



HAL
open science

On the density of cyclotomic lattices constructed from codes

Philippe Moustrou

► **To cite this version:**

Philippe Moustrou. On the density of cyclotomic lattices constructed from codes. International Journal of Number Theory, 2017, 13 (05), pp.1261-1274. 10.1142/S1793042117500695 . hal-03408766

HAL Id: hal-03408766

<https://hal.science/hal-03408766>

Submitted on 9 Apr 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ON THE DENSITY OF CYCLOTOMIC LATTICES CONSTRUCTED FROM CODES

PHILIPPE MOUSTROU

ABSTRACT. Recently, Venkatesh improved the best known lower bound for lattice sphere packings by a factor $\log \log n$ for infinitely many dimensions n . Here we prove an effective version of this result, in the sense that we exhibit, for the same set of dimensions, finite families of lattices containing a lattice reaching this bound. Our construction uses codes over cyclotomic fields, lifted to lattices via Construction A.

1. INTRODUCTION

The sphere packing problem in Euclidean spaces asks for the biggest proportion of space that can be filled by a collection of balls with disjoint interiors having the same radius. Here we focus on *lattice* sphere packings, where the centers of the balls are located at the points of a lattice, and we denote by Δ_n the supremum of the density that can be achieved by such a packing in dimension n . Let us recall that the exact value of Δ_n is known only for dimensions up to 8 [CSB87] and for dimension 24 ([CK09]). For other dimensions, only lower and upper bounds are known. Moreover, asymptotically, the ratio between these bounds is exponential.

Here we focus on lower bounds. The first important result goes back to the celebrated Minkowski-Hlawka theorem [Hla43], stating the inequality $\Delta_n \geq \frac{\zeta(n)}{2^{n-1}}$ for all n , where $\zeta(n)$ denotes the Riemann zeta function. Later, Rogers [Rog47] improved this bound by a linear factor: he showed that $\Delta_n \geq \frac{cn}{2^n}$ for every $n \geq 1$, with $c \approx 0.73$. The constant c was successively improved by Davenport and Rogers [DR47] ($c = 1.68$), Ball [Bal92] ($c = 2$) and Vance [Van11] ($c = 2.2$ when n is divisible by 4). Recently Venkatesh has obtained a more dramatic improvement [Ven13], showing that for n big enough, $\Delta_n \geq \frac{65963n}{2^n}$. Most importantly, he proves that for infinitely many dimensions n , $\Delta_n \geq \frac{n \log \log n}{2^{n+1}}$, thus improving for the first time upon the linear growth of the numerator.

Unfortunately, all these results are of existential nature: their proofs are non constructive by essence, due to the fact that they generally use random arguments over infinite families of lattices. It is then natural to ask for effective versions of these results. It is worth to explain what we mean here by effectiveness. Indeed,

Date: June 12, 2018

Keywords : Lattice sphere packings, Minkowski-Hlawka bound, cyclotomic fields, linear codes.

Mathematics Subject Classification : 11H31, 11H71.

This study has been carried out with financial support from the French State, managed by the French National Research Agency (ANR) in the frame of the "Investments for the future" Programme IdEx Bordeaux - CPU (ANR-10-IDEX-03-02).

designing a practical algorithm, i.e running in polynomial time in the dimension, to construct dense lattices appears to be out of reach to date. More modestly, one aims at exhibiting finite and explicit sets of lattices, possibly of exponential size, in which one is guaranteed to find a dense lattice.

In this direction, the first to give an effective proof of Minkowski-Hlawka theorem was Rush [Rus89]. Later, Gaborit and Zémor [GZ07] provided an effective analogue of Roger’s bound for the dimensions of the form $n = 2p$ with p a big enough prime number. In both constructions, the lattices are lifted from codes over a finite field, and run in sets of size of the form $\exp(kn \log n)$, with k a constant.

Let us now explain with more details two ingredients that play a crucial role in the proofs of the results above. The first one is *Siegel’s mean value theorem* [Sie45] which in particular states that, on average over the set \mathcal{L} of n -dimensional lattices of volume 1,

$$\mathbb{E}_{\mathcal{L}}[|B(r) \cap (\Lambda \setminus \{0\})|] = \text{Vol}(B(r)).$$

It follows that, if $\text{Vol}(B(r)) < 1$, then there exists a lattice $\Lambda \in \mathcal{L}$ such that $B(r) \cap (\Lambda \setminus \{0\}) = \emptyset$, i.e such that the minimum norm μ of its non zero vectors is greater than r . The density of the sphere packing associated to Λ then satisfies

$$\Delta(\Lambda) = \frac{\text{Vol}(B(\mu))}{2^n} > \frac{1}{2^n}.$$

It is worth to point out that the same reasoning holds if $\text{Vol}(B(r)) < 2$, because lattice vectors of given norm come by pairs $\{\pm x\}$. From this simple remark we get

$$\Delta_n > \frac{2}{2^n},$$

which is essentially Minkowski-Hlawka bound.

The second idea follows almost immediately from the previous observation: considering lattices affording a group of symmetries larger than the trivial $\{\pm \text{Id}\}$ should allow to replace the factor 2 in the numerator by a greater value. To this end, one needs a family of lattices, invariant under the action of a group, for which an analogue of Siegel’s mean value theorem holds. This idea is exploited in [GZ07], [Van11] and [Ven13]. In particular, this is how Venkatesh obtains the extra $\log \log n$ term, by considering cyclotomic lattices, i.e lattices with an additional structure of $\mathbb{Z}[\zeta_m]$ -modules. It turns out that, for a suitable choice of m , one can find such lattices in dimension $n = O(\frac{m}{\log \log m})$.

In this paper, we consider cyclotomic lattices constructed from codes, in order to deal with finite families of lattices. To be more precise, the codes we take are the preimages through the standard surjection associated to a prime ideal \mathfrak{P} of $\mathbb{Q}[\zeta_m]$

$$\mathbb{Z}[\zeta_m]^2 \rightarrow (\mathbb{Z}[\zeta_m]/\mathfrak{P})^2$$

of all one dimensional subspaces over the residue field $\mathbb{Z}[\zeta_m]/\mathfrak{P}$.

Our approach is simpler and more straightforward than the previous ones in several respects. On one hand, the analogue of Siegel’s mean value theorem in our situation boils down to a simple counting argument on finite sets (see Lemma 4). On the other hand, the group action, which is, as in [GZ07], that of a cyclic group, is in our case easier to deal with, because it is a free action. As a consequence, we can cope with arbitrary orders m , while Gaborit and Zémor only consider prime orders.

Our main theorem is an effective version of Venkatesh’s result:

Theorem 1. *For infinitely many dimensions n , a lattice Λ such that its density $\Delta(\Lambda)$ satisfies*

$$\Delta(\Lambda) \geq \frac{0.89n \log \log n}{2^n}$$

can be constructed with $\exp(1.5n \log n(1 + o(1)))$ binary operations.

This result follows from a more general analysis of the density on average of the elements in the families of m -cyclotomic lattices described above, see Theorem 2 and Proposition 1 for precise statements.

A lattice Λ is said to be *symplectic* if there exists an isometry σ exchanging Λ and its dual lattice, and such that $\sigma^2 = -\text{Id}$. Symplectic lattices are closely related to principally polarized Abelian varieties. In [Aut15], Autissier has adapted Venkatesh's approach to prove the existence of symplectic lattices with the same density. We show that, with some slight modifications, our construction leads to symplectic lattices, thus providing an effective version of Autissier's result (see Theorem 3 and Corollary 2).

The article is organized as follows: Section 2 recalls basics notions about lattices and cyclotomic fields, and introduces the construction of cyclotomic lattices from codes. In Section 3 we state and prove the main results discussed above. Section 4 is dedicated to the case of symplectic lattices.

Acknowledgements. I am most grateful to Christine Bachoc for introducing me to this problem, and for her support all along this work. I would also like to thank Arnaud Pêcher and Gilles Zémor for fruitful discussions, and Pascal Autissier for useful remarks that lead to improvements on the first version of the paper.

2. NOTATIONS AND PRELIMINARIES

2.1. Lattices in Euclidean spaces. Let E be a Euclidean space equipped with the scalar product $\langle \cdot, \cdot \rangle$. We denote by $\|\cdot\|$ the norm associated to this scalar product, by n the dimension of E , and by $B(r)$ the closed ball of radius r in E :

$$B(r) = \{x \in E, \|x\| \leq r\}.$$

By Stirling formula, we have

$$\text{Vol}(B(1)) = \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2} + 1)} \sim \frac{1}{\sqrt{n\pi}} \left(\sqrt{\frac{2\pi e}{n}} \right)^n$$

where $f \sim g$ means $\lim_{n \rightarrow \infty} f/g = 1$. Thus, if $\text{Vol}(B(r)) = V$, we get that

$$(1) \quad r \sim \sqrt{\frac{n}{2\pi e}} V^{\frac{1}{n}}.$$

A lattice $\Lambda \in E$ is a free discrete \mathbb{Z} -module of rank n (for a general reference on lattices, see e.g [CSB87]). A *fundamental region* of Λ is a region $\mathcal{R} \subset E$ such that for any $\lambda \neq \lambda' \in \Lambda$, the measure of $(\lambda + \mathcal{R}) \cap (\lambda' + \mathcal{R})$ is 0, and $E = \bigcup_{\lambda \in \Lambda} (\lambda + \mathcal{R})$.

The *volume* $\text{Vol}(\Lambda)$ of Λ is defined as the volume of any of its fundamental region. The *Voronoi region* of Λ is the particular fundamental region:

$$\mathcal{V} = \mathcal{V}_\Lambda = \{z \in E, \forall x \in \Lambda, \|z - x\| \geq \|z\|\}.$$

We denote by μ the *minimum* of Λ :

$$\mu = \mu_\Lambda = \min\{\|x\|, x \in \Lambda \setminus \{0\}\}$$

and by τ its *covering radius*:

$$\tau = \tau_\Lambda = \sup_{z \in E} \inf_{x \in \Lambda} \|z - x\|.$$

Taking balls of radius $\mu/2$ centered at the points of Λ , we get a *packing* in E , i.e a set of spheres with pairwise disjoint interiors. The *density* of this packing is given by

$$\Delta(\Lambda) = \frac{\text{Vol}(B(\mu))}{2^n \text{Vol}(\Lambda)}.$$

Finally, we define $\Lambda^\#$, the *dual lattice* of the lattice Λ :

$$\Lambda^\# = \{x \in E, \forall y \in \Lambda, \langle x, y \rangle \in \mathbb{Z}\}.$$

2.2. Cyclotomic fields. Let K be the cyclotomic field $\mathbb{Q}[\zeta_m]$, where ζ_m is a primitive m -th root of unity. This is a totally imaginary field of degree $\phi(m)$ over \mathbb{Q} . Let us define $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$. The trace form $\text{tr}(x\bar{y})$ where tr denotes the trace form of the number field K induces a scalar product on $K_\mathbb{R}$, denoted by $\langle \cdot, \cdot \rangle$, giving $K_\mathbb{R}$ the structure of a Euclidean space of dimension $\phi(m)$. We refer to [Was97] for general properties of cyclotomic fields.

For every fractional ideal \mathfrak{A} , we will use the same notation \mathfrak{A} for the lattice in $K_\mathbb{R}$ which is the image of \mathfrak{A} under the natural embedding $K \rightarrow K_\mathbb{R}$. We will need informations about lattices defined by fractional ideals of K .

The volume of \mathcal{O}_K is by definition the square root of the absolute value of the discriminant d_K of K . It is well known (e.g [Was97]) that for the cyclotomic fields

$$(2) \quad |d_K| = \frac{m^{\phi(m)}}{\prod_{\substack{l \in \mathbb{P} \\ l|m}} l^{\phi(m)/(l-1)}}$$

where \mathbb{P} is the set of prime numbers.

It is easy to see that the minimum of \mathcal{O}_K is $\sqrt{\phi(m)}$: indeed $\|1\| = \sqrt{\phi(m)}$ and the arithmetic geometric inequality gives $\|x\| \geq \sqrt{\phi(m)}$ for all $x \in \mathcal{O}_K$. For the minimum and the covering radius of general fractional ideals, we will apply the following estimates:

Lemma 1 ([Flu06], propositions 4.1 and 4.2.). *Let \mathfrak{A} be a fractional ideal of K , where K is a number field of degree n over \mathbb{Q} . Then we have :*

$$(i) \quad \frac{\mu_{\mathfrak{A}}}{\text{Vol}(\mathfrak{A})^{\frac{1}{n}}} \geq \frac{\sqrt{n}}{\sqrt{|d_K|}^{\frac{1}{n}}},$$

$$(ii) \quad \frac{\tau_{\mathfrak{A}}}{\text{Vol}(\mathfrak{A})^{\frac{1}{n}}} \leq \frac{\sqrt{n}}{2} \sqrt{|d_K|}^{\frac{1}{n}}.$$

2.3. Cyclotomic lattices constructed from codes. A standard construction of lattices lifts codes over \mathbb{F}_p to sublattices of \mathbb{Z}^n , this is the well known *Construction A* (see [CSB87, Chapter 7]). Here we will deal with a slightly more general construction in the context of cyclotomic fields.

Let us consider as before $K = \mathbb{Q}[\zeta_m]$ and $K_{\mathbb{R}}$ the Euclidean space associated with K . Let \mathfrak{P} be a prime ideal of \mathcal{O}_K lying over a prime number p which does not divide m . Then the quotient $F = \mathcal{O}_K/\mathfrak{P}$ is a finite field of cardinality $q = p^f$.

Let $E = K_{\mathbb{R}}^s$. We still denote by $\langle \cdot, \cdot \rangle$ the scalar product $\langle x, y \rangle = \sum_{i=1}^s \langle x_i, y_i \rangle$ induced on the $s\phi(m)$ -dimensional \mathbb{R} -vector space E by that of $K_{\mathbb{R}}$. Let Λ_0 be a lattice in E which is a \mathcal{O}_K -submodule of E . We consider the canonical surjection

$$\pi : \Lambda_0 \rightarrow \Lambda_0/\mathfrak{P}\Lambda_0.$$

The norm $\|\cdot\|$ on E associated with $\langle \cdot, \cdot \rangle$ induces a weight on the quotient space $\Lambda_0/\mathfrak{P}\Lambda_0$: if $c \in \Lambda_0/\mathfrak{P}\Lambda_0$,

$$wt(c) = \min\{\|z\|, \pi(z) = c\}.$$

The quotient $\Lambda_0/\mathfrak{P}\Lambda_0$ is a vector space of dimension s over the finite field F . We will call a F -subspace C of $\Lambda_0/\mathfrak{P}\Lambda_0$ a *code*. We denote by k its dimension and by d its minimal weight, with respect to the weight defined above. Finally we denote by Λ_C the lattice obtained from C

$$\Lambda_C = \pi^{-1}(C)$$

and give in the following lemma a summary of its properties:

Lemma 2. *Let C be a code of $\Lambda_0/\mathfrak{P}\Lambda_0$ of dimension k and minimal weight d . Then :*

(i) *The volume of Λ_C is*

$$\text{Vol}(\Lambda_C) = q^{s-k} \text{Vol}(\Lambda_0).$$

(ii) *The minimum of Λ_C is $\mu_{\Lambda_C} = \min\{d, \mu_{\mathfrak{P}\Lambda_0}\}$.*

(iii) *If $d \leq \mu_{\mathfrak{P}\Lambda_0}$, the packing density of Λ_C is:*

$$\Delta(\Lambda_C) = \frac{\text{Vol}(B(d))}{2^n q^{s-k} \text{Vol}(\Lambda_0)},$$

where $n = s\phi(m)$ is the dimension of E .

Proof. (i) The lattice $\pi^{-1}(C)$ contains the lattice $\mathfrak{P}\Lambda_0$ and we have:

$$|\pi^{-1}(C)/\mathfrak{P}\Lambda_0| = |C| = q^k,$$

so

$$\text{Vol}(\Lambda_C) = \frac{1}{q^k} \text{Vol}(\mathfrak{P}\Lambda_0) = q^{s-k} \text{Vol}(\Lambda_0).$$

(ii) and (iii) follow directly from the definitions. □

To conclude this subsection, we state a lemma that relates the Euclidean ball and the discrete ball $\overline{B}(r) := \{c \in \Lambda_0/\mathfrak{P}\Lambda_0, wt(c) \leq r\}$.

Lemma 3. *Assuming $r < \frac{\mu_{\mathfrak{P}\Lambda_0}}{2}$, we have:*

(i) $|\overline{B}(r)| = |\Lambda_0 \cap B(r)|$

(ii) $\text{Vol}(B(r - \tau_{\Lambda_0})) \leq |\overline{B}(r)| \text{Vol}(\Lambda_0) \leq \text{Vol}(B(r + \tau_{\Lambda_0}))$.

(iii) If $\overline{B}(r) \cap (C \setminus \{0\}) = \emptyset$, then

$$(3) \quad \Delta(\Lambda_C) > \frac{\text{Vol}(B(r))}{2^n q^{s-k} \text{Vol}(\Lambda_0)}.$$

Proof. (i) Let $c \in \Lambda_0/\mathfrak{P}\Lambda_0$ such that $wt(c) \leq r$. We want to prove that c has exactly one representative $x \in \Lambda_0$ which satisfies $\|x\| \leq r$. Indeed, if $y \in \Lambda_0$ with $y \neq x$ and $\pi(y) = \pi(x) = c$, we have $y = x + z$ with $z \in \mathfrak{P}\Lambda_0 \setminus \{0\}$. Then $\|x - y\| = \|z\| \geq \mu_{\mathfrak{P}\Lambda_0} > 2r$, a contradiction.

(ii) Let us consider

$$A = \bigcup_{x \in \Lambda_0 \cap B(r)} (x + \mathcal{V}_{\Lambda_0})$$

where \mathcal{V}_{Λ_0} is the Voronoi region of Λ_0 . The volume of A is

$$\text{Vol}(A) = |\Lambda_0 \cap B(r)| \text{Vol}(\Lambda_0) = |\overline{B}(r)| \text{Vol}(\Lambda_0)$$

so the wanted inequalities will follow from the inclusions

$$B(r - \tau_{\Lambda_0}) \subset A \subset B(r + \tau_{\Lambda_0}).$$

Let us start with the second inclusion. If $z \in x + \mathcal{V}_{\Lambda_0}$, by definition of the covering radius, we have

$$\|z - x\| \leq \tau_{\Lambda_0},$$

so if $\|x\| \leq r$, $\|z\| \leq r + \tau_{\Lambda_0}$. For the first inclusion, let y be such that $\|y\| \leq r - \tau_{\Lambda_0}$. If x denotes the closest point to y in Λ_0 , we have $y \in x + \mathcal{V}_{\Lambda_0}$ and $\|x\| \leq \|y\| + \|x - y\| \leq r$, so that $y \in A$.

(iii) It follows directly from Lemma 2. □

3. THE DENSITY OF CYCLOTOMIC LATTICES CONSTRUCTED FROM CODES

In this section, we introduce a certain family of lattices obtained from codes as described in the previous subsection, and show that for high dimensions, this family contains lattices having good density.

As before, $K = \mathbb{Q}[\zeta_m]$, $F = \mathcal{O}_K/\mathfrak{P} \simeq \mathbb{F}_q$. Let us set $s = 2$ and consider the Euclidean space $E = K_{\mathbb{R}}^2$, of dimension $2\phi(m)$, in which we fix $\Lambda_0 = \mathcal{O}_K^2$.

Definition 1. We denote by \mathcal{C} the set of the $(q+1)$ F -lines of $\Lambda_0/\mathfrak{P}\Lambda_0 = F^2$, and by $\mathcal{L}_{\mathcal{C}}$ the set of lattices of E constructed from the codes in \mathcal{C} :

$$\mathcal{L}_{\mathcal{C}} = \{\Lambda_C, C \in \mathcal{C}\}.$$

The following lemma evaluates the average of the value of $|\overline{B}(r) \cap C \setminus \{0\}|$ over the family \mathcal{C} :

Lemma 4. We have:

$$\mathbb{E}(|\overline{B}(r) \cap (C \setminus \{0\})|) < \frac{|\overline{B}(r)|}{q}.$$

Proof. It is a straightforward computation:

$$\begin{aligned}
\mathbb{E}(|\overline{B}(r) \cap (C \setminus \{0\})|) &= \frac{1}{|\mathcal{C}|} \sum_{C \in \mathcal{C}} |\overline{B}(r) \cap (C \setminus \{0\})| \\
&= \frac{1}{|\mathcal{C}|} \sum_{C \in \mathcal{C}} \sum_{\substack{c \in C \\ 0 < wt(c) \leq r}} 1 \\
&= \frac{1}{|\mathcal{C}|} \sum_{c \in \overline{B}(r) \setminus \{0\}} |\{C \in \mathcal{C}, c \in C\}|.
\end{aligned}$$

There is exactly one line passing through every non zero vector in F^2 . So

$$\mathbb{E}(|\overline{B}(r) \cap (C \setminus \{0\})|) = \frac{|\overline{B}(r) \setminus \{0\}|}{|\mathcal{C}|} < \frac{|\overline{B}(r)|}{q}.$$

□

From now on, q will vary with m , so we adopt the notation q_m instead of q . We show that the family $\mathcal{L}_{\mathcal{C}}$ of lattices contains, when m is big enough and when q_m grows in a suitable way with m , lattices having high density.

Theorem 2. *For every $1 > \varepsilon > 0$, if $\phi(m)^2 m = o(q_m^{\frac{1}{\phi(m)}})$, then for m big enough, the family of lattices $\mathcal{L}_{\mathcal{C}}$ contains a lattice $\Lambda \subset \mathbb{R}^{2\phi(m)}$ satisfying*

$$\Delta(\Lambda) > \frac{(1 - \varepsilon)m}{2^{2\phi(m)}}.$$

We start with a technical lemma.

Lemma 5. *Let $\rho_m = \sqrt{\frac{\phi(m)}{\pi e}} (q_m \text{Vol}(\Lambda_0))^{\frac{1}{2\phi(m)}}$. If $\phi(m)^2 m = o(q_m^{\frac{1}{\phi(m)}})$, then*

- (i) $\lim_{m \rightarrow \infty} \frac{\phi(m)\tau_{\Lambda_0}}{\rho_m} = 0$,
- (ii) *For m big enough, $\rho_m < \frac{\mu_{\mathfrak{A}\Lambda_0}}{2}$.*

Proof. (i) We have:

$$\frac{\phi(m)\tau_{\Lambda_0}}{\rho_m} = \frac{\sqrt{\pi e \phi(m)} \tau_{\Lambda_0}}{(q_m \text{Vol}(\Lambda_0))^{\frac{1}{2\phi(m)}}}.$$

Since $\Lambda_0 = \mathcal{O}_K \times \mathcal{O}_K$, we have $\tau_{\Lambda_0} = \sqrt{2}\tau_{\mathcal{O}_K}$ and $\text{Vol}(\Lambda_0) = \text{Vol}(\mathcal{O}_K)^2$. Then, by (ii) of Lemma 1,

$$\frac{\tau_{\mathcal{O}_K}}{\text{Vol}(\mathcal{O}_K)^{\frac{1}{\phi(m)}}} \leq \frac{\sqrt{\phi(m)}}{2} |d_K|^{\frac{1}{2\phi(m)}}.$$

Applying $|d_K| \leq m^{\phi(m)}$ (following (2)), we obtain

$$\frac{\tau_{\mathcal{O}_K}}{\text{Vol}(\mathcal{O}_K)^{\frac{1}{\phi(m)}}} \leq \frac{\sqrt{m\phi(m)}}{2}.$$

So

$$\frac{\phi(m)\tau_{\Lambda_0}}{\rho_m} \leq \sqrt{\frac{\pi e}{2}} \phi(m) \sqrt{m} q_m^{-\frac{1}{2\phi(m)}}$$

which tends to 0 when m goes to infinity, by hypothesis.

(ii) We have:

$$\begin{aligned}\rho_m &= \sqrt{\frac{\phi(m)}{\pi e}} (q_m \text{Vol}(\Lambda_0))^{\frac{1}{2\phi(m)}} \leq \frac{1}{2} \sqrt{\phi(m)} q_m^{\frac{1}{2\phi(m)}} |d_K|^{\frac{1}{2\phi(m)}} \\ &\leq \frac{1}{2} \sqrt{\phi(m)} q_m^{\frac{1}{2\phi(m)}} \sqrt{m}.\end{aligned}$$

Because $\mathfrak{P}\Lambda_0 = \mathfrak{P} \times \mathfrak{P}$, $\mu_{\mathfrak{P}\Lambda_0} = \mu_{\mathfrak{P}}$. Then, by (i) of Lemma 1, since $\text{Vol}(\mathfrak{P}) = q_m \sqrt{|d_K|}$,

$$\mu_{\mathfrak{P}} \geq q_m^{\frac{1}{\phi(m)}} \sqrt{\phi(m)}.$$

The hypothesis on q_m ensures in particular that for m big enough, we have $m < q_m^{\frac{1}{\phi(m)}}$, and thus

$$\rho_m < \frac{1}{2} \sqrt{\phi(m)} q_m^{\frac{1}{\phi(m)}} \leq \frac{\mu_{\mathfrak{P}\Lambda_0}}{2}.$$

□

Now we can prove Theorem 2.

Proof of Theorem 2. Let us fix $1 > \varepsilon > 0$. Let $r_m > 0$ be the radius such that $\text{Vol}(B_{r_m}) = (1 - \varepsilon)m q_m \text{Vol}(\Lambda_0)$. By (1), $r_m \sim \rho_m$, where ρ_m is the radius defined in Lemma 5. Applying Lemma 4, we get

$$\mathbb{E}(|\overline{B}(r_m) \cap (C \setminus \{0\})|) < \frac{|\overline{B}(r_m)|}{q_m}.$$

Because $r_m \sim \rho_m$, by (ii) of Lemma 5, $r_m < \frac{\mu_{\mathfrak{P}\Lambda_0}}{2}$, so we can apply (ii) of Lemma 3, so that

$$\begin{aligned}\mathbb{E}(|\overline{B}(r_m) \cap (C \setminus \{0\})|) &< \frac{\text{Vol}(B(r_m + \tau_{\Lambda_0}))}{q_m \text{Vol}(\Lambda_0)} = \frac{\text{Vol}(B(r_m))}{q_m \text{Vol}(\Lambda_0)} \left(1 + \frac{\tau_{\Lambda_0}}{r_m}\right)^{2\phi(m)} \\ &= (1 - \varepsilon)m \left(1 + \frac{\tau_{\Lambda_0}}{r_m}\right)^{2\phi(m)}.\end{aligned}$$

Now applying (i) of Lemma 5, we have $\lim_{m \rightarrow \infty} \left(1 + \frac{\tau_{\Lambda_0}}{r_m}\right)^{2\phi(m)} = 1$, and so, for m big enough,

$$(4) \quad \mathbb{E}(|\overline{B}(r_m) \cap (C \setminus \{0\})|) < m.$$

Now comes the crucial argument involving the action of the m -roots of unity. From (4), there is at least one code C in \mathcal{C} which satisfies $|\overline{B}(r_m) \cap (C \setminus \{0\})| < m$. Because the codes we consider are stable under the action of the m -roots of unity, which preserves the weight of the codewords, and because the length of every non zero orbit under this action is m , we can conclude that $\overline{B}(r_m) \cap (C \setminus \{0\}) = \emptyset$, and so by (iii) of Lemma 3 that,

$$\Delta(\Lambda_C) > \frac{\text{Vol}(B(r_m))}{2^{2\phi(m)} q_m \text{Vol}(\Lambda_0)} = \frac{(1 - \varepsilon)m}{2^{2\phi(m)}}.$$

□

Theorem 2 shows that for every big enough dimension of the form $n = 2\phi(m)$ our construction provides lattices having density approaching $\frac{m}{2^n}$, thus larger than $\frac{cn}{2^n}$ with $c = 1/2$. A particular sequence of dimensions leads to a better lower bound:

Corollary 1. *For infinitely many dimensions, the family \mathcal{L}_C contains a lattice $\Lambda \subset \mathbb{R}^n$ satisfying*

$$\Delta(\Lambda) \geq \frac{0.89n \log \log n}{2^n}.$$

Proof. To get the optimal gain between m and $2\phi(m)$, we take $m = \prod_{\substack{l \in \mathbb{P} \\ l \leq X}} l$, where

X is a positive real number, which tends to infinity. Thanks to Mertens' theorem [Har], we can evaluate:

$$(5) \quad \frac{m}{\phi(m)} \sim e^\gamma \log \log m.$$

where γ is the Euler-Mascheroni constant which satisfies $\gamma > 0.577$.

So we get

$$(6) \quad m \sim \phi(m) e^\gamma \log \log m \sim \frac{e^\gamma}{2} n \log \log n.$$

Let us set $\delta := 2e^{-\gamma} 0.89$. Because $\frac{e^\gamma}{2} > 0.89$, $\delta < 1$. Then by Theorem 2, we get a lattice $\Lambda \subset \mathbb{R}^n$ such that

$$\Delta(\Lambda) > \frac{\delta m}{2^n}.$$

So by (6), for m big enough,

$$\Delta(\Lambda) \geq \frac{0.89n \log \log n}{2^n}.$$

□

Finally we evaluate the complexity of constructing a lattice Λ with the desired density:

Proposition 1. *Let $n = 2\phi(m)$. For every $1 > \varepsilon > 0$, the construction of a lattice $\Lambda \subset \mathbb{R}^n$ satisfying*

$$\Delta(\Lambda) > \frac{(1 - \varepsilon)m}{2^{2\phi(m)}}$$

requires $\exp(1.5n \log n(1 + o(1)))$ binary operations.

We need to find a prime ideal \mathfrak{P} such that $q_m = |\mathcal{O}_K/\mathfrak{P}|$ satisfies the condition required in *Theorem 2*. Let us recall that $q_m = p_m^{f_m}$ where p_m is the prime number lying under \mathfrak{P} , and f_m is the order of p_m in the group $(\mathbb{Z}/m\mathbb{Z})^*$ (see [Was97]). We will restrict our attention to the case $f_m = 1$, i.e when $p_m \equiv 1 \pmod{m}$. In that case, p_m decomposes totally in $\mathbb{Q}[\zeta_m]$, and $q_m = p_m$. We use Siegel-Walfisz theorem in order to give an upper bound for the smallest such prime number:

Lemma 6. *For m big enough, there is a prime number p_m congruent to $1 \pmod{m}$ such that:*

$$\frac{1}{2}(m^3 \log m)^{\phi(m)} \leq p_m \leq (m^3 \log m)^{\phi(m)}.$$

Proof. Let us denote by $\pi(x, m, a)$ the number of primes $p < x$ such that $p = a \pmod m$. Siegel-Walfisz theorem (see [IH04]) gives that for any $A > 0$:

$$\pi(x, m, a) = \frac{Li(x)}{\phi(m)} + \mathcal{O}\left(\frac{x}{(\log x)^A}\right),$$

where the implied constant depends only on A , and $Li(x) = \int_2^x \frac{dt}{\log t}$. Applying this theorem to $x = (m^3 \log m)^{\phi(m)}$, $a = 1$, and $A = 2$ we get

$$\pi(x, m, 1) - \pi(x/2, m, 1) = \frac{1}{\phi(m)} \int_{x/2}^x \frac{dt}{\log t} + \mathcal{O}\left(\frac{x}{(\log x)^2}\right).$$

We have $\frac{1}{\phi(m)} \int_{x/2}^x \frac{dt}{\log t} > \frac{x}{2\phi(m) \log x}$, which grows faster than the error term since $\log x \sim 3\phi(m) \log(m)$, and thus ensures the existence of a prime p_m between $x/2$ and x . \square

Proof of Proposition 1. Applying Lemma 6, the complexity of finding q_m satisfying the condition of Theorem 2 is

$$\mathcal{O}(m^3 \log m)^{\phi(m)} = e^{3\phi(m) \log(m)(1+o(1))} = e^{1.5n \log(n)(1+o(1))}.$$

The corresponding family of lattices \mathcal{L}_C has $q_m + 1$ elements. By construction, each of these lattices is generated by vectors with coefficients which are polynomial in n . So, the cost of computing their density, which can be done with $2^{O(n)}$ operations, following [HPS], is negligible compared with the enumeration of the family. \square

4. SYMPLECTIC CYCLOTOMIC LATTICES

For a survey about symplectic lattices, we refer to [Ber97]. Here we briefly introduce this notion.

Let E be a Euclidean space, and Λ a lattice in E . Then an *isoduality* is an isometry σ of E such that $\sigma(\Lambda) = \Lambda^\#$. If Λ affords an isoduality, then it is called isodual. If moreover σ satisfies $\sigma^2 = -\text{Id}$, then Λ is called *symplectic*.

Now we explain how to change the lattice Λ_0 in such a way that our construction provides symplectic lattices.

Let

$$\Lambda_0 = \alpha^{-1} \mathcal{O}_K \times \alpha \mathfrak{P}^{-1} \mathcal{O}_K^\#,$$

where $\alpha = (q|d_K|)^{\frac{1}{2\phi(m)}}$. The volume of Λ_0 is now

$$(7) \quad \text{Vol}(\Lambda_0) = \text{Vol}(\mathcal{O}_K) \text{Vol}(\mathfrak{P}^{-1} \mathcal{O}_K^\#) = \frac{\text{Vol}(\mathcal{O}_K) \text{Vol}(\mathcal{O}_K^\#)}{q} = \frac{1}{q}.$$

Let us define the map

$$\sigma : \begin{array}{ccc} K_{\mathbb{R}}^2 & \rightarrow & K_{\mathbb{R}}^2 \\ (x_1, x_2) & \mapsto & (-x_2, x_1) \end{array}.$$

It is clear that σ is an isometry, and that $\sigma^2 = -\text{Id}$.

In the following lemma, we show that the lattices we defined in Definition 1 are now symplectic:

Lemma 7. *If C is a F -line of $\Lambda_0/\mathfrak{P}\Lambda_0$, then the lattice Λ_C is symplectic.*

Proof. Let us prove that $\sigma(\Lambda_C) \subset \Lambda_C^\#$. Let us take $(x_1, x_2) \in \Lambda_C$. We have to show that for every $(y_1, y_2) \in \Lambda_C$, $\langle \sigma(x_1, x_2), (y_1, y_2) \rangle \in \mathbb{Z}$, that is

$$(8) \quad \text{tr}(-x_2 y_1) + \text{tr}(x_1 y_2) \in \mathbb{Z}.$$

According to the definition of C , we have $C = F(u_1, u_2)$ with $u_1 \in \alpha^{-1}\mathcal{O}_K$ and $u_2 \in \alpha\mathfrak{P}^{-1}\mathcal{O}_K^\#$. So there exists $\lambda, \mu \in \mathcal{O}_K$ such that

$$\begin{cases} x_1 = \lambda u_1 & \text{mod } \alpha^{-1}\mathfrak{P} \\ x_2 = \lambda u_2 & \text{mod } \alpha\mathcal{O}_K^\# \end{cases} \quad \text{and} \quad \begin{cases} y_1 = \mu u_1 & \text{mod } \alpha^{-1}\mathfrak{P} \\ y_2 = \mu u_2 & \text{mod } \alpha\mathcal{O}_K^\# \end{cases}.$$

This implies that

$$\text{tr}(x_1 y_2) = \text{tr}(\lambda \mu u_1 u_2) \pmod{\mathbb{Z}}$$

and

$$\text{tr}(x_2 y_1) = \text{tr}(\lambda \mu u_1 u_2) \pmod{\mathbb{Z}},$$

so that (8) is satisfied.

To conclude the proof it is enough to notice that $\text{Vol}(\Lambda_C) = q \text{Vol}(\Lambda_0) = 1$, which implies $\sigma(\Lambda_C) = \Lambda_C^\#$. \square

We again consider the set \mathcal{C} of lines of $\Lambda_0/\mathfrak{P}\Lambda_0$. It is clear that the result of Lemma 4 remains valid for this new family of codes. The general strategy underlying the proof of Theorem 2 applies to the family of lattices associated to these codes, so that we get analogues in this context :

Theorem 3. *For every $1 > \varepsilon > 0$, if $\phi(m)^2 m = o(q_m^{\frac{1}{\phi(m)}})$, then for m big enough, the family of **symplectic** lattices \mathcal{L}_C contains a lattice $\Lambda \subset \mathbb{R}^{2\phi(m)}$ satisfying*

$$\Delta(\Lambda) > \frac{(1 - \varepsilon)m}{2^{2\phi(m)}}.$$

Corollary 2. *For infinitely many dimensions, the family \mathcal{L}_C contains a **symplectic** lattice $\Lambda \subset \mathbb{R}^n$ satisfying*

$$\Delta(\Lambda) \geq \frac{0.89n \log \log n}{2^n}.$$

The proofs of Theorem 3 and Corollary 2 are similar to those of Theorem 2 and Corollary 1. However, we need to prove that Lemma 5 still holds, even if we changed Λ_0 :

Lemma 8. *Let $\rho_m = \sqrt{\frac{\phi(m)}{\pi e}} (q_m \text{Vol}(\Lambda_0))^{\frac{1}{2\phi(m)}} = \sqrt{\frac{\phi(m)}{\pi e}}$.*

If $\phi(m)^2 m = o(q_m^{\frac{1}{\phi(m)}})$, then

- (i) $\lim_{m \rightarrow \infty} \frac{\phi(m)\tau_{\Lambda_0}}{\rho_m} = 0$,
- (ii) *For m big enough, $\rho_m < \frac{\mu_{\mathfrak{P}\Lambda_0}}{2}$.*

Proof. (i) We have:

$$\frac{\phi(m)\tau_{\Lambda_0}}{\rho_m} = \sqrt{\pi e \phi(m)} \tau_{\Lambda_0}.$$

Let us set $\mathfrak{A}_1 = \alpha^{-1}\mathcal{O}_K$ and $\mathfrak{A}_2 = \alpha\mathfrak{P}^{-1}\mathcal{O}_K^\#$. Then $\Lambda_0 = \mathfrak{A}_1 \times \mathfrak{A}_2$ and the covering radius of Λ_0 is $\tau_{\Lambda_0} = \sqrt{\tau_{\mathfrak{A}_1}^2 + \tau_{\mathfrak{A}_2}^2}$. So we have to bound both

covering radii $\tau_{\mathfrak{A}_1}$ and $\tau_{\mathfrak{A}_2}$. Applying (ii) of Lemma 1, and because $\text{Vol}(\mathfrak{A}_1) = \text{Vol}(\mathfrak{A}_2) = \frac{1}{\sqrt{q}}$, we have, for $i \in \{1, 2\}$,

$$\tau_{\mathfrak{A}_i} \leq \frac{\sqrt{\phi(m)}}{2} |d_K|^{\frac{1}{2\phi(m)}} q^{-\frac{1}{2\phi(m)}} \leq \frac{\sqrt{m\phi(m)} q^{-\frac{1}{2\phi(m)}}}{2}.$$

So

$$\tau_{\Lambda_0} \leq \sqrt{2} \max\{\tau_{\mathfrak{A}_1}, \tau_{\mathfrak{A}_2}\} \leq \sqrt{m\phi(m)} q^{-\frac{1}{2\phi(m)}}$$

and finally

$$\frac{\phi(m)\tau_{\Lambda_0}}{\rho_m} \leq \sqrt{\pi e} \phi(m) \sqrt{m} q_m^{-\frac{1}{2\phi(m)}}$$

which tends to 0 when m goes to infinity, by hypothesis.

- (ii) Let us set $\mathfrak{B}_1 = \alpha^{-1}\mathfrak{P}$ and $\mathfrak{B}_2 = \alpha \mathcal{O}_K^\#$. Then $\mathfrak{P}\Lambda_0 = \mathfrak{B}_1 \times \mathfrak{B}_2$, and clearly $\mu_{\mathfrak{P}\Lambda_0} = \min\{\mu_{\mathfrak{B}_1}, \mu_{\mathfrak{B}_2}\}$. Then, applying (i) of Lemma 1, since $\text{Vol}(\mathfrak{B}_1) = \text{Vol}(\mathfrak{B}_2) = \sqrt{q}$, we have, for $i \in \{1, 2\}$,

$$\mu_{\mathfrak{B}_i} \geq \frac{\sqrt{\phi(m)} q^{\frac{1}{2\phi(m)}}}{|d_K|^{\frac{1}{2\phi(m)}}} \geq \frac{\sqrt{\phi(m)} q^{\frac{1}{2\phi(m)}}}{\sqrt{m}}.$$

So

$$\mu_{\mathfrak{P}\Lambda_0} \geq \frac{\sqrt{\phi(m)} q^{\frac{1}{2\phi(m)}}}{\sqrt{m}}.$$

The hypothesis on q_m ensures in particular that for m big enough, m satisfies $\sqrt{m} < q_m^{\frac{1}{2\phi(m)}}$, and thus

$$\rho_m = \sqrt{\frac{\phi(m)}{\pi e}} < \frac{1}{2} \frac{\sqrt{\phi(m)} q^{\frac{1}{2\phi(m)}}}{m} \leq \frac{\mu_{\mathfrak{P}\Lambda_0}}{2}.$$

□

As the condition on the growth of q_m does not change, the estimation for the complexity of construction in this context is the same:

Proposition 2. *Let $n = 2\phi(m)$. For every $1 > \varepsilon > 0$, the construction of a **symplectic** lattice $\Lambda \subset \mathbb{R}^n$ satisfying*

$$\Delta(\Lambda) > \frac{(1 - \varepsilon)m}{2^{2\phi(m)}}$$

requires $\exp(1.5n \log n(1 + o(1)))$ binary operations.

REFERENCES

- [Aut15] Pascal Autissier. Variétés abéliennes et théorème de Minkowski-Hlawka. *Manuscripta Mathematica*, 2015.
- [Bal92] Keith Ball. A lower bound for the optimal density of lattice packings. *Internat. Math. Res. Notices*, (10):217–221, 1992.
- [Ber97] Anne-Marie Bergé. Symplectic lattices. *Contemporary Math.*, 272:9–22, 1997.
- [CK09] Henry Cohn and Abhinav Kumar. Optimality and uniqueness of the Leech lattice among lattices. *Ann. of Math. (2)*, 170(3):1003–1050, 2009.
- [CSB87] J. H. Conway, N. J. A. Sloane, and E. Bannai. *Sphere-packings, Lattices, and Groups*. Springer-Verlag New York, Inc., New York, NY, USA, 1987.

- [DR47] H. Davenport and C. A. Rogers. Hlawka's theorem in the geometry of numbers. *Duke Math. J.*, 14:367–375, 1947.
- [Flu06] Eva Bayer Fluckiger. Upper bounds for euclidean minima of algebraic number fields. *Journal of Number Theory*, 121(2):305 – 323, 2006.
- [GZ07] Philippe Gaborit and Gilles Zémor. On the construction of dense lattices with a given automorphisms group. *Ann. Inst. Fourier (Grenoble)*, 57(4):1051–1062, 2007.
- [Har] G. H. Hardy. Note on a Theorem of Mertens. *J. London Math. Soc.*, S1-2(2):70.
- [Hla43] Edmund Hlawka. Zur Geometrie der Zahlen. *Math. Z.*, 49:285–312, 1943.
- [HPS] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Algorithms for the shortest and closest lattice vector problems. In *In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, IWCC, volume 6639 of Lecture Notes in Computer Science*, pages 159–190. Springer.
- [IH04] Kowalski E. Iwaniec H. *Analytic number theory*. 2004.
- [Rog47] C. A. Rogers. Existence theorems in the geometry of numbers. *Ann. of Math. (2)*, 48:994–1002, 1947.
- [Rus89] J. A. Rush. A lower bound on packing density. *Invent. Math.*, 98(3):499–509, 1989.
- [Sie45] Carl Ludwig Siegel. A mean value theorem in geometry of numbers. *Ann. of Math. (2)*, 46:340–347, 1945.
- [Van11] Stephanie Vance. Improved sphere packing lower bounds from Hurwitz lattices. *Adv. Math.*, 227(5):2144–2156, 2011.
- [Ven13] Akshay Venkatesh. A note on sphere packings in high dimension. *Int. Math. Res. Not. IMRN*, (7):1628–1642, 2013.
- [Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

INSTITUT DE MATHÉMATIQUES DE BORDEAUX, UMR 5251, UNIVERSITÉ DE BORDEAUX, 351
COURS DE LA LIBÉRATION, 33400 TALENCE, FRANCE.

E-mail address: philippe.moustrou@u-bordeaux.fr