Dense packings via lifts of codes to division rings

Nihar Gargava and Vlad Serban

École Polytechnique Fédérale de Lausanne,
Ecublens, District de l'Ouest lausannois, Vaud, 1015, Switzerland
nihar.gargava@epfl.ch, vlad.serban@epfl.ch

Abstract. We obtain algorithmically effective versions of the dense lattice sphere packings constructed from orders in $\mathbb{Q}$-division rings by the first author. The lattices in question are lifts of suitable codes from prime characteristic to orders $\mathcal{O}$ in $\mathbb{Q}$-division rings and we prove a Minkowski–Hlawka type result for such lifts. Exploiting the additional symmetries under finite subgroups of units in $\mathcal{O}$, we show that this leads to effective constructions of lattices approaching the best known lower bounds on the packing density Δ_n in a variety of new dimensions n. This unifies and extends a number of previous constructions.

Keywords: Sphere packing problem · Codes · Division rings · Lattices · Effective results.

1 Introduction

The sphere packing problem in $\mathbb{R}^n$ is concerned with maximizing the proportion of Euclidean space covered by a set of balls of equal radius and disjoint interiors. We will mostly be concerned with the *lattice* sphere packing problem, where the balls are required to be centered at points on an n-dimensional lattice Λ. The proportion achieved by a particular lattice, called the packing density of Λ, is then given by

$$\Delta(\Lambda) := \frac{\mathrm{Vol}(\mathbb{B}_n(\lambda_1(\Lambda)))}{2^n \mathrm{Vol}(\Lambda)},$$

where $\lambda_1(\Lambda)$ denotes the shortest vector length in Λ, $\mathbb{B}_n(r)$ the ball of radius r and $\mathrm{Vol}(\Lambda)$ denotes the covolume of the lattice. We also denote by Δ_n the supremum of lattice packing densities that can be achieved in n dimensions. Its value is only known in a handful of dimensions, see for instance the summary [9, 1.5.] as well as [7]. The density is achieved by highly symmetric lattices such as root lattices or the Leech lattice. Owing to highly celebrated results [14,29,8], some of these are even known to solve the general sphere packing problem. For arbitrary dimensions, the best known upper and lower bounds on Δ_n are however exponentially far apart as n increases (see e.g., the survey article [6] for more background). In this article we shall be concerned with lower bounds as n increases and with giving effective constructions of lattices approaching these bounds.

The classical Minkowski–Hlawka theorem [15] states that $\Delta_n \geq 2\frac{\zeta(n)}{2^n}$, a bound which Rogers [21] later improved by a linear factor to $\Delta_n \geq \frac{cn}{2^n}$ for $c = 2/e \approx 0.74$. The constant was subsequently sharpened to $c = 1.68$ by Davenport-Rogers [10] and $c = 2$ by Ball [2] for all n. More recently, Vance [26] showed using lattices which are modules over the Hurwitz integers that one may take $c = 24/e \approx 8.83$ and Venkatesh [28] showed that for n large enough one may take $c = 65963$. Moreover, by considering lattices from maximal orders in cyclotomic fields, Venkatesh was able to achieve for infinitely many dimensions the improvement $\Delta_n \geq \frac{n \log \log n}{2^{n+1}}$. The first author [13] then extended such results to lattices coming from orders $\mathcal{O}$ in arbitrary $\mathbb{Q}$-division algebras. This was achieved by proving a Siegel mean value theorem (see [24,13]) in this setting and exploiting the additional symmetries of the lattices under the group of finite order units in $\mathcal{O}^\times$ to obtain dense packings. In particular, new sequences of dimensions such that $\Delta_n \geq \frac{c_1 \cdot n \log \log(n)^{c_2}}{2^n}$ for constant $c_1, c_2 > 0$ are uncovered. In this paper, we make these purely existential results for $\mathbb{Q}$-division algebras effective by exhibiting finite sets of lattices which for large enough dimension must contain a lattice approaching the non-constructive lower bound.

Indeed, for orders $\mathcal{O}$ in a $\mathbb{Q}$-division algebra, we consider for suitable primes p and for $t \geq 2$ the reduction map $\phi_p : \mathcal{O}^t \to (\mathcal{O}/p\mathcal{O})^t$ and may identify the quotient with a product of matrix rings over a finite field $\mathbb{F}_q$. The sets of lattices $\mathbb{L}_p$ we consider are then re-scaled pre-images via ϕ_p of codes in $(\mathcal{O}/p\mathcal{O})^t$ of a certain fixed $\mathbb{F}_q$-dimension. We refer the reader to Section 3 for detailed statements, whereas some useful preliminary results on lattices from division algebras are established in Section 2.

We then exploit in Section 4 the extra symmetries of these lattices under finite subgroups of $\mathcal{O}^\times$ to obtain:

Theorem 1. *Let A be a central simple division algebra over a number field K with ring of integers $\mathcal{O}_K$. Let $\mathcal{O}$ be an $\mathcal{O}_K$-order in A. Let $n^2 = [A : K]$, $m = [K : \mathbb{Q}]$ and let $t \geq 2$ be a positive integer. Let G_0 be a fixed finite subgroup of $\mathcal{O}^\times$. Then there exists a lattice Λ in dimension n^2mt achieving*

$$\Delta(\Lambda) \geq \frac{|G_0| \cdot t}{2^{mn^2t} \cdot e(1 - e^{-t})}.$$

Moreover, there exists for any $\varepsilon > 0$ an $\mathcal{O}$-lattice Λ_ε in dimension n^2mt of packing density

$$\Delta(\Lambda_\varepsilon) \geq (1 - \varepsilon) \cdot \frac{|G_0| \cdot t}{2^{mn^2t} \cdot e(1 - e^{-t})}$$

which can be constructed effectively. Indeed, Λ_ε is obtained by applying Proposition 6 to a suitable sublattice of $\mathcal{O}^t$ obtained as a pre-image via reduction modulo primes $\mathfrak{p}$ of $\mathcal{O}_K$ of large enough norm of a code. The code in question is isomorphic to k copies of simple left $\mathcal{O}/\mathfrak{p}\mathcal{O}$-modules for some $nt - t < k < nt$.

Note that Proposition 6 mentioned in the theorem is a version of a lemma of Minkowski extended to the division algebra setting. The theorem above is derived from Theorem 5 by mimicking an approach of Rogers [21], later used by Vance [26] and Campello [5].

In order to obtain the densest packings asymptotically, one therefore seeks families of orders $\mathcal{O}$ with large finite unit groups $G_0 \subset \mathcal{O}^*$. Building on Amitsur's classification [1] and following [13], we give examples of such families. For instance, one may consider quaternion algebras over cyclotomic fields and hope to combine the improvements over the Minkowski-Hlawka bounds obtained by Vance and Venkatesh. However, in this particular case, even if the lower bound obtained exceeds $n \log\log n \cdot 2^{-(n+1)}$ in less than astronomical dimensions, due to a parity condition on the dimension the asymptotic growth is smaller (see also [13, Fig. 1]).

In particular, we obtain in Proposition 2:

Proposition 2. *Let $m_k = \prod_{\substack{p \leq k \text{ prime} \\ 2 \nmid \mathrm{ord}_2 p}} p$ and set $n_k := 8\varphi(m_k)$. Then for any $\varepsilon > 0$ there is an effective constant c_ε such that for $k > c_\varepsilon$ a lattice Λ in dimension n_k with density*

$$\Delta(\Lambda) \geq (1 - \varepsilon)\frac{24 \cdot m_k}{2^{n_k}}$$

can be constructed in $e^{4.5 \cdot n_k \log(n_k)(1+o(1))}$ binary operations. This construction leads to the asymptotic density of $\Delta(\Lambda) \geq (1 - e^{-n_k})\frac{3 \cdot n_k (\log\log n_k)^{7/24}}{2^{n_k}}$.

We ought to stress that such effective lower bounds on the density are not the first of their kind but that there is a rather rich history of such results. Rush [23], building on work with Sloane [22], recovered the Minkowski-Hlawka bound via coding-theoretic results such as the Varshamov-Gilbert bound and by lifting codes via the Leech-Sloane Construction A (see [9, Chapter 5]). The connection between random coding and such averaging results was further explicited by Loeliger [16]. This leads to families of approximate size $e^{n^2 \log n}$ in which to search for lattices achieving the Minkowski-Hlawka bound. Gaborit and Zémor [12] exploited additional structures to reduce the family size to $e^{n \log n}$. Finally, Moustrou [19] used a similar approach for cyclotomic lattices to obtain an effective version of Venkatesh's result. This approach was further formalized by Campello

[5], where an example of such results for quaternion algebras is also mentioned. Our work thus owes a lot to these existing constructions. In particular, our approach is chiefly based on Moustrou's and Campello's work [19,5] and simply extends the scope of their results to division algebras, allowing symmetries from arbitrarily large non-commutative finite groups. We also note that the utility of codes from division rings is well-studied, see for example [4], [11], [27].

We hope, then, that this article provides a useful addition to both the mathematical and coding-theoretic literature. The effective results we arrive at in Section 5 typically have a complexity of $e^{C\cdot n\log n(1+o(1))}$, which is similar to [19, Theorem 1]. However, effective version of Vance's result (see Corollary 1) has complexity $e^{1/4\cdot n^2\log n(1+o(1))}$ and it should be similar for other constructions obtained by increasing the $\mathcal{O}$-rank of the lattices.

The large running times correspond to the times taken in running an exhaustive search through all the finite candidates of lattices and it would be interesting to examine if one can further reduce the complexity of this search. It should be remarked that the approach mentioned in this research can still be used to quickly generate one of these random lattices in high dimensions that have prescribed symmetries and large minimal vectors on average.

We conclude by remarking that the mean value results for lattice sums in $\mathbb{L}_p$ for $p\to\infty$ as in Theorem 5 prompt the question of whether the points in the moduli space of $\mathcal{O}$-lattices of fixed dimension corresponding to $\Lambda\in\mathbb{L}_p$ become equidistributed in the limit in p. This leads to an interesting number-theoretic question emanating from coding theory that the authors hope to pursue in their future work.

2 Preliminaries on division rings

In this section, we recall some definitions and results on central simple algebras and in particular division rings. The primary reference is Reiner's book [20]. Let $\mathcal{O}_K$ denote a Dedekind ring with quotient field K and let A denote a separable K-algebra.

Definition 1. *An $\mathcal{O}_K$-order in A is a subring $\mathcal{O}$ of A having the same identity element and such that $\mathcal{O}$ is a* full *$\mathcal{O}_K$-lattice in K, i.e. $\mathcal{O}$ is a finitely generated $\mathcal{O}_K$-submodule of A such that $K\cdot\mathcal{O}=A$.*

A prime ideal of $\mathcal{O}$ is a proper two-sided ideal $\mathfrak{p}$ in $\mathcal{O}$ such that $K\cdot\mathfrak{p}=A$ and such that for every pair of two sided ideals S,T in Λ, we have that $S\cdot T\subset\mathfrak{p}$ implies $S\subset\mathfrak{p}$ or $T\subset\mathfrak{p}$.

For a prime p of $\mathcal{O}_K$ we shall denote by $\mathcal{O}_p, A_p$ the localizations at p of the $\mathcal{O}_K$-order $\mathcal{O}$ and of A and by $\hat{\mathcal{O}}_p, \hat{A}_p$ the respective completions. Finally let $\mathrm{rad}(R)$ denote the Jacobson radical of a ring R. Then we have (see [20, Thm 22.3,22.4]) the characterization:

Theorem 3. *The prime ideals of an $\mathcal{O}_K$-order $\mathcal{O}$ coincide with the maximal two-sided ideals of $\mathcal{O}$. If $\mathfrak{p}$ is a prime ideal of Λ, then $p=\mathfrak{p}\cap\mathcal{O}_K$ is a non-zero prime of $\mathcal{O}_K$, and $\overline{\mathcal{O}}:=\mathcal{O}/\mathfrak{p}$ is a finite dimensional simple algebra over the residue field $\mathcal{O}_K/p$. Moreover, when A is a central simple K-algebra, there is a bijection $\mathfrak{p}\leftrightarrow p$ between the set of primes of $\mathcal{O}$ and of $\mathcal{O}_K$, given by*

$$p=R\cap\mathfrak{p}\ \textit{and}\ \mathfrak{p}=\mathcal{O}\cap\mathrm{rad}(\mathcal{O}_p).$$

We now summarize the behavior of $\mathcal{O}$ and A under localization as well as the splitting behavior for central simple algebras:

Theorem 4. *Let $\mathcal{O}$ be a maximal order in a central simple K-algebra A. Let p denote a prime of $\mathcal{O}_K$. Then the completion $\hat{A}_p$ is a central simple $\hat{K}_p$-algebra and $\hat{\mathcal{O}}_p$ is a maximal order. Moreover:*

1. *For almost every prime p of $\mathcal{O}_K$, we have that*

$$\hat{A}_p\cong M_n(\hat{K}_p), \tag{2.1}$$

*with $n^2=[A:K]$ (*split *or* unramified *case). Moreover p is split if and only if the corresponding prime ideal $\mathfrak{p}$ of $\mathcal{O}$ as in Theorem 3 is just $p\mathcal{O}$.*

2. *The order $\Lambda = M_n(\hat{\mathcal{O}}_p)$ is a maximal $\hat{\mathcal{O}}_{K_p}$-order in $M_n(\hat{K}_p)$ having a unique maximal two-sided ideal $\pi_{\hat{K}_p}\Lambda$, where $\pi_{\hat{K}_p}$ is a prime element of the discrete valuation ring $\hat{\mathcal{O}}_{K_p}$. The powers*
$$(\pi_{\hat{K}_p}\Lambda)^n = \pi_{\hat{K}_p}^n \cdot \Lambda \text{ for } n = 0, 1, 2, \dots$$
exhaust all the non-zero two-sided ideals of Λ and any maximal $\hat{\mathcal{O}}_{K_p}$-order is of the form $u\Lambda u^{-1}$ for $u \in \mathrm{GL}_n(\hat{K}_p)$.
3. *For all but finitely many primes p of $\mathcal{O}_K$, the quotient $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is isomorphic to $M_n(\mathbb{F}_q)$, where $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_q$.*

Proof. These are well-known results, see e.g. [20, Theorems 17.3, 32.1].

In what follows, we will thus use the same notation $\mathfrak{p}$ for the primes of $\mathcal{O}_K$ and the corresponding prime in $\mathcal{O}$ in the split case.

2.1 Lattices from orders

The central simple algebras A are equipped with natural embeddings $A \hookrightarrow A \otimes_{\mathbb{Q}} \mathbb{R}$. An $\mathcal{O}_K$-order then embeds as a lattice into this space.

Lemma 1. *Any semisimple $\mathbb{R}$-algebra A admits an involution $(\ )^* : A \to A$ such that the following conditions are satisfied.*

- *For any $a, b \in A$, we have $(ab)^* = b^*a^*$.*
- *The trace yields a positive definite quadratic form $a \mapsto \mathrm{T}(a^*a)$ on A, meaning that $\mathrm{T}(a^*a)$ is always non-negative and is zero only when $a = 0$. Moreover, this quadratic form induces the inner product $\langle x, y\rangle = \mathrm{T}(x^*y)$ on A.*

In particular, when A is a division algebra over $\mathbb{Q}$, such an involution exists on $A \otimes_{\mathbb{Q}} \mathbb{R}$.

Proof. See e.g. [13, Corollary 35]

We will denote $A \otimes_{\mathbb{Q}} \mathbb{R}$ by $A_{\mathbb{R}}$. Involutions with the properties as described in Lemma 1 will henceforth be called “positive involutions”. An element $a \in A_{\mathbb{R}}$ such that $a^* = a$ and $x \mapsto \mathrm{T}(x^*ax)$ is a positive definite real quadratic form on $A_{\mathbb{R}}$ is called symmetric and positive definite.

For lattice constructions, we will be considering $t \geq 2$ copies of orders $\mathcal{O}$ in division algebras A with center a number field K and our lattices will be $\mathcal{O}^t \subseteq A^t \hookrightarrow (A_{\mathbb{R}})^t$. We will endow the space $A_{\mathbb{R}}^t$ with the norm induced by the following quadratic form:
$$(x_1, x_2, \dots, x_t) \mapsto \sum_{i=1}^{t} \mathrm{T}(x_i^* a x_i),$$
where $(-)^*$ is a positive involution as defined above and $a \in A_{\mathbb{R}}$ is a symmetric positive definite element to be fixed later.

2.2 Norm-trace inequality

Recall that for a finite dimensional algebra A over any field k we have norm and trace functions $N_{A/k}, T_{A/k} : A \to k$ given by the determinant and trace of the left multiplication maps respectively. It will be useful to establish some of their properties; for instance we later use the norm-trace inequality to give lower bounds on the Euclidean norm of certain lattice points via Lemma 5.

Lemma 2. *Consider a finite dimensional semisimple $\mathbb{R}$-algebra $A_{\mathbb{R}}$ together with a positive involution $(\ )^*$. Let $a \in A_{\mathbb{R}}$ be a symmetric positive definite element and let $d = \dim_{\mathbb{R}} A_{\mathbb{R}}$. Then $\mathrm{N}(a) > 0$, $\mathrm{T}(a) > 0$ and $\frac{1}{d}\mathrm{T}(a) \geq \mathrm{N}(a)^{\frac{1}{d}}$.*

Hence for $a \in A_{\mathbb{R}}$ symmetric positive definite, we get
$$\frac{1}{d}\mathrm{T}(x^*ax) \geq \mathrm{N}(x)^{\frac{2}{d}}\,\mathrm{N}(a)^{\frac{1}{d}}. \tag{2.2}$$

Proof. See [13, Lemma 40].

The following definition and ensuing lemma can also be found in [20, 9.13-14].

Definition 2. *Suppose A is a central simple L-algebra and $K \subseteq L$ is a subfield such that $[L : K] < \infty$. Then for each $a \in A$, we define the "relative reduced trace" $\mathrm{tr}_{A/K} : A \to K$ and "relative reduced norm" $\mathrm{nr}_{A/K} : A \to K$ as*

$$\mathrm{tr}_{A/K} = \mathrm{T}_{L/K} \circ \mathrm{tr}_{A/L}, \ \mathrm{nr}_{A/K} = \mathrm{N}_{L/K} \circ \mathrm{nr}_{A/L}\,.$$

Lemma 3. *When $[L : K] < \infty$ for any $a \in A$:*

$$\mathrm{T}_{A/K}(a) = \sqrt{[A:L]}\,\mathrm{tr}_{A/K}, \ \mathrm{N}_{A/K}(a) = \mathrm{nr}_{A/K}(a)^{\sqrt{[A:L]}}.$$

We may now establish the following lemmas:

Lemma 4. *Let A be a division algebra over $\mathbb{Q}$ whose center is K and $[A : K] = n^2$. Let $\mathcal{O} \subseteq A$ be a maximal order in the division algebra. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ for which A splits and let $\mathbb{F}_q = \mathcal{O}_K/\mathfrak{p}$ denote the residue field. Then the following diagram commutes:*

$$\begin{tikzcd}
\mathcal{O} \arrow[r, "\mathrm{nr}_{A/K}"] \arrow[d, "\phi_p"] & \mathcal{O}_K \arrow[d, "\pi_{\mathfrak{p}}"] \\
\mathcal{O}/\mathfrak{p}\mathcal{O} \cong M_n(\mathbb{F}_q) \arrow[r, "\det"] & \mathbb{F}_q,
\end{tikzcd}$$

where the vertical maps designate reduction modulo $\mathfrak{p}$.

Proof. Follows (not so easily) from [20, Theorem 17.3].

Lemma 5. *With the same setting, let $(\ )^* : A_{\mathbb{R}} \to A_{\mathbb{R}}$ be a positive involution. If $x \in \mathcal{O} \setminus \{0\}$ (which we may identify with its image in $A_{\mathbb{R}}$) is such that $\phi_p(x)$ is a non-invertible matrix, then*

$$\|x\| \geq \left(\sqrt{[A:\mathbb{Q}]}\,\mathrm{N}(a)^{\frac{1}{2[A:\mathbb{Q}]}}\right) q^{\frac{1}{\sqrt{[A:K]}[K:\mathbb{Q}]}}. \tag{2.3}$$

where $a \in A_{\mathbb{R}}$ is symmetric positive definite and $\|x\|^2 := \mathrm{T}(x^*ax)$ on $A_{\mathbb{R}}$.

Proof. We get by Lemma 4 that $\mathfrak{p} \mid \mathrm{nr}_{A/K}(x)$ and hence

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) \mid \mathrm{N}_{K/\mathbb{Q}} \circ \mathrm{nr}_{A/K}(x) \quad \Rightarrow \quad N_{K/\mathbb{Q}}(\mathfrak{p}) \mid \mathrm{nr}_{A/\mathbb{Q}}(x) \quad \Rightarrow \quad N_{K/\mathbb{Q}}(\mathfrak{p})^{\sqrt{[A:K]}} \mid \mathrm{N}_{A/\mathbb{Q}}(x).$$

The claim then follows From Lemma 2.

Lemma 6. *Let A be a central simple division K-algebra for K a number field and let $\mathcal{O}$ be a maximal $\mathcal{O}_K$-order which we identify with the corresponding lattice in $A_{\mathbb{R}} = A \otimes_{\mathbb{Q}} \mathbb{R}$. Then, with respect to any quadratic form $q_a(x) = \mathrm{T}(x^*ax)$ for a symmetric positive definite element $a \in A_{\mathbb{R}}$, one may define the shortest vector length λ_{1,q_a}, Hermite parameter γ_{q_a} and covering radius τ_{q_a}, and they are subject to the following:*

1. *The shortest vector length satisfies $\lambda_{1,q_a}(\mathcal{O}) \geq \sqrt{[A:\mathbb{Q}]} \cdot \mathrm{N}(a)^{1/(2[A:\mathbb{Q}])}$.*
2. *For any two-sided $\mathcal{O}$-ideal I (by which we mean a full $\mathcal{O}_K$-lattice in $\mathcal{O}$), the Hermite parameter satisfies*
$$\gamma_{q_a}(I) \geq \frac{[A:\mathbb{Q}]}{d(\mathcal{O}/\mathbb{Z})^{1/[A:\mathbb{Q}]}}$$
3. *The covering radius satisfies*
$$\tau_{q_a}(\mathcal{O}) \leq d(\mathcal{O}/\mathbb{Z})^{1/[A:\mathbb{Q}]} \cdot \left(\frac{\sqrt{[A:\mathbb{Q}]}}{2\pi} + \frac{3}{\pi}\right) \cdot \mathrm{N}(a)^{-1/(2[A:\mathbb{Q}])},$$

where $d(\mathcal{O}/\mathbb{Z})$ denotes the discriminant of $\mathcal{O}$ computed with respect to a $\mathbb{Z}$-basis.

Proof. Proof can be generalized from [3, Section 4].

3 An averaging result for lifts

As before, let A denote a central simple K-algebra for K a number field and assume A is a division ring. We set $n^2 = [A : K]$ and $m = [K : \mathbb{Q}]$. Let $\mathcal{O}$ denote an order in A.

Lemma 7. *Let k be a finite field. Let R be a f.d. semisimple k-algebra and V be a simple (left) R-module of finite dimension over k. Fix integers $n_1 \leq n_2 \leq n_3$. Consider $V^{\oplus n_3}$ as an R-module and consider the sets*

$$U = \{v \in V^{\oplus n_3} \mid Rv \simeq V^{\oplus n_1}\}, \quad \mathcal{C}_{n_2,n_3} \quad = \{C \subseteq V^{\oplus n_3} \mid C \text{ is an } R\text{-submodule}, C \simeq V^{\oplus n_2}\}.$$

Assuming that U is non-empty, then the number $|\{C \in \mathcal{C}_{n_2,n_3} \mid u \in C\}|$ is independent of u.

Proof. For each $u \in U$, $C \mapsto C/Ru$ is a bijection from $\{C \in \mathcal{C}_{n_2,n_3} \mid u \in C\}$ to $\mathcal{C}_{n_2-n_1,n_3-n_1}$.

Finally, we define following [5, Def 2]:

Definition 3. *A function $f : \mathbb{R}^d \to \mathbb{R}$ is called semi-admissible if f is Riemann-integrable and there exist positive constants $b, \delta > 0$ such that*

$$|f(\mathbf{x})| \leq \frac{b}{(1 + \|\mathbf{x}\|)^{d+\delta}} \text{ for all } \mathbf{x} \in \mathbb{R}^d.$$

Theorem 5. *For an integer $t \geq 2$ we consider an infinite family of surjective reduction maps $\phi_p : \mathcal{O}^t \to M_n(\mathbb{F}_q)^t$ as given in each coordinate by Lemma 4. Let $f : \mathbb{R}^{n^2mt} \to \mathbb{R}$ be a semi-admissible function. For a fixed $n \leq k < nt$, set*

$$\mathbb{L}_{k,p} = \{\beta_p \phi_p^{-1}(C) \mid C \in \mathcal{C}_{k,p}\}, \quad \mathcal{C}_{k,p} \quad = \{C \subseteq M_n(\mathbb{F}_q)^{\oplus t} \mid C \text{ is a } M_n(\mathbb{F}_q)\text{-submodule } \simeq (\mathbb{F}_q^n)^{\oplus k}\}.$$

where the constant β_p normalizing the covolume of lattices in $\mathbb{L}_{k,p}$ to $V := \operatorname{Vol}(\mathcal{O}^t)$ is given by $\beta_p = q^{\frac{nk-n^2t}{n^2mt}}$. Then if $(n-1)t < k < nt$, we have that

$$\lim_{p\to\infty} \mathbb{E}_{\mathbb{L}_{k,p}} \left(\sum_{x \in (\beta_p \phi_p^{-1}(C))^*} f(x) \right) \leq V^{-1} \cdot \int_{\mathbb{R}^{n^2mt}} f(x)dx,$$

where the limit is taken over primes in the family and $(\beta_p\phi_p^{-1}(C))^*$ denotes the non-zero vectors in $\beta_p\phi_p^{-1}(C)$.

Proof. Let us define $U_p = \{v \in M_n(\mathbb{F}_q)^{\oplus t} \mid \dim_{\mathbb{F}_q}(M_n(\mathbb{F}_q)v) = n^2\}$.

Now, let us show that the following sum tends to zero as $p \to \infty$.

$$\sum_{\substack{x \in (\beta_p\phi_p^{-1}(C))* \\ \phi_p(x/\beta_p) \notin U_p}} f(x) = \sum_{\substack{x \in (\phi_p^{-1}(C))* \\ \phi_p(x) \notin U_p}} f(\beta_p x)$$

If $x \in \mathcal{O}^{\oplus t}$ is such that $\phi_p(x) \notin U_p$, then at least one of the $\mathcal{O}$-coordinates will guarantee the following lower bound from Lemma 5,

$$\|\beta_p x\| \gg \beta_p \cdot q^{\frac{1}{nm}} = q^{\frac{nk-n^2t}{n^2mt}} \cdot q^{\frac{1}{nm}} = q^{\frac{1}{nmt}(k-(nt-t))}, \tag{3.1}$$

which gets arbitrarily large as $p \to \infty$. Since f decays rapidly at infinity we get for each individual lattice in $\mathbb{L}_p$ that this sum converges to 0 as $p \to \infty$.

Now we discuss the terms that remain. Observe that Lemma 7 forces that if $\phi_p(x) \in U_p$, then $|U_p||\{C \in \mathcal{C}_k \mid \phi_p(x) \in C\}| \leq |\mathcal{C}_k|q^{nt}$. Now let $g : M_n(\mathbb{F}_q)^{\oplus t} \to \mathbb{R}^+$ denote the function $g(c) = \sum_{x\in\phi_p^{-1}(c)^*} f(\beta_p x)$. We have that

$$\begin{aligned} \mathbb{E}_{\mathcal{C}_k}[\sum_{c \in \mathcal{C} \cap U_p} g(c)] &= \sum_{x \in U_p} \mathbb{E}_{\mathcal{C}_k}[g(x)\mathbf{1}_C(x)] \\ &= \sum_{x \in U_p} g(x) \frac{|\{C \in \mathcal{C}_k \mid \phi_p(x) \in C\}|}{|\mathcal{C}_k|} \leq \sum_{x \in U_p} g(x) \frac{q^{nk}}{|U_p|}. \end{aligned}$$

The result now follows: note that we have an approximation of the Riemann integral of f as

$$\lim_{p\to\infty} \sum_{x\in\mathcal{O}^{\oplus t}\setminus\{0\}} \beta_p^{n^2mt} f(\beta_p x) = V^{-1}\int_{\mathbb{R}^{n^2mt}} f(x)dx$$

since $\beta_p \to 0^+$ as p becomes large and the ratio $\frac{|U_p|}{|M_n(\mathbb{F}_q)|^t} \to 1$, as $p \to \infty$. Switching the limit in p and summation in r is allowed by dominated convergence, as f decays rapidly.

4 Improved bounds

We will now show how to leverage the extra symmetries under finite groups $G_0 \subset \mathcal{O}^\times$ of the lattices obtained in $\mathbb{L}_p$ in order to obtain sphere packings of density exceeding the Minkowski–Hlawka bound.

Given a lattice $\Lambda \subset A_{\mathbb{R}}^t$ which is an $\mathcal{O}$-module and such a choice of norm we however first define the *k-th A-minimum* $\min_k(\Lambda)$ to be the smallest r such that the closed ball $\mathbb{B}_{A_{\mathbb{R}}}(r)$ of radius r contains k $A_{\mathbb{R}}$-linearly independent lattice vectors (under the left $A_{\mathbb{R}}$-action on $A_{\mathbb{R}}^t$). In particular, $\min_1(\Lambda)$ is the shortest vector length $\lambda_1(\Lambda)$ in Λ. We begin by remarking that a lemma of Minkowski [18] which was extended by Vance [26, Theorem 2.2] holds even more generally:

Proposition 6. *Let $t \geq 2$ and Λ denote an $\mathcal{O}$-lattice in $A_{\mathbb{R}}^t$. Then Λ contains a left $A_{\mathbb{R}}$-module basis $\{v_1, \ldots, v_t\}$ such that $\|v_i\| = \min_i(\Lambda)$. Moreover, if* $\mathrm{Vol}(\Lambda) = 1$, *there exists an $\mathcal{O}$-lattice Λ' of covolume one in $A_{\mathbb{R}}^t$ such that $\lambda_1(\Lambda') = \prod_{i=1}^t \min_i(\Lambda)^{1/t}$.*

Proof. One must cautiously generalize the proof of [26, Theorem 2.2] (replacing 4 by the appropriate dimension mn^2).

Remark 1. Doing only slight modifications of the **SMP** algorithm, effectively finding the v_i can be achieved in an exponential running time of $O(2^{2t})$. Details can be found in [17].

We also record the lemma:

Lemma 8. *Let $G_0 \subset \mathcal{O}^*$ denote a finite group. Then any $\mathcal{O}$-lattice $\Lambda \in \mathbb{L}_p$ in Theorem 5 is G_0-symmetric. Furthermore, we may choose a symmetric positive definite element $a \in A_{\mathbb{R}}$ such that for all such Λ the induced norm satisfies*

$$\|x\|^2 = \sum_{i=1}^t \mathrm{T}(x_i^* a x_i) = \|g\cdot x\|^2,\ \forall g \in G_0, x \in \Lambda.$$

Proof. The morphisms ϕ_p preserve the multiplicative structure and the codes in $\mathcal{C}$ we are pulling back are $\phi_p(\mathcal{O})$-modules. For the second part, we may set $a = \sum_{g\in G_0} g^* g$.

From now on, we may and will assume a norm as in Lemma 8 has been chosen on $A_{\mathbb{R}}$. We can prove Theorem 1.

Proof. (**of Theorem 1**)

We define f to be the radial function f_r of bounded support given by

$$f_r(y) = \begin{cases} \frac{1}{mn^2} & \text{if } 0 \leq \|y\| < re^{(1-t)/mn^2t} \\ \frac{1}{mn^2t} - \log(\frac{\|y\|}{r}) & \text{if } re^{(1-t)/mn^2t} \leq \|y\| \leq re^{1/mn^2t} \\ 0 & \text{else} \end{cases}$$

This function is indeed semi-admissible and we have that $\int_{\mathbb{R}^{mn^2t}} f_r(y)dy = V_{mn^2t} \cdot r^{mn^2t} \cdot \frac{e(1-e^{-t})}{mn^2t}$, where V_{mn^2t} denotes the volume of the unit ball in mn^2t-dimensional Euclidean space. For a small $0 < \varepsilon < 1$ we may find $r \geq 0$ so that

$$V_{mn^2t} \cdot r^{mn^2t} \cdot \frac{e(1-e^{-t})}{mn^2t} = (1-\varepsilon)\cdot \frac{|G_0||\mathrm{Vol}(\mathcal{O}^t)|}{mn^2}.$$

Taking $\mathbb{L}_p$ and k satisfying the assumptions of Theorem 5, we may therefore for p large enough find a lattice $\varLambda \in \mathbb{L}_p$ of volume $\mathrm{Vol}(\mathcal{O}^t)$ such that

$$\sum_{y \in \varLambda^*} f_r(y) \leq (1-\varepsilon)\frac{|G_0|}{mn^2} < \frac{|G_0|}{mn^2}.$$

We now use the fact that the units of finite order $G_0 < \mathcal{O}^\times$ act freely on non-zero vectors of $\varLambda$ and that $\|gv\| = \|v\|$ for $g \in G_0$ for our choice of norm (see Lemma 8). Indeed, letting $\{v_1, \ldots, v_t\}$ be linearly independent vectors achieving the A-minima $\|v_j\| = \min_j(\varLambda)$ as guaranteed by Proposition 6, we then have that

$$\sum_{y \in \varLambda^*} f_r(y) \geq \sum_{j=1}^{t} \sum_{g \in G_0} f_r(gv_j) = |G_0| \sum_{j=1}^{t} f_r(v_j).$$

In other words, $\sum_{j=1}^t f_r(v_j) < 1/(mn^2)$ so that by definition of f_r we must have

$$\min_j(\varLambda) \geq re^{(1-t)/(mn^2t)} \text{ for all } j. \tag{4.1}$$

Moreover, it must then be by definition of f_r that

$$\sum_{j=1}^{t} \log\left(\frac{\min_j(\varLambda)}{r}\right) > 0 \Rightarrow \prod_{j=1}^{t} \min_j(\varLambda)^{1/t} > r, \tag{4.2}$$

and hence from proposition 6 we deduce the existence of a lattice $\tilde{\varLambda}$ with volume equal to $\mathrm{Vol}(\varLambda)$ and shortest vector length $\lambda_1(\tilde{\varLambda}) > r$. We thus obtain for all such ε the existence of a lattice $\tilde{\varLambda}_\varepsilon$ of volume $\mathrm{Vol}(\mathcal{O}^t)$ and packing density

$$\varDelta(\tilde{\varLambda}_\varepsilon) \geq (1-\varepsilon) \cdot \frac{|G_0| \cdot t}{2^{mn^2t} \cdot e(1-e^{-t})}.$$

Letting $\varepsilon \to 0$, the result follows by Mahler compactness.

Remarks 7.
The lower bounds on the density in Theorem 1 have the advantage of producing a factor t in the numerator for lattices constructed from $\mathcal{O}^t$. Via a simpler approach, taking f to be the indicator function of a ball one finds an $\mathcal{O}$- lattice $\varLambda$ which outperforms the bound above in the case when $t = 2$. This is exactly the lower bound obtained in [13].

4.1 Classification of finite subgroups of $\mathcal{O}^\times$ and bounds.

See [13, 2.2–3].

5 Notes on effectivity

Our results such as Theorem 5 imply that dense lattices in dimension mn^2t can be found among pre-images of codes in characteristic p as $p \to \infty$. In this last section we show how large it suffices to take p in order to guarantee a lattice of packing density greater than $(1-\varepsilon)\frac{|G_0|}{2^{mn^2t}}$ is found, with $G_0 < \mathcal{O}^*$ designating the units of finite order in $\mathcal{O}$.

5.1 Varying the division ring

We first focus on the case of $t = 2$ in Theorem 1 when in fact the better bounds are obtained by taking the simpler indicator function $f = \mathbb{1}_{\mathbb{B}(r)}$ of a ball of appropriate radius as in Remark 7.

Theorem 8. *Let A denote central simple division K-algebras for number fields K and denote $[A:K]=n^2$ and $[K:\mathbb{Q}]=m$. Let $\mathcal{O}$ denote a maximal order in such A. Fix $0<\varepsilon<1$. Assume the prime $\mathfrak{p}|p$ in $\mathcal{O}_K$ is chosen large enough with respect to m,n so that the size of the residue field $|\mathcal{O}_K/\mathfrak{p}|=q$ satisfies:*

1. *we have as m,n increase the relation:*
$$(n^2m)^2\mathrm{Vol}(\mathcal{O})^{2/(mn^2)}|G_0|^{-1/(mn^2)}=o(q^{1/mn}),$$
2. *the ratio $\frac{|M_n(\mathbb{F}_q)|^2}{|M_n(\mathbb{F}_q)|^2-|M_n(\mathbb{F}_q)\backslash\mathrm{GL}_n(\mathbb{F}_q)|^2}<(1+\varepsilon/3)$.*

Then there exists an effective constant $C_\varepsilon>0$ such that in dimension $2n^2m>C_\varepsilon$ there exists a lattice $\Lambda\in\mathbb{L}_p$ with packing density
$$\Delta(\Lambda)\ge(1-\varepsilon)\frac{|G_0|}{2^{2n^2m}}.$$

Here $\mathbb{L}_p$ denotes the set of scaled preimages of generalized codes of $\mathbb{F}_q$-dimension $2n^2-n$ via the reduction map $\phi_p:\mathcal{O}^2\to(\mathcal{O}/\mathfrak{p}\mathcal{O})^2$ as in Theorem 5.

Proof. Tracing through the proof of Theorem 5 for $t=2$ and $k=2n-1$ (the only sensible choice), we find that the term
$$\sum_{x\in(\phi_p^{-1}(C))^*,\phi_p(x)\notin U_p}f(\beta_px)$$
is trivial for $f=\mathbb{1}_{\mathbb{B}(r)}$ and some $C\in\mathcal{C}_{k,p}$ as soon as
$$r<n\sqrt{m}q^{\frac{1}{2nm}}\le\left(\mathrm{N}(a)^{1/2n^2m}\cdot n\sqrt{m}\right)q^{\frac{1}{2nm}}. \tag{5.1}$$
via Lemma 5 and (3.1), where $a=\sum_{g\in G_0}g^*g$.

The expected value for the remaining terms for fixed characteristic p can then be seen to be bounded by a classical geometry of numbers result (see [5, Lemma 4] or [19, Lemma 3 (2)])
$$\frac{q^{n(2n-1)}}{q^{2n^2}-(q^{n^2}-\prod_i(q^n-q^i))^2}\sum_{x\in(\mathcal{O}^2)^*}\mathbb{1}_{\mathbb{B}(r)}(\beta_px)\le\frac{q^{n(2n-1)}(r+\beta_p\tau(\mathcal{O}^2))^{2n^2m}}{q^{2n^2}-(q^{n^2}-\prod_i(q^n-q^i))^2}\frac{V_{2n^2m}}{\beta_p^{2n^2m}\mathrm{Vol}(\mathcal{O}^2)},$$
where $\tau(\mathcal{O}^2)$ denotes the packing radius of $\mathcal{O}^2$ and V_d denotes the volume of the d-dimensional unit ball. Writing $S_n(q):=\frac{q^{n(2n-1)}}{q^{2n^2}-(q^{n^2}-\prod_{i=0}^{n-1}(q^n-q^i))^2}\ge\beta_p^{2n^2m}$ we arrive at:
$$\mathbb{E}\le\frac{S_n(q)}{\beta_p^{2n^2m}}r^{2n^2m}\frac{V_{2n^2m}}{\mathrm{Vol}(\mathcal{O}^2)}\cdot\left(1+\frac{\tau(\mathcal{O}^2)\beta_p}{r}\right)^{2n^2m} \tag{5.2}$$
Observe now that $\frac{S_n(q)}{\beta_p^{2n^2m}}=\frac{|M_n(\mathbb{F}_q)|^2}{|M_n(\mathbb{F}_q)|^2-|M_n(\mathbb{F}_q)\backslash\mathrm{GL}_n(\mathbb{F}_q)|^2}$, so that we can assume q is large enough so that $\frac{S_n(q)}{\beta_p^{2n^2m}}<(1+\varepsilon/3)$.

It now suffices to show that under the parameters above, we can bound $\left(1+\frac{\tau(\mathcal{O}^2)\beta_p}{r}\right)^{2n^2m}<(1+\varepsilon/3)$ for large enough dimension, since then we get from the inequality (5.2) the existence of a lattice in $\mathbb{L}_p$ with the desired lower bound on the paking density. Recall that $\beta_p=q^{-1/2nm}$ with our parameters and we have from Lemma 6 that
$$\tau(\mathcal{O}^2)=\sqrt{2}\cdot\tau(\mathcal{O})\le\mathrm{Vol}(\mathcal{O})^{2/n^2m}\cdot(n\sqrt{m}+6)/(\sqrt{2}\pi).$$
We thus have
$$\frac{\tau(\mathcal{O}^2)\beta_p}{r}\lesssim\mathrm{Vol}(\mathcal{O})^{1/(mn^2)}|G_0|^{-1/(2mn^2)}q^{-1/(2mn)}$$

But under the assumptions of the theorem on q, the result now follows since as mn^2 goes to infinity the term $2mn^2 \cdot \frac{\tau(\mathcal{O}^2)\beta_p}{r}$ becomes arbitrarily small. Assuming p and q chosen large enough for each n, m as in the assumptions of the theorem, we get an effective constant C_ε guaranteeing $\left(1 + \frac{\tau(\mathcal{O}^2)\beta_p}{r}\right)^{2n^2m} < (1 + \varepsilon/3)$ for $n^2m > C_\varepsilon$.

We may then for instance apply this result to specific families of maximal orders in division rings of increasing $\mathbb{Q}$-dimension. One may arrange for the size of the finite units G_0 to be known in this family via Amitsur's results ([1]). Moreover, the computation of the volume $\mathrm{Vol}(\mathcal{O})$ reduces to a computation of $\sqrt{d(\mathcal{O}/\mathbb{Z})}$, since the $\mathbb{Z}$-discriminant $d(\mathcal{O}/\mathbb{Z})$ can be defined as the ideal generated by $\{\det(\mathrm{tr}_{A/\mathbb{Q}}\, x_i x_j)_{1 \le i,j \le [A:\mathbb{Q}]}\}$ for $x_i \in \mathcal{O}$ a $\mathbb{Z}$-basis.

Example 1. When $n = 1$, by considering cyclotomic fields $\mathbb{Q}(\zeta_m)$ Moustrou thus finds via a version of Theorem 8, effective dense lattices in dimensions $2\varphi(m)$ for large enough m and shows a suitable q can be found in time $O(m^3 \log(m))^{\varphi(m)}$, see [19, Theorem 1, Prop 3.1].

Proof. (**of Proposition 2**) From [1], we know that the construction $A_k = \left(\frac{-1,-1}{\mathbb{Q}(\zeta_{m_k})}\right)$ yields a division algebra since $\mathrm{ord}_m\, 2$ is odd.

From discriminant calculations, we obtain that the first condition amounts to

$$(m_k \varphi(m_k)^2)^{2\varphi(m_k)} = o(q).$$

Using an effective version of the Čebotarev density theorem (see e.g., [25]), in at most around $e^{3/4n \log n}$ steps, one can find a prime p that split completely in $\mathbb{Q}(\zeta_{m_k})$ and

$$\left| \frac{|M_2(\mathbb{F}_p)|^2}{|M_2(\mathbb{F}_p)|^2 - |M_2(\mathbb{F}_p) \setminus \mathrm{GL}_2(\mathbb{F}_p)|^2} - 1 \right| = o(e^{-n_k}),$$

which deals with the second condition of Theorem 8. The time estimate for enumerating the lattice family is then of $e^{4.5 \cdot n_k \log(n_k)(1+o(1))}$ binary operations since the number of codes we consider in Theorem 8 here amounts to $O(p^6)$. The costs of the remaining computations, such as computing the packing density of lattices, are also exponential in the dimension, but being of cost $2^{O(n_k)}$ do not contribute to the main term of the estimate.

5.2 Varying the rank t

Finally, we remark that one also obtains effective good asymptotic lattices from our constructions by fixing the division ring A and maximal order $\mathcal{O}$ and instead varying the rank of the $\mathcal{O}$-lattices as in Vance's construction [26]. In particular, one obtains an effective version of Vance's construction which we record here. The general case is handled in the same way and is left to the reader.

Proposition 9. *For any $0 < \varepsilon < 1$, there exists a lattice in $\mathbb{H}^t$ which is a free rank t module over the ring of Hurwitz integers $\mathcal{H}$, whose geometric mean of the quaternionic minima satisfy*

$$\prod_{j=1}^{t} \min_j(\Lambda)^{1/t} > r$$

where r is defined by $\mathrm{Vol}(\mathbb{B}(r)) = (1-\varepsilon)\frac{24t\mathrm{Vol}(\mathcal{H}^t)\cdot}{e(1-e^{-t})}$, and which, provided the odd prime p satisfies $t^2 = o(p)$ and t is large enough, lies in the set of (rescaled) lifts

$$\mathbb{L}_p = \{p^{\frac{1-t}{2t}} \phi_p^{-1}(C) : C \in \mathcal{C}_{t+1}\},$$

where $\phi_p : \mathcal{H}^t \to (\mathcal{H}/p\mathcal{H})^t \cong M_2(\mathbb{F}_p)^t$ is the reduction map and $\mathcal{C}_{t+1}$ is the set of left $M_2(\mathbb{F}_p)$-submodules of $M_2(\mathbb{F}_p)^t$ isomorphic to $t+1$ copies of the simple left module $\mathbb{F}_p^2$.

Proof. Consider the proof of Theorem 1. Then for any $t \geq 2$ the support of the radial function $f_r(y)$ is contained in the ball of radius $re^{1/mn^2t} = re^{1/4t}$. Choose r such that

$$\mathrm{Vol}(\mathbb{B}(r)) = (1-\varepsilon)\frac{24t\mathrm{Vol}(\mathcal{H}^t)\cdot}{e(1-e^{-t})} \tag{5.3}$$

First consider any $t < k < 2t$. Pulling back codes of $\mathbb{F}_p$-dimension $2k$ as in Theorem 5, in order to lift the averaging result we see that the support of f has to be contained in the ball of radius $2p^{1/4}$, so that we arrive at the condition

$$e^{(1+\ln(t)-2t)/(4t)} \cdot \frac{2^{-3/8}}{\sqrt{\pi}}\sqrt{t} < p^{1/4}.$$

Thus for $t \geq 2$ it in particular suffices to take $p \geq t^2$. Note that here any odd prime p is unramified and can be used in the construction. Inspecting the proof of Theorem 5, we have that

$$\mathbb{E} \leq \frac{p^{d(k)}}{|U_p| \cdot \beta_p^{4t}} \cdot \sum_{x\in\mathcal{O}^t\setminus\{0\}} \beta_p^{4t} f_r(\beta_p i(x)) = \frac{p^{4t}}{p^{4t}-(p^3+p^2-p)^t} \cdot \sum_{x\in\mathcal{O}^t\setminus\{0\}} \beta_p^{4t} f_r(\beta_p i(x))$$

as $\beta_p = p^{k/2t-1}$, and it therefore remains to bound the difference

$$\varDelta(p,t) = \left| \beta_p^{4t} \cdot \sum_{x\in\mathcal{O}^t\setminus\{0\}} f_r(\beta_p i(x)) - V^{-1}\int_{\mathbb{R}^{4t}} f_r(x)dx \right|. \tag{5.4}$$

We note that in particular f_r has derivative bounded by $C_r = e^{1/4}/r$. Tiling the support of f_r by Voronoï cells of diameter the packing radius $\tau(\beta\mathcal{O}^t)$, we can bound the error in approximating the Riemann integral via the lattice sum on each individual cell by $\mathrm{Vol}(\mathcal{O}^t)\beta_p^{4t} \cdot C_r \cdot 2\tau(\beta\mathcal{O}^t)$. For large enough p, t, we may estimate that the support of f_r is covered by $\sim \beta^{-4t}e \cdot \frac{Vol(\mathbb{B}(r))}{\mathrm{Vol}(\mathcal{O}^t)}$ cells, so that we arrive at the total error estimate

$$\varDelta(p,t) \lesssim 2eC_r \cdot \beta_p \frac{\mathrm{Vol}(\mathbb{B}(r))}{\mathrm{Vol}(\mathcal{O}^t)} \cdot \sqrt{t} \cdot \tau(\mathcal{O}) \tag{5.5}$$

We therefore obtain for r satisfying (5.3) the bound as p, t become large of

$$\varDelta(p,t) = O(t) \cdot p^{\frac{k-2t}{2t}}.$$

We see that in particular the condition $t^2 = o(p)$ suffices to guarantee for any given $\varepsilon > 0$ that $\varDelta(p,t) < \varepsilon$ for large enough rank t. We have thus shown that for any ε we can find t large enough so that under our assumptions on p there exists $\Lambda \in \mathbb{L}_p$ with $\sum_{y\in\Lambda'} f_r(y) \leq (1-\varepsilon)\cdot 6$. The result now follows as in the proof of Theorem 1.

We therefore conclude:

Corollary 1. *Given any* $0 < \varepsilon < 1$*, for large enough* t *a lattice* $\tilde{\Lambda}$ *in dimension* $4t$ *whose packing density satisfies*

$$\varDelta(\tilde{\Lambda}) \geq (1-\varepsilon) \cdot \frac{24t}{2^{4t} \cdot e(1-e^{-t})}$$

can be constructed with $e^{4t^2\log(t)(1+o(1))}$ *bit operations.*

Acknowledgements

We would like to thank Gauthier Leterrier, Martin Stoller and Maryna Viazovska for helpful conversations on the topics of this paper. We thank Matthew De Courcy-Ireland for insightful comments on a previous version of this manuscript.

Nihar Gargava got funded by the Swiss National Science Foundation (SNSF), Project funding (Div. I-III), “Optimal configurations in multidimensional spaces”, 184927.

References

1. Amitsur, S.A.: Finite subgroups of division rings. Trans. Amer. Math. Soc. **80**, 361–386 (1955)
2. Ball, K.: A lower bound for the optimal density of lattice packings. Int. Math. Res. Not. IMRN **1992**(10), 217–221 (05 1992). https://doi.org/10.1155/S1073792892000242, https://doi.org/10.1155/S1073792892000242
3. Bayer Fluckiger, E.: Upper bounds for Euclidean minima of algebraic number fields. J. Number Theory **121**(2), 305–323 (2006). https://doi.org/https://doi.org/10.1016/j.jnt.2006.03.002, https://www.sciencedirect.com/science/article/pii/S0022314X0600062X
4. Berhuy, G., Oggier, F.: An introduction to central simple algebras and their applications to wireless communication. Amer. Math. Soc. (2013)
5. Campello, A.: Random ensembles of lattices from generalized reductions. IEEE Trans. Inform. Theory **64**(7), 5231–5239 (2018). https://doi.org/10.1109/TIT.2018.2803839
6. Cohn, H.: A conceptual breakthrough in sphere packing. Notices Amer. Math. Soc. **64** (11 2016). https://doi.org/10.1090/noti1474
7. Cohn, H., Kumar, A.: Optimality and uniqueness of the Leech lattice among lattices. Ann. of Math. **170** (03 2004). https://doi.org/10.4007/annals.2009.170.1003
8. Cohn, H., Kumar, A., Miller, S.D., Radchenko, D., Viazovska, M.: The sphere packing problem in dimension 24. Ann. of Math. **185**(3), 1017–1033 (2017), http://www.jstor.org/stable/26395748
9. Conway, J., Sloane, N.: Sphere Packings, Lattices and Groups, Grundlehren Math. Wiss., vol. 290. Springer (01 1988). https://doi.org/10.1007/978-1-4757-2016-7
10. Davenport, H., Rogers, C.A.: Hlawka's theorem in the geometry of numbers. Duke Math. J. **14**(2), 367 – 375 (1947). https://doi.org/10.1215/S0012-7094-47-01429-4, https://doi.org/10.1215/S0012-7094-47-01429-4
11. Ducoat, J., Oggier, F.: On skew polynomial codes and lattices from quotients of cyclic division algebras. Adv. Math. Commun. **10**(1), 79–94 (2016)
12. Gaborit, P., Zémor, G.: On the construction of dense lattices with a given automorphisms group. Ann. Inst. Fourier **57**(4), 1051–1062 (2007), http://eudml.org/doc/10250
13. Gargava, N.P.: Lattice packings through division algebras. arXiv **abs/2107.04844** (2021)
14. Hales, T.C.: A proof of the Kepler conjecture. Ann. of Math. **162**, 1063–1183 (2005)
15. Hlawka, E.: Zur Geometrie der Zahlen. Math. Z. **49**, 285–312 (1943), http://eudml.org/doc/169025
16. Loeliger, H.A.: Averaging bounds for lattices and linear codes. IEEE Trans. Inform. Theory pp. 1767–1773 (1997)
17. Micciancio, D., Goldwasser, S.: Complexity of lattice problems: a cryptographic perspective, vol. 671. Springer Sci. & Bus. Media (2012)
18. Minkowski, H.: Geometrie der Zahlen. B.G. Teubner (1910), https://books.google.ch/books?id=MusGAAAAYAAJ
19. Moustrou, P.: On the density of cyclotomic lattices constructed from codes. Int. J. Number Theory **13** (03 2016). https://doi.org/10.1142/S1793042117500695
20. Reiner, I.: Maximal Orders. Lond. Math. Soc. Monogr. Ser., Clarendon Press (2003), https://books.google.ch/books?id=0liBQgAACAAJ
21. Rogers, C.A.: Existence theorems in the geometry of numbers. Ann. of Math. **48**(4), 994–1002 (1947), http://www.jstor.org/stable/1969390
22. Rush, J., Sloane, N.: An improvement to the Minkowski-Hlawka bound for packing superballs. Mathematika **34**, 8 – 18 (06 1987). https://doi.org/10.1112/S0025579300013231
23. Rush, J.A.: A lower bound on packing density. Invent. Math. **98**(3), 499–510 (1989), http://eudml.org/doc/143740
24. Siegel, C.L.: A mean value theorem in geometry of numbers. Ann. of Math. **46**, 340 (1945)
25. Thorner, J., Zaman, A.: A unified and improved Chebotarev density theorem. Algebra Number Theory **13** (03 2018). https://doi.org/10.2140/ant.2019.13.1039
26. Vance, S.: Improved sphere packing lower bounds from Hurwitz lattices. Advan. Math. **227** (05 2011). https://doi.org/10.1016/j.aim.2011.04.016
27. Vehkalahti, R., Luzzi, L.: The DMT of real and quaternionic lattice codes and DMT classification of division algebra codes. ArXiv **abs/2102.09910** (2021)
28. Venkatesh, A.: A note on sphere packings in high dimension. Int. Math. Res. Not. IMRN **2013**(7), 1628–1642 (03 2012). https://doi.org/10.1093/imrn/rns096, https://doi.org/10.1093/imrn/rns096
29. Viazovska, M.S.: The sphere packing problem in dimension 8. Ann. of Math. **185**(3), 991–1015 (2017), http://www.jstor.org/stable/26395747