer (✉)
Chaire de Structures Algébriques et Géométriques École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland
e-mail: annika.meyer@rwth-aachen.de

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 $|\ .\ |$ denotes 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, the asymptotic behaviour of $|B_r(z) \cap L|$, i.e. as r goes to infinity, has been extensively studied (see [6,17,24], for example).

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 Mazo and Odlyzko for the standard lattice and arbitrary z (cf. Lemma 1 of [19]), and 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 $\sqrt{\mu(L)}$ 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.

An obvious method to obtain an upper bound on $|B_r(z) \cap L|$ is to enumerate all points in $B_r(z) \cap L$ and then count them. To enumerate the lattice points, one can use the Fincke–Pohst method (also called *sphere decoding*, cf. [12]). However, the results obtained this way will be specific for the lattice and the chosen center of the sphere. This paper gives upper bounds on $|B_r(z) \cap L|$ which are independent from the center of the sphere and only depend on certain lattice parameters.

The first method we use to bound $|B_r(z) \cap L|$ from above resembles the one used by Kabatiansky, Levenshtein et al. to derive an upper bound on the *kissing number* of a lattice, i.e. the number of its shortest nonzero vectors (see [9, Chap. 9] for a survey). The bounds on $|B_r(z) \cap L|$ we obtain using this method only depend on the dimension and the *minimum* of L,

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

If $r^2 \leq \min(L)$ then Theorem 1 shows that the lattice points in $B_r(z)$ correspond to the elements of a *spherical code* with a certain minimum angle. This gives rise to an upper bound on $|B_r(z) \cap L|$, since there exist various methods to bound the cardinality of a spherical code with a given minimum angle. The most general approach, due to Kabatiansky and Levenshtein, uses linear programming, and is briefly outlined in Sect. 2. Calculations using this linear programming method are summarised in Table 1 for some well known lattices, such as root lattices in dimension up to ten and the Leech lattice, for $r = \sqrt{\mu(L)}$. This choice of r is motivated by the coding theoretic application in Sect. 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 an upper bound on $|B_r(z) \cap L|$ when $r^2 > \min(L)$, we present a different approach in Sect. 3, based on Gaussian measures on L (cf. [2]). 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 bound $\gamma_{r,L}$ depends on the dimension of the lattice and on the number of lattice vectors of each length smaller than some δ, where $\delta > (\frac{n}{2\pi})^{\frac{1}{2}}$. Hence $\gamma_{r,L}$ can be computed from the *theta series* of the lattice.

Table 1 Upper bounds on the number of lattice points in a sphere of radius $\sqrt{\mu(L)}$ for some well known lattices L

Type	n	θ	$[\beta_0, \ldots, \beta_d]$	$A(n, \theta)$	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	$\cos^{-1}\left(\frac{1}{6}\right)$	[1, 2.226, 2.178, 1.010]	10	12	10
	5	$\cos^{-1}\left(\frac{1}{3}\right)$	[1, 2.187, 2.659, 1.941, 0.695, 0, 0, 0.413]	≤ 24	26	20
	6	$\cos^{-1}\left(\frac{5}{12}\right)$	[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	$\cos^{-1}\left(\frac{1}{5}\right)$	[1, 2.143, 2.084, 1.116]	16	20	16
	6	$\cos^{-1}\left(\frac{1}{3}\right)$	[1, 2.166, 2.589, 1.946, 0.722, 0, 0, 0.037]	≤ 37	42	32
	7	$\cos^{-1}\left(\frac{3}{7}\right)$	[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	–	–	$--$	1, 211	512
E	6	$\cos^{-1}\left(\frac{1}{4}\right)$	[1, 1.852, 2.029, 1.311]	27	37	27
	7	$\cos^{-1}\left(\frac{1}{3}\right)$	[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

The bounds obtained for $r = \sqrt{\mu(L)}$ are also in Table 1, and show that in general neither of the two methods to bound $|B_r(z) \cap L|$ is superior to the other. Moreover, our observations let us conjecture the following.

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

From our calculations, summarised in Table 1, we can verify this conjecture in some cases, as follows.

Remark 1 Let L be one of the lattices A_n ($n \in \{2, 3, 4\}$), D_n ($n \in \{3, 4, 5\}$), E_n ($n \in \{6, 7, 8\}$) or the Leech lattice Λ_{24}. Then $\mu(L) \leq \min(L)$ and L satisfies Conjecture 1.

In Sect. 5 we give a coding theoretic application of our results. Lattices are used as code books in important modern communication systems, like MIMO fading channels (cf. [4,5]). In this context decoding a received signal $z \in \mathbb{R}^n$ means finding a lattice point closest to z, i.e. finding $u \in L$ such that $|z-u| \leq |z-l|$ for all $l \in L$. This problem is commonly called the *Closest Vector Problem*. It is NP hard—see [14,16,18] for a study of its complexity.

In this paper we give an algorithm that solves the Closest Vector Problem *approximately* for lattices that are constructed from lattices of smaller dimension. That is, given $z \in \mathbb{R}^n$, one 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. Our algorithm is a generalisation of *Babai's Nearest Plane Procedure* (see [1] and Remark 2 in this paper). Moreover, our algorithm can be used for *Bounded Distance Decoding* (cf. Proposition 2): It always solves the exact version of the Closest Vector Problem if the error vector is sufficiently small, i.e. if $d(z, L) \leq \delta_L$ for some positive real δ_L depending only on L, where

$$d(z, L) = \min\{|z-l| \mid l \in L\}.$$

The lattices considered in this paper are given in the following form. Given positive integers n_i for $i \in \{1, \ldots, t\}$ with $n := \sum_{i=1}^{t} n_i$ and lattices W_i in $\mathbb{R}^{n_i}$ as well as linear maps $f_i : \mathbb{R}^{n_1+\cdots+n_i} \to \mathbb{R}^{n_{i+1}}$, $i \in \{1, \ldots, t-1\}$, consider the lattice

$$\mathcal{L} = \{(l_1, \ldots, l_t) \in \mathbb{R}^n \mid l_1 \in W_1,\ l_i - f_{i-1}(l_1, \ldots, l_{i-1}) \in W_i,\ i \in \{2, \ldots, t\}\}.$$

For example, lattices obtained from Turyn's construction and from Construction A (cf. Chapts. 5 and 8 of [9], respectively) are naturally given in this form (see Lemma 4 and Sect. 5.2, respectively). These include very well known lattices such as the Leech lattice and the recently found extremal unimodular even lattice in dimension 72 (cf. [22]). Moreover, since every lattice is *isometric* to a lattice which has a structure as above, our algorithm can be used for decoding with any lattice in $\mathbb{R}^n$ (see Remark 2). The recursive definition of the points in $\mathcal{L}$ allows to approximate a vector $(z_1, \ldots, z_t) \in \mathbb{R}^{n_1+\cdots+n_t}$ by successive approximations in the W_i. The respective algorithm is given in Sect. 5. A variant of this algorithm uses sphere decoding as a subroutine to obtain all points of W_1 in a certain small sphere B around z_1 first. Proposition 3 gives an approximation factor in terms of the covering radii of the lattices W_i. 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 and from Construction A (Sects. 5.1 and 5.2, respectively). 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 [22]).

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

A *spherical code* in $\mathbb{R}^n$ is a finite subset of the unit sphere $B_1(0)$, i.e. a set of vectors in $\mathbb{R}^n$ of length one. A spherical code $\mathcal{C}$ is said to have *minimum angle* θ if the angle between two distinct elements of $\mathcal{C}$ is at least θ. An upper bound on the cardinality of a spherical code with a given minimum angle can be calculated by solving a certain linear program, an approach due to Kabatiansky and Levenshtein (see [9, Chap. 9]) that will be outlined in this section.

Lattices give rise to spherical codes with certain minimum angles. For instance, the vectors of minimum nonzero length in L, when normalised as to be of length one, form a spherical

code with minimum angle $\frac{\pi}{3}$ (cf. [9, Chap. 2.3]). This has been used by Odlyzko and Sloane in [9, Chap. 13] to derive an upper bound on the number of vectors of minimal nonzero length in a lattice, also called the *kissing number*.

In Theorem 1 we observe that more generally, for every sphere $B_r(z)$ with $r^2 \leq \min(L)$ centered at *any* point $z \in \mathbb{R}^n$, the lattice points contained in that sphere give rise to a spherical code with a certain minimum angle.

This enables us to obtain an upper bound on $|B_r(z) \cap L|$ using the linear programming bounds for spherical codes. The results are summarised in Table1. In the remainder of this section, for reader's convenience we give a very brief and simplified explanation of the linear programming method for spherical codes. For a more detailed description, the reader is referred to [9, Chap. 9].

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*

$$\mathcal{C} := \{|x - z|^{-1} (x - z) \mid x \in B_r(z) \cap L\}$$

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

Proof For any $x, y \in B_r(z) \cap L$, 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 $a \in (0, r]$ consider the real function $f_a : t \mapsto \frac{a^2+t^2-\min(L)}{2at}$. This function is increasing since by assumption $a \leq r \leq \sqrt{\min(L)}$ and hence for any real t,

$$\frac{\mathrm{d}\, f_a}{\mathrm{d}t}(t) = \frac{t^2 - a^2 + \min(L)}{2at^2} \geq 0.$$

For symmetry reasons, it follows that the right hand side of 2 is maximised if $|x - z| = |y - z| = r$. In this case, eqnarray 2 reads $\cos(\theta) \leq 1 - \frac{\min(L)}{2r^2}$ as desired. □

In the paper [21] the interested reader may find similar techniques as the one used in the proof of Theorem 1. In what follows, to illustrate the results in Table 1 we briefly outline Kabatiansky's and Levenshtein's approach to bound $A(n, \theta)$ from above by means of a linear program. For a more detailed outline, the reader may refer to Chapter 9 of [9].

The variables of the *primal* linear program model the *weight distribution* of the putative spherical code, which is defined below. By $\angle(c, c')$ we denote the angle between two real vectors of the same dimension.

Definition 1 Let $\mathcal{C}$ be a spherical code. For $t \in [-1, 1]$ let

$$\omega_t := \frac{1}{|\mathcal{C}|} |\{(c, c') \in \mathcal{C} \times \mathcal{C} \mid \cos \angle(c, c') = t\}|.$$

Then $(\omega_t)_{t\in[-1,1]}$ is called the *weight distribution* of $\mathcal{C}$.

One derives linear inequalities for the ω_t, considering the action of the special orthogonal group on the complex vector space of *spherical harmonics*.

Definition 2 The space $\mathrm{Harm}(k, n)$ of *spherical harmonics of degree k in dimension n* is the complex vector space of all functions f on

$$\partial B_1(0) = \{v \in \mathbb{R}^n \mid |v| = 1\}$$

that are represented by a homogeneous element $p_f \in \mathbb{C}[X_1, \ldots, X_n]$ of total degree k and satisfy Laplace's equation

$$\nabla^2 f = \frac{\mathrm{d}^2 f}{\mathrm{d}X_1^2} + \cdots + \frac{\mathrm{d}^2 f}{\mathrm{d}X_n^2} = 0.$$

This space is equipped with a Hermitian scalar product,

$$\langle f, g\rangle = \int\limits_{\partial B_1(0)} f(z)\overline{g(z)} d\lambda_n(z),$$

where λ_n is the normalised Lebesgue measure on $\partial B_1(0)$.

The special orthogonal group $\mathrm{SO}(n)$ acts naturally on $\mathrm{Harm}(k, n)$ by $g \cdot f := (z \mapsto f(g^{-1}z))$, for $g \in \mathrm{SO}(n)$ and $f \in \mathrm{Harm}(k, n)$. Since this action leaves the above scalar product invariant, the representation $\rho : \mathrm{SO}(n) \to \mathrm{End}_{\mathbb{C}}(\mathrm{Harm}(k, n))$ induced by this operation is *unitary*. Explicitly, this means that if $\mathcal{F} := (f_1, \ldots, f_m)$, with $m = \dim(\mathrm{Harm}(k, n))$, is an orthonormal basis of $\mathrm{Harm}(k, n)$ with respect to the above scalar product then for every $g \in \mathrm{SO}(n)$ the matrix $M(g)$ defined by $(\rho(g))(f_i) = \sum_{j=1}^m M(g)_{ij} f_j$ for $i \in \{1, \ldots, m\}$ is unitary.

We may assume that $h \cdot f_1 = f_1$ for all $h \in H := \mathrm{Stab}_{\mathrm{SO}(n)}(z_0)$ for some element $z_0 \in \partial B_1(0)$, i.e. that f_1 is constant on the orbits of H on $\partial B_1(0)$. So by means of the bijection $\kappa : H \backslash \mathrm{SO}(n) \to \partial B_1(0),\ H \cdot g \mapsto g^{-1} \cdot z_0$ one can define a function

$$J_k : \partial B_1(0) \times \partial B_1(0) \to \mathbb{C},\ (z, z') \mapsto (M(g)\overline{M(g')}^{\mathrm{tr}})_{1,1},$$

where $\kappa(Hg) = z$ and $\kappa(Hg') = z'$.

Using the fact that ρ is unitary, one easily verifies that J_k does not depend on the choice of the basis $\mathcal{F}$ and moreover, that

(1) J_k is $\mathrm{SO}(n)$-*invariant*, i.e. $J_k(gx, gy) = J_k(x, y)$ for all $x, y \in \partial B_1(0)$ and all $g \in \mathrm{SO}(n)$ and
(2) J_k is *positive definite*, i.e. $\sum_{x,y\in U} J_k(x, y) \geq 0$ for all $U \subseteq \partial B_1(0)$.

Due to (1) and since the function $\partial B_1(0) \times \partial B_1(0) \to [-1, 1],\ (z, z') \mapsto \cos \angle(z, z')$ is a separating invariant for the diagonal action of $\mathrm{SO}(n)$ on $\partial B_1(0) \times \partial B_1(0)$, one can define a so-called *zonal spherical function*

$$\phi_k : [-1, 1] \to \mathbb{R},\ t \mapsto J_k(x, y), \quad \text{where } x, y \in \partial B_1(0) \text{ s.t. } \cos \angle(x, y) = t.$$

The zonal spherical function is a scalar multiple of a *Jacobi polynomial*; we have $\phi_k(t) = \binom{k+\alpha}{\alpha}^{-1} P_k^{\alpha,\alpha}(t)$ with $\alpha = \frac{n-3}{2}$.

Now because of (2), the weight distribution $(\omega_t)_{t\in[-1,1]}$ of any spherical code $\mathcal{C}$ satisfies

$$\begin{aligned}\sum_t \omega_t \phi_k(t) &= |\mathcal{C}|^{-1} \sum_t |\{(c, c') \in \mathcal{C} \times \mathcal{C} \mid \cos \angle(c, c') = t\}| \cdot J_k(c, c') \\ &= |\mathcal{C}|^{-1} \sum_{c,c'\in\mathcal{C}} J_k(c, c') \geq 0.\end{aligned}$$

From the above and the obvious inequalities $\omega_t \geq 0$ for all $t \in T$ and $\omega_1 = 1$, one derives the following linear program that outputs an upper bound on $|\mathcal{C}| = \sum_t \omega_t$:
Primal program: Choose a natural number N and a finite subset $T = \{t_1, \ldots, t_s\}$ of $[-1, \cos(\theta)]$. Maximise $\sum_{t\in T} \omega_t$ subject to the constraints $\omega_t \geq 0$ and $\sum_{t\in T} \phi_i(t)\omega_t \geq -\phi_i(1)$ for all $i \in \{1, \ldots, N\}$.
Changing to the dual linear program allows to give an upper bound on $|\mathcal{C}|$ that is independent from the choice of T, in Lemma 1.
Dual Program: Minimise $\sum_{i=1}^{N} \beta_i \phi_i(1)$ subject to the conditions $\beta_i \geq 0$ and $\sum_{i=1}^{N} \beta_i \phi_i(t) \leq -1$ for all $t \in T$.

Together with Theorem 1 this yields the following lemma, which is a slight modification of the main theorem in [9, Chap. 13].

Lemma 1 *Let L be a lattice in $\mathbb{R}^n$ and let r be a positive real such that $\frac{\min(L)}{4} \leq r^2 \leq \min(L)$. Let p be a real polynomial satisfying the following conditions:*

(i) $p(t) \leq 0$ *for* $-1 \leq t \leq 1 - 2\frac{\min(L)}{2r^2}$,

(ii) *if* $p(t) = \sum_{i=0}^{d} \beta_i P_i^{\alpha,\alpha}$ *is the expansion of p in terms of Jacobi polynomials, where* $\alpha = \frac{n-3}{2}$ *and d is the degree of p, then* $\beta_0 > 0$ *and* $\beta_i \geq 0$ *for* $i \in \{1, \ldots, d\}$.

Then $|B_r(z) \cap L| \leq \frac{p(1)}{\beta_0}$ *for every* $z \in \mathbb{R}^n$.

Note that to find p in Lemma 1, one may use the dual program described above, choosing some finite subset $T \subset [-1, \cos(\theta)]$ that is not too small, and then verify that $p := \sum_{i=1}^{N} \beta_i \phi_i$ satisfies the conditions of Lemma 1.

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 $(\cdot, \cdot)\colon \mathbb{R}^n \times \mathbb{R}^n,\ (v, w) \mapsto v_1 w_1 + \cdots + v_n w_n$ is the standard scalar product on $\mathbb{R}^n$. Moreover, let $\det(L)$ be the determinant of a Gram matrix of L.

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 by a vector $z \in \mathbb{R}^n$, i.e. $L - z := \{l - z \mid l \in L\}$, to derive an upper bound on $|B_r(z) \cap L|$. Gaussian measures have already been used by Banaszczyk in [2] to prove *transcendence theorems* for lattices. In Lemma 1 of [19], they are used to give an upper bound on the number of points of the standard lattice in a small sphere. The latter result is generalised to arbitrary lattices in the following theorem.

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 $|L \cap B_r(z)| \leq \gamma_{r,L,z}$, 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 $\gamma_{r,L,z} \leq \gamma_{r,L}$, where

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

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

To calculate the bound from Theorem 2 for a given lattice, one has to enumerate the lattice points within a small sphere centered at 0. This problem may seem quite similar to the initial problem of counting the number of lattice points in a small sphere. But in the initial problem, the center of the sphere is arbitrary, wheras in the calculation of the bound from Theorem 2 the sphere is centered at 0. So the number of lattice points contained in a small sphere centered *anywhere* is controlled by the lattice points of length at most δ. Moreover, the enumeration of all lattice points within $B_\delta(0)$ may be easier than the initial one, since the number of lattice points of any length can be read off from the lattice's theta series.

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

Lemma 2 (cf. Lemma 2.9 of [20]) *With f as above, we have*

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

for every $z \in \mathbb{R}^n$.

Proof Our proof uses the Poisson summation formula for lattices, which states that for every lattice L in $\mathbb{R}^n$ and every 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 $\hat{g} : \mathbb{R}^n \to \mathbb{C}, \quad y \mapsto \int_{\mathbb{R}^n} e^{2\pi i(x,y)} g(x)dx$ 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, whereas the Fourier transform of the translate is $y \mapsto e^{-2\pi i(z,y)} f(y)$. Hence Poisson summation yields

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

□

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*

$$\sum_{x\in L-B_\delta(0)} f(x) \le (1 - R_\delta^{-1}) \sum_{x\in L} f(x),$$

where R_δ is as in Theorem 2.

Proof of Theorem 2 To prove the first statement of Theorem 2, consider the inequality chain

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

The first inequality simply stems from the fact that $|L \cap B_r(z)| = |(L - z) \cap B_r(0)|$. The second inequality is part of the assertion of Lemma 2. Let $\delta > \left(\frac{n}{2\pi}\right)^{\frac{1}{2}}$, then it follows from Lemma 3 that

$$\sum_{y \in L^\sharp - B_\delta(0)} f(y) \leq (1 - R_\delta^{-1}) \sum_{y \in L^\sharp} f(y).$$

Hence the right hand side of the above inequality chain is bounded above by

$$\begin{aligned} \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp} f(y) &\leq \det(L)^{-\frac{1}{2}} \left(\sum_{y \in L^\sharp \cap B_\delta(0)} f(y) + (1 - R_\delta^{-1}) \sum_{y \in L^\sharp} f(y) \right) \\ &= \det(L)^{-\frac{1}{2}} \sum_{y \in L^\sharp \cap B_\delta(0)} f(y)\, R_\delta, \end{aligned}$$

which proves the first statement of the theorem. The second statement is proved analogously, using the inequality $\sum_{x \in L - z} f(x) \leq \sum_{x \in L} f(x)$ from Lemma 2. □

4 Results for some well known lattices

For some well known lattices L, the following table gives upper bounds on $|B_{\sqrt{\mu(L)}}(z) \cap L|$, where $z \in \mathbb{R}^n$ is arbitrary ($n = \dim(L)$).

If $\mu(L) \leq \min(L)$ then Theorem 1 applies, i.e. the set $B_{\sqrt{\min(L)}}(z) \cap L$ corresponds to a spherical code in $\mathbb{R}^n$ with minimum angle θ as given in Theorem 1. An upper bound on $\max_{z \in \mathbb{R}^n} |B_{\sqrt{\mu(L)}}(z) \cap L|$ is hence given by $A(n, \theta)$. To calculate an upper bound on $A(n, \theta)$, the author implemented the linear programming method described in [9, Chap. 13] in MAGMA [3], obtaining a polynomial p as in Lemma 1. The coefficients of p in the expansion in terms of Jacobi polynomials are given in the fourth column, rounded to three decimal places, as a sequence $[\beta_0, \ldots, \beta_d]$, meaning that $p(t) = \beta_0 P_0^{\alpha,\alpha}(t) + \cdots + \beta_d P_d^{\alpha,\alpha}(t)$, where α and d are as in Lemma 1.

The penultimate column gives the bound obtained from Theorem 2. This bound was calculated using the respective lattice's theta series. 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 one. The last column of the table gives the maximal number $|B_{\sqrt{\mu(L)}}(z) \cap L|$ attained at a deep hole z of L. Obviously, if this number equals the given upper bound on $A(n, \theta)$ then this bound is attained and equals $A(n, \theta)$. In this case the lattice points closest to the deep hole form an optimal spherical code.

5 A recursive decoding algorithm for lattices

In this section we describe a recursive decoding algorithm for lattices, viewing them as constructed from lattices of smaller dimension by a procedure resembling the *gluing method* (see [9, Chap. 4]). Roughly speaking, the algorithm decodes a lattice by decoding its lower dimensional lattice components.

Lattices obtained from Turyn's construction and from Construction A have a particular structure of this kind. Among these lattices there are the Leech lattice and Nebe's extremal even unimodular lattice in dimension 72 [22]; in Sect. 5.1 the algorithm is applied to these lattices.

The lattices considered here are of the following form: Let $n_1, \ldots, n_t$ be positive integers and let $W_1, \ldots, W_t$ be lattices in $\mathbb{R}^{n_i}$. Moreover, let

$$f_i : \mathbb{R}^{n_1+\cdots+n_i} \to \mathbb{R}^{n_{i+1}}$$

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

$$\mathcal{L} := \{(l_1, \ldots, l_t) \in \mathbb{R}^n \mid l_1 \in W_1,\ l_i - f_{i-1}(l_1, \ldots, l_{i-1}) \in W_i\ (i = 2, \ldots, t)\}. \quad (\dagger)$$

Clearly $\mathcal{L}$ is a lattice in $\mathbb{R}^n$. The following is a natural algorithm to find a point nearby a given vector in $\mathbb{R}^n$ in a lattice $\mathcal{L}$ as above. The meaning of *nearby* will be precised in Proposition 1.

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.
Output: A point in $\mathcal{L}$ nearby z.

(1) Compute the set C of all closest lattice points in $W_1 - z_1$.
(2) For each point $c \in C$ found in step (1), let $F(c)$ be the lattice point $(c_1, \ldots, c_t) \in \mathcal{L}$ defined recursively by $c_1 := c$ and $c_i := f_{i-1}(c_1, \ldots, c_{i-1})$ for $i = 2, \ldots, t$. Moreover, let $\mathcal{L}' := \mathcal{L}(W_2, \ldots, W_t, f_2, \ldots, f_{t-1})$, and let

$$z' = ((z - F(c))_2, \ldots, (z - F(c))_t),$$

where $(z - F(C))_i \in \mathbb{R}^{n_i}$ is the ith component vector of $z - F(c)$, for $i \in \{2, \ldots, t\}$. Iterate steps (1) and (2) to find the set C' of all points in $\mathcal{L}'$ closest to z', and output the set $\{F(c) + (0, c') \mid c \in C,\ c' \in C'\}$.

Among all the approximations found, choose one that is closest to z.

Remark 2 (i) A lattice is of the form (†) if it is generated by the rows of an upper block triangular matrix. Then generator matrices for the W_i are given by the quadratic blocks around the diagonal, and basis matrices for the linear maps f_i can be read off from the entries on the right of each block. In particular, lattices whose basis matrix is a scalar multiple of an integral matrix are of the form (†) since their Hermite normal form provides an upper triangular basis matrix.

(ii) Every lattice L in $\mathbb{R}^n$ is *isometric* to a lattice of the form (†), that is, there exists an isometry φ_L of $\mathbb{R}^n$ such that $\varphi_L(L)$ is of the form (†). Algorithm $\mathcal{A}'$ may hence be applied to approximate $\varphi_L(z)$ in $\varphi_L(L)$. If $\varphi_L(x)$ is the obtained approximation, then x is an approximation of z in L, with $|x - z| = |\varphi_L(x) - \varphi_L(z)|$.
The desired isometry is obtained via a QR factorisation of a basis matrix of L. More explicitly, let $B = (b_1, \ldots, b_n)$ be a basis of L and let $B^* = (|b_1^*|^{-1} b_1^*, \ldots, |b_n^*|^{-1} b_n^*)$ be its Gram Schmidt orthonormalisation (i.e. $(b_1^*, \ldots, b_n^*)$ is the Gram Schmidt orthogonalisation of B). Let M^B be the corresponding basis change matrix, defined by $b_i = \sum_{j=1}^n M_{ij}^B |b_j^*|^{-1} b_j^*$. Since this is a lower triangular matrix, according to (i) the lattice L^B generated by the rows of M^B is, up to coordinate permutation, of the form (†). Moreover, the isometry φ_L which maps B^* to the standard basis of $\mathbb{R}^n$ maps L to L^B.

(iii) The *Nearest Plane Procedure* (NPP), given by Babai in [1], is actually Algorithm $\mathcal{A}'$ in a special case.

Recall that given a basis $B = (b_1, \ldots, b_n)$ for a lattice L in $\mathbb{R}^n$, Babai's algorithm solves the Closest Vector Problem for L recursively. An approximation factor of 2^n is achieved if B is LLL reduced (see also Remark 3). To approximate $x \in \mathbb{R}^n$, let U be the real vector space generated by $b_1, \ldots, b_{n-1}$ and choose $l \in L$ such that the distance between x and the affine hyperplane $l + U$ is minimised. Then let $x' \in U$ be the orthogonal projection of $x - l$ onto U and repeat the above procedure with x' and the lattice L' generated by $b_1, \ldots, b_{n-1}$. Since here the dimension is lower, iteration of this process yields an approximation $l' \in L'$ of x'. Then $l' + l$ is the NPP approximation to x.

Since the closest affine hyperplane $l + U$ (with $l \in L$) can be found using the Gram Schmidt orthogonalisation $(b_1^*, \ldots, b_n^*)$ of B, one easily verifies that the NPP is indeed Algorithm $\mathcal{A}'$ applied to

$$\mathcal{L}(|b_n^*|\mathbb{Z}, \ldots, |b_1^*|\mathbb{Z}, f_1, \ldots, f_{n-1}) \cong L,$$

where the f_i are given by the coefficients of the basis change matrix M^B defined in (ii).

Proposition 1 *Let $\mathcal{L} = \mathcal{L}(W_1, \ldots, W_t, f_1, \ldots, f_{t-1})$ and let $z \in \mathbb{R}^n$, where $n = \dim(\mathcal{L})$. Let $w \in \mathcal{L}$ be the approximation of z obtained using Algorithm $\mathcal{A}'$. Then*

$$|z - w|^2 \leq \gamma_t \cdot |z - l|^2$$

for all $l \in \mathcal{L}$, where γ_t is defined recursively by

$$\gamma_1 := 4\frac{\mu(W_t)}{\min(W_t)} \quad \text{and} \quad \gamma_j := \max\{4\frac{\sum_{i=t-j+1}^{t} \mu(W_i)}{\min(W_{t-j+1})}, \gamma_{j-1} + 1\}$$

for $j \in \{2, \ldots, t\}$.

Proof Let $u \in \mathcal{L}$ be a closest lattice point to z, and write $u = (u_1, \ldots, u_t)$, $z = (z_1, \ldots, z_t)$ and $w = (w_1, \ldots, w_t)$ according to the partition of n given by the dimensions of the lattices W_i. We distinguish two cases.

Case 1: u_1 is a closest lattice point in W_1–z_1, so without loss of generality $w_1 = u_1$. We proceed by induction on t. Let $t = 1$. Recall that always $4\mu(W_t) \geq \min(W_t)$ since the packing radius of a lattice is at most equal to its covering radius. So $\gamma_1 \geq 1$, and the claim of the Theorem follows for $t = 1$.

Now let $t \geq 2$. As in the definition of Algorithm $\mathcal{A}'$, for a given $y_1 \in W_1$ the lattice point $(y_1, \ldots, y_t) \in \mathcal{L}$ defined recursively by $y_i := f_{i-1}(y_1, \ldots, y_{i-1})$, for $i = 2, \ldots, t$, will be denoted by $F(y_1)$.

As a preparation for the induction step, observe that

$$\begin{aligned} |z - w|^2 &= |z_1 - w_1|^2 + |(z_2 - w_2, \ldots, z_t - w_t)|^2 \\ &\leq |z - u|^2 + |(w_1, z_2, \ldots, z_t) - w|^2 \\ &= |z - u|^2 + |(w_1, z_2, \ldots, z_t) - F(w_1) - (w - F(w_1))|^2. \end{aligned}$$

Since u is a closest lattice point in $\mathcal{L}$ to z, $u - F(w_1)$ is a closest lattice point to $z' := (w_1, z_2, \ldots, z_t) - F(w_1)$ in $\mathcal{L}' := \mathcal{L}(W_2, \ldots, W_t, f_2, \ldots, f_{t-1})$. Moreover, $w - F(w_1)$ is an approximation of z' in $\mathcal{L}'$ obtained in the iteration step of Algorithm $\mathcal{A}'$. Hence by induction and the above inequality chain

$$\begin{aligned}|z-w|^2 &\le |z-u|^2 + \gamma_{t-1}|z' - (u - F(w_1))|^2 \\ &\le |z-u|^2 + \gamma_{t-1}|z-u|^2 \\ &= (1+\gamma_{t-1})|z-u|^2 \le \gamma_t |z-u|^2.\end{aligned}$$

Case 2: u_1 is not a closest lattice point in $W_1 - z_1$. In this case $|z-u|^2 \ge |z_1 - u_1|^2 \ge \frac{\min(W_1)}{4}$. Since on the other hand by construction $|z-w|^2 \le \sum_{i=1}^{t} \mu(W_i)$, it follows that

$$|z-w|^2 \le \left(\sum_{i=1}^{t} \mu(W_i)\right) \cdot \frac{4}{\min(W_1)} |z-u|^2 \le \gamma_t \cdot |z-u|^2,$$

which shows the assertion.

Remark 3 In [1], Babai gives an approximation factor of 2^n for the NPP, provided that one starts with an LLL reduced basis of the lattice L in $\mathbb{R}^n$.

This coincides with the approximation factor given in Proposition 1: Using the NPP means using the structure $L \cong \mathcal{L}(|b_n^*|\mathbb{Z}, \ldots, |b_1^*|\mathbb{Z}, f_2, \ldots, f_n)$ as described in Remark 2, i.e. $(b_1^*, \ldots, b_n^*)$ is the Gram Schmidt orthogonalisation of the lattice basis $B = (b_1, \ldots, b_n)$. In this case the reals γ_j from Proposition 1 are

$$\gamma_1 = 4\frac{\mu(|b_n^*|\mathbb{Z})}{\min(|b_n^*|\mathbb{Z})} = 4\frac{|b_n^*|^2}{4|b_n^*|^2} = 1,$$

and

$$\gamma_j = \max\{\frac{|b_n^*|^2 + \cdots + |b_{n-j+1}^*|^2}{|b_n^*|^2}, \gamma_{j-1} + 1\}$$

for $j \ge 2$. The condition that B be LLL reduced implies that $|b_{i-1}^*|^2 \le 2|b_i^*|^2$ for $i \in \{2, \ldots, n\}$. Hence

$$\frac{|b_n^*|^2 + \cdots + |b_{n-j+1}^*|^2}{|b_n^*|^2} \le \frac{|b_n^*|^2(1 + 2 + \cdots + 2^{j-1})}{|b_n^*|^2} = 2^j - 1.$$

This means that $\gamma_j \le 2^j$ for all $j \ge 2$, yielding the desired approximation factor.

If $d(z, \mathcal{L})$ is sufficiently small then Algorithm $\mathcal{A}'$ always finds the closest lattice point to z. This constrained version of the Closest Vector Problem is called *Bounded Distance Decoding*. For Babai's NPP, it is well known that it solves the Closest Vector Problem on z and a lattice L if

$$d(z, L) \le \min\{\frac{|b_i^*|}{2} \mid i \in \{1, \ldots, n\}\},$$

where $n = \dim(L)$ and $(b_1^*, \ldots, b_n^*)$ is a Gram Schmidt orthogonalisation of the chosen lattice basis. This generalises to arbitrary lattices and Algorithm $\mathcal{A}'$ as follows.

Proposition 2 *[Algorithm $\mathcal{A}'$ and Bounded Distance Decoding]*
Let $\mathcal{L} = \mathcal{L}(W_1, \ldots, W_t, f_1, \ldots, f_{t-1})$ and let $z \in \mathbb{R}^n$, where $n = \dim(\mathcal{L})$. If

$$d(z, \mathcal{L}) \le \min\left\{\frac{\sqrt{\min(W_i)}}{2} \mid i \in \{1, \ldots, t\}\right\}$$

then Algorithm $\mathcal{A}'$ solves the Closest Vector Problem for $\mathcal{L}$ and z.

Proof Let w be an approximation in $\mathcal{L}$ of z found by Algorithm $\mathcal{A}'$, and let $u \in \mathcal{L}$ be a closest lattice point to z. Write $z = (z_1, \ldots, z_t)$ with $z_i \in \mathbb{R}^{n_i}$, where $n_i = \dim(W_i)$ for $i = 1, \ldots, t$. Analogously, write $w = (w_1, \ldots, w_t)$ and $u = (u_1, \ldots, u_t)$.

By definition of the lattice minimum, if $B = B_{\frac{\sqrt{(\min(W_1))}}{2}}(z_1)$ contains two distinct elements of W_1 then these elements both lie on the border of B. On the other hand, by assumption

$$|u_1 - z_1| \leq d(z, \mathcal{L}) \leq \frac{\sqrt{\min(W_1)}}{2},$$

so $u_1 \in W_1$ is contained in B. Since w_1 is a closest lattice point in W_1–z_1, this yields $|u_1 - z_1| = |w_1 - z_1|$, so u_1 is closest in W_1–z_1, too. Now let the notation be as in the definition of Algorithm $\mathcal{A}'$. Since u_1 is a closest lattice point in W_1–z_1, Algorithm $\mathcal{A}'$ is iterated for $\mathcal{L}' = \mathcal{L}(W_2, \ldots, W_t, f_2, \ldots, f_{t-1})$ and $z' = ((z - F(u_1))_2, \ldots, (z - F(u_1))_t)$. By construction $d(z', \mathcal{L}') \leq d(z, \mathcal{L})$ and hence the claim follows by induction on t. □

The following algorithm is a natural modification of Algorithm $\mathcal{A}'$ as to obtain a better approximation. The closer the parameter r is set to $\sqrt{\mu(\mathcal{L})}$, the better the obtained approximation.

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 $i \in \{1, \ldots, t\}$), a lattice $\mathcal{L} = \mathcal{L}(W_1, \ldots, W_t, f_1, \ldots, f_{t-1})$ as above and a real number $r \in (0, \sqrt{\mu(\mathcal{L})}]$.
Output: A point in $\mathcal{L}$ nearby z.

(1) Compute the set $C = W_1 \cap B_r(z_1)$ (e.g. by sphere decoding).
(2) For each point $c \in C$ found in step (1), let $F(c)$ be the lattice point $(c_1, \ldots, c_t) \in \mathcal{L}$ defined recursively by $c_1 := c$ and $c_i := f_{i-1}(c_1, \ldots, c_{i-1})$ for $i = 2, \ldots, t$. Moreover, let $\mathcal{L}' := \mathcal{L}(W_2, \ldots, W_t, f_2, \ldots, f_{t-1})$, and let

$$z' = ((z - F(c))_2, \ldots, (z - F(c))_t).$$

Iterate steps (1) and (2) to find the set C' of all points in $\mathcal{L}'$ closest to z', and output the set $\{F(c) + (0, c') \mid c \in C,\ c' \in C'\}$.

Among all the approximations found, choose one that is closest to z.

The following two propositions are immediate from Propositions 1 and 2, respectively.

Proposition 3 *Let $\mathcal{L} = \mathcal{L}(W_1, \ldots, W_t, f_1, \ldots, f_{t-1})$ be as above. Let w be the approximation of z found by Algorithm $\mathcal{A}$, using sphere decoding with radius $r \leq \sqrt{\mu(\mathcal{L})}$ in the first step. Define real numbers γ_j by*

$$\gamma_1 := 4\frac{\mu(W_t)}{\min(W_t)} \quad \text{and} \quad \gamma_j := \max\{4\frac{\sum_{i=t-j+1}^{t} \mu(W_i)}{\min(W_{t-j+1})}, \gamma_{j-1} + 1\}$$

for $j \in \{2, \ldots, t-1\}$. Then

$$|w - z|^2 < \max\{r^{-2} \sum_{i=1}^{t} \mu(W_i), 1 + \gamma_{t-1}\} \quad |l - z|^2$$

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

Proposition 4 (Algorithm $\mathcal{A}$ and bounded distance decoding)
Let $\mathcal{L} = \mathcal{L}(W_1, \ldots, W_t, f_1, \ldots, f_{t-1})$ and let $z \in \mathbb{R}^n$, where $n = \dim(\mathcal{L})$. Let $r \in (0, \sqrt{\mu(\mathcal{L})}]$. If

$$d(z, \mathcal{L}) \leq \min\{r, \frac{\sqrt{\min(W_i)}}{2} \mid i \in \{2, \ldots, t\}\}$$

then Algorithm $\mathcal{A}$ with sphere decoding at radius r in the first step solves the Closest Vector Problem for $\mathcal{L}$ and z.

5.1 Application to lattices obtained from Turyn's construction

In [25], Turyn gave a construction of a lattice in dimension $s \cdot t$ based upon a polarisation of a lattice in dimension s (where s and t are integers, with $t \geq 2$), as follows. The Leech lattice, for instance, can be constructed in this way from a polarisation of E_8 (cf. [15, Cor. 2.11]), and Nebe's extremal even unimodular lattice in dimension 72 (cf. [22]), in turn, is obtained by a polarisation of the Leech lattice.

Definition 3 (cf. [23]) Let L be a lattice in $\mathbb{R}^s$ 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 $t \geq 2$, one defines $\mathcal{M} = \mathcal{M}(L, M, N, t)$ by

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

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

Lemma 4 *With L, M, N, s and t as above, we have*

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

where there are $t-2$ copies of N, $\iota_i : \mathbb{R}^{i \cdot s} \to \mathbb{R}^s,\ (u_1, \ldots, u_i) \mapsto u_1$ for $i \in \{1, \ldots, t-2\}$. The map f is defined as follows: Choose a basis $(a_1+b_1, \ldots, a_s+b_s)$ of $L = M+N$, where $a_i \in N$ and $b_i \in M$ for $i \in \{1, \ldots, s\}$. Then let the linear map $\pi_N : \mathbb{R}^s \to \mathbb{R}^s,\ a_i+b_i \mapsto a_i$, so in particular $\pi_N(l) \in N$ and $l - \pi_N(l) \in M$ for every $l \in L$. Now let

$$f : \perp_{i=1}^{t-1} \mathbb{R}^s \to \mathbb{R}^s,\ \ (u_1, \ldots, u_{t-1}) \mapsto u_1 - \pi_N(u_2 + \cdots + u_{t-1}).$$

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

Proposition 5 *Let $\mathcal{M}$ be as above and let w be the approximation in $\mathcal{M}$ of z found by Algorithm $\mathcal{A}'$, using sphere decoding with radius $r \in [\sqrt{\mu(L)}, \sqrt{\mu(\mathcal{M})}]$. Then for all $m \in \mathcal{M}$,*

$$|z - w|^2 \leq (16t - 12)\frac{\mu(L)}{\min(L)} \cdot |z - m|^2.$$

Proof Recall that always $4\mu(L) \geq \min(L)$, since the packing radius of a lattice is at most equal to its covering radius. Moreover, $4\mu(L) \geq \mu(N) \geq \mu(L)$ since $2L \subseteq N \subseteq L$. Using these inequalities, one easily verifies that the numbers γ_j from Proposition 3 satisfy

$$\gamma_j \leq 16\frac{\mu(L)}{\min(L)} + 4(j-1)\frac{\mu(N)}{\min(N)}$$

for $j \in \{1, \ldots, t-1\}$. Hence $\gamma_t = \gamma_{t-1} + 4\frac{\mu(L)}{\min(L)} = (16t - 12)\frac{\mu(L)}{\min(L)}$ as claimed. □

Example 1 (Algorithm $\mathcal{A}$ for Nebe's extremal even unimodular lattice Λ_{72} in dimension 72 [22]) This lattice of minimum 8 is obtained from a polarisation of the Leech lattice Λ_{24} with $t = 3$ and $M \cong N \cong \sqrt{2}\Lambda_{24}$.

Using Proposition 1 and the fact that $\mu(\Lambda_{24}) = \frac{1}{2}\min(\Lambda_{24})$, one easily verifies that Algorithm $\mathcal{A}'$ yields an approximation factor of 14. For Algorithm $\mathcal{A}$ with sphere decoding

at radius $\sqrt{\mu(\Lambda_{24})}$ one obtains an approximation factor of seven; the effort for Algorithm $\mathcal{A}$ compared to Algorithm $\mathcal{A}'$ is increased by a factor of at most

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

by the computational result in Table 1. It follows from Proposition 2 that whenever Algorithm $\mathcal{A}'$ outputs a vector within a distance of $\frac{\sqrt{\min(\Lambda_{24})}}{2}$ from z, that vector is an optimal approximation. The same holds for Algorithm $\mathcal{A}$ when used with sphere decoding at radius $r = \sqrt{\mu(\Lambda_{24})}$ and output vectors at distance at most $\sqrt{\mu(\Lambda_{24})}$ from z, by Proposition 4.

5.2 Application to lattices obtained from construction A

Let C be a binary linear code, i.e. a subspace of the vector space $\mathbb{F}_2^n$, for some positive integer n. Then

$$L(C) := \{(z_1, \ldots, z_n) \in \mathbb{Z}^n \mid z_i \equiv c_i \pmod 2 \text{ for some } (c_1, \ldots, c_n) \in C\}$$

is a lattice in $\mathbb{R}^n$, with $2\mathbb{Z}^n \subset L(C)$, called the *codelattice* of C. The above way to construct a lattice from C is called Construction A (cf. [9, Chap. 5]).

Possibly after a permutation of the coordinates, we may assume that C has a generator matrix of the form

$$\left(\begin{array}{c|c} & v_1 \\ I_k & \vdots \\ & v_k \end{array}\right),$$

where I_k is the identity matrix of size $k = \dim(C)$ and $v_1, \ldots, v_k \in \mathbb{F}_2^{1\times(n-k)}$. Then $L(C) = \mathcal{L}(\mathbb{Z}^k, 2\mathbb{Z}^{n-k}, f)$ with $f : \mathbb{R}^k \to \mathbb{R}^{n-k}$, $e_i \mapsto v_i$ for $i \in \{1, \ldots, k\}$, where e_i is the ith standard basis vector in $\mathbb{R}^k$. Proposition 3 now gives an approximation factor of

$$\max\left\{n - k + 1, \frac{4n - 3k}{4r^2}\right\}$$

for Algorithm $\mathcal{A}$, when applied with sphere decoding at radius $r \in [\sqrt{\mu(\mathbb{Z}^k)} = \frac{\sqrt{k}}{2}, \sqrt{\mu(L(C))}]$. Let us remark that, as seen in the proof of Theorem 2,

$$|B_{\mu(\mathbb{Z}^k)}(v) \cap \mathbb{Z}^k| \le e^{\pi k \frac{\alpha^2}{4}} \sum_{l\in\mathbb{Z}^k} e^{-\pi\alpha^2(l,l)} = (e^{\pi\frac{\alpha^2}{4}} \sum_{l\in\mathbb{Z}} e^{-\pi\alpha^2 l^2})^k,$$

for every $z \in \mathbb{R}^k$ and every scaling factor $\alpha \in \mathbb{R} - \{0\}$. Plugging in $\alpha = 0.76$ yields

$$|B_{\mu(\mathbb{Z}^k)}(v) \cap \mathbb{Z}^k| \le 2.0891^k.$$

This shows the geometrically obvious observation that Conjecture 1 holds for the lattices $\mathbb{Z}^k$, where $k \in \{1, 2\}$. Although it may seem intuitive that Conjecture 1 holds for the standard lattice in any dimension, in fact it does not.

Example 2 Consider the lattice $L = \mathbb{Z}^{44}$, which has a (squared) covering radius of $\mu = \frac{44}{4} = 11$. All the deep holes of L are translates of $(\frac{1}{2}, \ldots, \frac{1}{2})$ by lattice points. Hence it is easy to see that if z is a deep hole of L then $B_{\sqrt{\mu}}(z) \cap L$ is the set of vertices of a 44-dimensional hypercube with side length 1. Hence $|B_{\sqrt{\mu}}(z) \cap L| = 2^{44}$. On the other hand, the set $B_{\sqrt{\mu}}(0) \cap L$ is just the set of all vectors of length up to $\sqrt{\mu}$ in L. As one may verify

using the theta series of L, the latter set has cardinality $19061913603401 > 2^{44}$. Hence the function defined in Conjecture 1 does not take its maximum in a deep hole of L (note that $\min(L) = 1 < \mu$).

Acknowledgments During the development of this study, the author was supported by the Alexander von Humboldt Foundation.

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. Symb. Comput. **24**, 235–265 (1997).
4. Caire G., Damen M.O., Gamal, H.E.: 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., Gamal, H.E.: 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. Iberoam. **11**, 417–429 (1995).
7. Cohn-Vossen S., Hilbert D.: Geometry and the Imagination. Chelsea Publishing Company, London (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, New York (1988).
10. Conway J.H., Sloane N.J.A.: On the covering multiplicity of lattices. Discret. Comput. Geom. **8**, 109–130 (1992).
11. Delsarte P., Goethals J.M., Seidel J.J.: Spherical codes and designs. Geom. Dedic. **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. Comput. **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. Goldwasser S., Micciancio D.: Complexity of Lattice Problems, A Cryptographic Perspective. In: Springer International Series in Engineering and Computer Science, vol. 671. Springer, New York (2002).
15. Griess Jr., R. L.: Rank 72 high minimum norm lattices. J. Num. Theory **130**, 1512–1519 (2010).
16. Guruswami V., Micciancio D., Regev, O.: The complexity of the covering radius problem. Comput. Complex. **14**, 90–121 (2005).
17. Heath-Brown D. R.: Lattice points in the sphere. Numb. Theory Prog. **2**, 883–892 (1999).
18. Khot S.: Inapproximability Results for Computational Problems on Lattices.The LLL Algorithm: Survey and Applications, Chap. 14, pp. 453–473. Information Security and Cryptography, Prague (2010).
19. Mazo J. E., Odlyzko A. M.: Lattice points in high-dimensional spheres. Monatsh. Math. **110**, 47–61 (1990).
20. Micciancio D., Regev O.: Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. **37**, 267–302 (2007).
21. Micciancio D., Voulgaris P.: Faster Exponential Time Algorithms for the Shortest Vector Problem, pp. 1468–1480. SODA, Remsen (2010).
22. Nebe G.: An even unimodular 72-lattice with minimum 8. J. Reine Angew. Math. http://arxiv.org/abs/1008.2862.
23. Quebbemann H.-G.: A construction of integral lattices. Mathematika **31**, 137–140 (1984).
24. Tsang K.-M.: Counting lattice points in the sphere. Bull. Lond. Math. Soc. **32**, 679–688 (2000).
25. Turyn R. J.: Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. J. Comb. Theory **16**, 313–333 (1974).