Dense Packings via Lifts of Codes to Division Rings

Nihar Gargava and Vlad Serban

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 \(\Delta_n\) in a variety of new dimensions \(n\). This unifies and extends a number of previous constructions.

Index Terms—Lattices, sphere packings, random codes, codes over matrix rings, division rings.

I. 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 \(\Lambda\). The proportion achieved by a particular lattice, called the packing density of \(\Lambda\), is then given by

\[
\Delta(\Lambda) := \frac{\text{Vol}(\mathbb{B}_n(\lambda_1(\Lambda)))}{2^n \text{Vol}(\Lambda)},
\]

where \(\lambda_1(\Lambda)\) denotes the shortest vector length in \(\Lambda\), \(\mathbb{B}_n(r)\) a ball of radius \(r\) and \(\text{Vol}(\Lambda)\) denotes the covolume of the lattice. We also denote by \(\Delta_n\) 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 [1, 1.5.] as well as [2]. The density is achieved by highly symmetric lattices such as root lattices or the Leech lattice. Owing to highly celebrated results [3], [4], [5], some of these are even known to solve the general sphere packing problem. For arbitrary dimensions, the best known upper and lower bounds on \(\Delta_n\) 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 [7] states that \(\Delta_n \geq \frac{2}{\pi}n\), a bound which Rogers [8] later improved by a linear factor to \(\Delta_n \geq \frac{2}{\pi\sqrt{2}}n\) for \(c = 2/e \approx 0.74\). The constant was subsequently sharpened to \(c = 1.68\) by Davenport-Rogers [9] and \(c = 2\) by Ball [10] for all \(n\). More recently, Vance [11] showed using lattices which are modules over the Hurwitz integers that one may take \(c = 24/e \approx 8.83\) and Venkatesh [12] 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 \(\Delta_n \geq \frac{n}{\log \log(n/\pi)}\). 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 [13], [14]) 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 \(\Delta_n \geq \frac{c_1^n \log \log(c_2^n + 1)}{2^n}\) for constant \(c_1, c_2 > 0\) are uncovered.

Lattices provide an important tool for coding, for instance for the Additive White Gaussian Noise (AWGN) model. For such applications it is often desirable to have lattices that are “good” in the sense of achieving high packing densities (see e.g., [15]). The sphere packing problem is moreover crucially connected to optimizing parameters of codes and energy optimization (see e.g., [1], [16]). However, despite having Minkowski’s lower bound for over a century, producing explicit families of lattices that achieve these asymptotic bounds in less than astronomical running time has proved elusive. Currently known polynomial time algorithms produce lattices whose densities are exponentially worse than these bounds [17]. In this paper, we make the currently best known 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 bounds stated above.

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 \(\phi_p : \mathcal{O}^t \rightarrow (\mathcal{O}/p\mathcal{O})^t\) and may identify the quotient with a product of matrix rings over a finite field \(\mathbb{F}_q\). The sets of lattices \(L_p\) we consider are then re-scaled pre-images via \(\phi_p\) of codes in \((\mathcal{O}/p\mathcal{O})^t\) of a certain fixed \(\mathbb{F}_q\)-dimension. Our first main result, Theorem 21, is in effect a Siegel mean value theorem for these sets of lifts of codes valid for general finite dimensional \(\mathbb{Q}\)-division algebras. We refer the
reader to Section III for detailed statements, whereas some useful preliminary results on lattices from division algebras are established in Section II.

In Section IV, the extra symmetries of these lattices under finite subgroups of \( O^K \) is exploited to obtain (see Theorem 25):

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

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

Moreover, there exists for any \( \varepsilon > 0 \) an \( O \)-lattice \( \Lambda_\varepsilon \) in dimension \( n^2 mt \) of packing density

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

which can be constructed. Indeed, \( \Lambda_\varepsilon \) is obtained by applying Proposition 22 to a suitable sublattice of \( O' \) obtained as a pre-image via reduction modulo primes \( p \) of \( O_K \) of large enough norm of a code. The code in question is isomorphic to \( k \) copies of simple left \( \mathcal{O}/p\mathcal{O} \)-modules for some \( nt - t < k < nt \).

Note that Proposition 22 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 21 by mimicking an approach of Rogers [8], later used by Vance [11] and Campello [18]. In this way, we combine nearly all of these existence results and generalize them in one theorem.

In order to obtain the densest packings asymptotically, one therefore seeks families of orders \( O \) with large finite unit groups \( G_0 \subset O^\times \). Building on Amitsur’s classification [19] 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, due to a parity condition on the dimension, this is not quite the case and one obtains asymptotic lower bounds

\[
\Delta_n \geq 3 \cdot (\log \log n)^{7/24n} \cdot (1 + o(1))
\]

Still, the lower bound obtained exceeds the lower bound from cyclotomic fields \( n \log \log n \cdot 2^{-(n+1)} \) in less than astronomical dimensions due to the improved constant. Moreover, one can exhibit lattices from non-commutative rings that achieve the same asymptotic density as the cyclotomic lattices (see Proposition 7).

Finally, in Section V we establish effectiveness by giving lower bounds on the norm of the prime \( p \) so that packing densities such as in Theorem 1 can be achieved, both by varying the division algebra and its dimension (Theorem 28) and by varying the rank of the \( O \)-lattices to obtain an effective version of Vance’s results (Proposition 33). As an application, we obtain in Proposition 31:

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

\[
\Delta(\Lambda) \geq (1-\varepsilon)\cdot \frac{2^{\frac{24 \cdot m_k}{2^{n_k}}} \cdot (1 + o(1))}{2^{n_k}}
\]

which 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 \( \Delta(\Lambda) \geq (1-\varepsilon^{-n_k})\cdot \frac{2^{\frac{24 \cdot m_k}{2^{n_k}}} \cdot (1 + o(1))}{2^{n_k}} \).

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 [20], building on work with Sloane [21], 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 [1, Chapter 5]). The connection between random coding and such averaging results was further explicited by Loeliger [15]. Finally, Moustrou [23] used a similar approach for cyclotomic lattices to obtain an effective version of Venkatesh’s result. This approach was further formalized by Campello [18], 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 [18], [23] and 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 by coding theorists, see for example [24], [25], [26].

We hope that this article provides a useful addition to both the coding-theoretic and mathematical literature. The effective results we arrive at in Section V typically have a complexity of \( e^{C \cdot n \log(n)/(1+o(1))} \), which is similar to [23, Theorem 1]. However, the effective version of Vance’s result (see Corollary 34) 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 \( O \)-rank of the lattices.

The running times correspond to an exhaustive search through all the finitely many lattice candidates and it would be interesting to examine if one can further reduce the complexity of this search. It should be remarked that our results can still be used to quickly generate one of these random lattices in high dimensions that have prescribed symmetries and are expected to have large minimal vectors. Furthermore, our results hint towards the algebraic structures that one might look for in order to construct explicit families of lattices that are asymptotically “good”.

## II. Preliminaries on Division Rings and Resulting Bounds

In this section, we recall some definitions and results on division rings as well as on lattices from orders in \( \mathbb{Q} \)-division rings. The primary reference for the algebraic background is Reiner’s book [27] and we shall refer to the first author’s work [13] for some results on the lattices. Let \( O_K \) denote...
the ring of integers of a number field $K$ and let $A$ denote a separable $K$-algebra.

Definition 3: An $O_K$-order in $A$ is a subring $O$ of $A$ having the same identity element and such that $O$ is a full $O_K$-lattice in $K$, i.e. $O$ is a finitely generated $O_K$-submodule of $A$ such that $K \cdot O = A$.

The existence of $O_K$-orders and maximal orders is easily shown. From now on let $O$ denote such an order. We shall assume $O$ is maximal since this suffices for our applications.

A. Lattices From Orders

The central simple algebras $A$ are equipped with natural embeddings $A \hookrightarrow A \otimes \mathbb{Q} \mathbb{R}$. The latter space being a semisimple $\mathbb{R}$-algebra, it can be identified with a product of matrix rings over $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$ respectively, depending on the signature of $K$ and the splitting behavior of $A$ at infinity. An $O_K$-order then embeds as a lattice into this space. We establish some properties of these lattices in the next two subsections.

Lemma 4: Any semisimple $\mathbb{R}$-algebra $A$ admits an involution $(\cdot)^*: A \to A$ 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 $a \mapsto T(a^* a)$ on $A$, meaning that $T(a^* a)$ is always non-negative and is zero only when $a = 0$. Moreover, this quadratic form induces the inner product $\langle x, y \rangle = T(x^* y)$ 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 4 will henceforth be called “positive involutions”. An element $a \in A_\mathbb{R}$ such that $a^* = a$ and $x \mapsto T(x^* a x)$ is a positive definite real quadratic form on $A_\mathbb{R}$ is called symmetric and positive definite. For instance, for any unit $a$ the element $a^* a$ is symmetric positive definite.

In practice, 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 $O^t \subseteq A^t \hookrightarrow (A_\mathbb{R})^t$. We will endow the space $A^t_\mathbb{R}$ with the norm induced by the following quadratic form:

$$\begin{aligned}
A^t_\mathbb{R} &\to \mathbb{R} \\
(x_1, x_2, \ldots, x_t) &\mapsto \sum_{i=1}^t T(x_i^* a x_i),
\end{aligned}$$

where $(-)^*$ is a positive involution as defined above and $a \in A_\mathbb{R}$ is a symmetric positive definite element to be fixed later. This makes $A^t_\mathbb{R}$ into an Euclidean space of real dimension $mn^2 t$ and $O^t$ embeds as a lattice into that space.

B. Finite Subgroups of $O^t$, Examples and Bounds

Recently, dense packings from $O$-lattices were found for special types of division algebras by Venkatesh [12] when $A = K = \mathbb{Q}(\zeta_m)$ and by Vance [11] when $A = \left(\begin{smallmatrix} -1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ is a quaternion algebra. They exploit that the respective $O$-lattices are invariant under $\mathbb{Z}/m\mathbb{Z} \subset O^\times$ and the binary tetrahedral group $\mathbb{T}^* \cong SL_2(\mathbb{F}_3) \subset O^\times$ of order 24, respectively.

More generally, from finite subgroups $G_0 < O^\times$, the first author [13] obtained an improvement of $|G_0|/2$ on the Minkowski bound from suitable $O$-lattices. Moreover, the finite groups $G_0 < O^\times$ which can occur for $\mathbb{Q}$-division algebras have been completely classified by Amitsur [19]. For instance, one may attempt to combine the two improvements by Vance and Venkatesh and consider the following:

Proposition 5: Assume $m$ is a positive integer such that $2$ has odd order modulo $m$. Then the algebra $\mathbb{Q}(\zeta_m) \otimes \mathbb{Q}$ is a division algebra with center $\mathbb{Q}(\zeta_m)$ and has a maximal $\mathbb{Z}(\zeta_m)$-order $O$ with subgroup $\mathbb{T}^* \times \mathbb{Z}/m\mathbb{Z} \subset O^\times$.

Proof: See [19, Theorems 6a, 7].

Maximizing the ratio $|G_0|/8\phi(m) = 3m/\phi(m)$ of finite units against the lattice dimension subject to the parity condition above, the first author obtained the nonconstructive:

Proposition 6: Let $m_k = \prod_{p \leq k \text{ prime}} p$. There exist for some fixed constant $C > 0$ lattice packings in dimension $8\phi(m_k)$ of density

$$\Delta \geq C(\log \log \varphi(m_k))^{7/24} \cdot 24 \cdot \varphi(m_k)^{1/24}.$$  (3)

Moreover, for any $C < 1$ the bound in (3) is valid for $m_k$ large enough.

Proof: This is [13, Theorem 30].

We refer the reader to the discussion in [13, Sections 2.2-3] for Amitsur’s classification and ways to deduce good packing bounds.

As a final example, consider division algebras $A = \left(\begin{smallmatrix} \zeta_m & 1 \\ -1 & \zeta_m^{-1} \end{smallmatrix}\right)$. The dihedral group $D_{2m} \subset O^\times$ then acts on $O$-lattices, leading to the nonconstructive result:

Proposition 7: There exists an infinite sequence of dimensions $\{d_n\}$ in which a packing density

$$\Delta_{d_n} \geq \frac{1}{2} \log \log d_n \log \frac{d_n}{2m}$$

is achieved and the lattice achieving this packing density is invariant under the action of a non-commutative group.

Proof: See [13, Prop 31] for details.

With the goal of making such results constructive, we now establish some properties of reduction maps to finite $\mathbb{F}_p$-algebras.

C. Primes, Completions and Reductions

The reader unfamiliar with completions may skip all but the statement of Lemma 9 in this subsection. For a prime ideal $p$ of $O_K$ we shall denote by $O_p, A_p$ the localizations at $p$ of the $O_K$-order $O$ and of the algebra $A$ and by $\hat{O}_p, \hat{A}_p$ the respective completions. We have:

Theorem 8: Let $O$ be a maximal order in a central simple $K$-algebra $A$. Let $p$ denote a prime of $O_K$. Then the completion $\hat{A}_p$ is a central simple $\hat{K}_p$-algebra and $\hat{O}_p$ is a maximal order. Moreover:

1) All but finitely many primes $p$ of $O_K$ are split (or unramified), namely

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

with $n^2 = [A : K]$.

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
2) The order $\Lambda = M_n(\hat{O}_p)$ is a maximal $\hat{O}_K$-order in $M_n(\hat{K}_p)$ and any maximal $\hat{O}_K$-order is of the form $u\Delta u^{-1}$ for $u \in \text{GL}_n(\hat{K}_p)$.

Proof: These are well-known results, see e.g. [27, Theorems 17.3, 32.1].

We can now establish the following lemma which will provide the necessary reduction maps in order to lift codes from characteristic $p$ to division rings:

Lemma 9: Let $K$ be a number field and $A$ a division algebra with center $K$ so that $[A : K] = n^2$. Let $O$ be a maximal $\hat{O}_K$-order in $A$. Then for all but finitely many primes $p$ of $O_K$ (the split primes), the quotient $O/pO$ is isomorphic to $M_n(F_q)$, where $O_K/pO_K \cong F_q$.

Proof: The completion satisfies $\hat{A}_p \cong M_n(\hat{K}_p)$ when $p$ splits and the order $\hat{O}_p$ in the local case is maximal and conjugate to $M_n(\hat{O}_K)$. In particular, we then have $O/pO \cong M_n(\hat{O}_K)/\text{rad}(M_n(\hat{O}_K))$, where $\text{rad}(M_n(\hat{O}_K))$ denotes the unique maximal two-sided ideal of $M_n(\hat{O}_K)$ (see [27, Theorems 22.3,22.4]). The latter quotient is then easily seen to equal $M_n(\hat{O}_K/p\hat{O}_K) \cong M_n(F_q)$.

If one wishes to ensure $q = p$ is moreover a prime number this can be achieved for infinitely many $p$ due to Čeboarev density, by imposing that $p$ splits completely in $O_K$.

D. Norm-Trace Inequality

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 key lower bounds on the Euclidean norm of certain lattice points via Lemma 13.

Lemma 10: Consider a finite dimensional semisimple $\mathbb{R}$-algebra $A_R$ together with a positive involution $(\cdot)^*$. Let $a \in A_R$ be a symmetric positive definite element and let $d = \dim_{\mathbb{R}} A_R$. Then $N(a) > 0, T(a) > 0$ and

$$\frac{1}{d} T(a) \geq N(a)^{\frac{1}{d}}.$$  

(4)

Proof: See [13, Lemma 40].

Corollary 11: In the same setting as above, we have for any $x \in A_R$ and for $a \in A_R$ symmetric positive definite that

$$\frac{1}{d} T(x^*ax) \geq N(x)^{\frac{d}{2}} N(a)^{\frac{1}{2}}.$$  

(5)

Proof: Note that $x^*ax$ is symmetric and positive definite when $x$ is a unit in $A_R$. If $x$ is not a unit, then the right-hand side is trivial.

We remark that appropriate scalar matrices show the inequalities above are sharp. For central simple $K$-algebras $A$, one can furthermore define the “reduced norm” and the “reduced trace” which we denote by $\nu_A/K, tr_{A/K} : A \to K$. Definitions and properties can be found in [27, Section 9]. We can now turn to establishing a preparatory lemma as well as the main result of this subsection, Lemma 13:

Lemma 12: Let $A$ be a division algebra over $\mathbb{Q}$ whose center is $K$ and $[A : K] = n^2$. Let $O \subseteq A$ be a maximal order in the division algebra. Let $p$ be a prime ideal of $O_K$ for which $A$ splits and let $F_q = O_K/p$ denote the residue field. Then the following diagram commutes:

$$
\begin{array}{ccc}
O & \xrightarrow{\nu_{A/K}} & O_K \\
\downarrow{\pi_p} & & \downarrow{\pi_p} \\
O/pO & \cong & M_n(F_q) \\
\end{array}
$$

(6)

where the vertical maps designate reduction modulo $p$.

Proof: The reduced norm $\nu_{A/K}(a)$ may be computed as the determinant of the corresponding matrix in $M_n(E)$, where $E$ is a splitting field for $A$ (and is independent of that choice). We may in particular choose $E$ to be the $p$-adic completion $\hat{K}_p$. If the image $O_p$ of $O$ in $\hat{K}_p = M_n(\hat{O}_K)$, then one obtains the desired result from the obvious commutativity of the diagram

$$
\begin{array}{ccc}
M_n(\hat{O}_K) & \xrightarrow{\text{det}} & M_n(F_q) \\
\downarrow{\pi_p} & & \downarrow{\pi_p} \\
O_p/pO_p & \cong & M_n(F_q) \\
\end{array}
$$

(7)

Now it is not necessarily the case that $O_p = M_n(O_{\hat{K}_p})$. However, since all the maximal orders are conjugate by Theorem 8 and the reduced norm is invariant under conjugation we may assume $\nu_{A/K}$ and $\phi_p$ on $O$ factor through $M_n(O_{\hat{K}_p})$. The commutativity of diagram (6) then follows from that of (7).

Lemma 13: Let $A$ be a $\mathbb{Q}$-division algebra with center $K$, let $O$ denote a maximal order and let $p$ be a prime of $O_K$ at which $A$ is split, so that we have a reduction map

$$\phi_p : O \to O/pO \cong M_n(F_q),$$

with $n = \sqrt{|A : K|}$. Let $(\cdot)^* : A_R \to A_R$ be a positive involution. If $x \in O \setminus \{0\}$ (which we may identify with its image in $A_R$) is such that $\phi_p(x)$ is a non-invertible matrix, then

$$\|x\| \geq \left(\sqrt{|A : \mathbb{Q}|} \cdot N(a)^{\frac{1}{|\mathbb{A}[A/K]|}} \cdot q^{\sqrt{|\mathbb{A}[A/K]|}} \right)^{\frac{1}{d}}.$$  

(8)

where $a \in A_R$ is symmetric positive definite and $\|x\|^2 := T(x^*ax)$ on $A_R$.

Proof: We know from the norm-trace inequality that

$$\frac{1}{|\mathbb{A}[A/K]|} T(x^*x) \geq N(x)^{\frac{d}{2}} N(a)^{\frac{1}{2}}.$$  

(9)

Since $\text{det} \circ \phi_p(x) = 0$, we get by Lemma 12 that $p | \nu_{A/K}(x)$ and hence

$$N_{K/\mathbb{Q}}(p) | N_{K/\mathbb{Q}} \circ \nu_{A/K}(x)$$

(10)

Using the property $N_{A/\mathbb{Q}}(x)^2 \cdot \sqrt{|A : K|} = N_{K/\mathbb{Q}} \circ \nu_{A/K}(x)$ (see [27, 9.13-14]), we deduce:

$$N_{K/\mathbb{Q}}(p)^{\frac{1}{\sqrt{|A : \mathbb{Q}|}}} | N_{A/\mathbb{Q}}(x).$$  

(11)

Since $N_{A/\mathbb{Q}}(x)^2 \in \mathbb{Z}_{\geq 0}$ and $x \neq 0$, this gives us a lower bound on $N_{A/\mathbb{Q}}(x)^2$. Thus we have:

$$\frac{1}{|\mathbb{A}[A/K]|} T(x^*x) \geq N_{K/\mathbb{Q}}(p)^{\frac{2}{\sqrt{|\mathbb{A}[A/K]|}}} N(a)^{\frac{1}{\sqrt{|\mathbb{A}[A/K]|}}}.$$  

(12)
which proves the claim given that \( N_{K/Q}(p) = |\mathcal{O}_K/p| = q \).

We also record the following result which will be used for some estimates in Section V:

**Lemma 14:** 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 \( A_k = A \otimes_{Q} \mathbb{R} \). Then, with respect to any quadratic form \( q_{a}(x) = T(xa^tx) \) for a symmetric positive definite element \( a \in A_k \), one may define the shortest vector length \( \lambda_{1,q_{a}} \), Hermite parameter \( \gamma_{q_{a}} \) and covering radius \( \tau_{q_{a}} \), and they are subject to the following:

1) The shortest vector length satisfies \( \lambda_{1,q_{a}}(\mathcal{O}) \geq \sqrt{|A : Q|} \cdot N(a)^{1/2[\bar{A}:Q]} \).
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 \( \gamma_{q_{a}}(I) \geq \frac{|A : Q|}{d(\mathcal{O}/\mathbb{Z})^{1/[A:Q]}} \).
3) The covering radius \( \tau_{q_{a}}(\mathcal{O}) \) is bounded above by \( d(\mathcal{O}/\mathbb{Z})^{1/[A:Q]} \cdot \left( \frac{\sqrt{|A : Q|}}{2\pi} + \frac{3}{\pi} \right) \cdot N(a)^{-1/[\bar{A}:Q]} \),

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

**Proof:** The first part follows trivially from the norm-trace inaccuracy. For the second statement, we know \( I \) also yields a lattice in \( A_k \) and the proof follows in this more general setting along the same lines as in [28, Section 4] for ideal lattices in number fields. The third statement then follows via a transference theorem [29, (1.9)] refining a result of Banaszczyk [30]. Note that under our choice of inner product \( \langle x, y \rangle = T(xa^ty) \) corresponding to \( q_{a} \), the dual lattice \( \mathcal{O}_K^t \) is just \( a^{-1} \) times the image under the involution \( -(\cdot)^* \) of the inverse different \( \Delta(\mathcal{O}/\mathbb{Z})^{-1} = \{ x \in A : \text{tr}_{A/Q}(x \cdot \mathcal{O}) \subset \mathbb{Z} \} \) and therefore has the same parameters.

We now have the necessary tools in place to tackle the main results of the paper.

### III. A General Averaging Result for Lifts

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 \( m = [K : Q] \). Let \( \mathcal{O} \) denote a maximal order in \( A \). The purpose of this section is to prove a discrete version of a Siegel mean value theorem (see [12], [13], [14]) for \( \mathcal{O} \)-lattices obtained via lifts of codes in characteristic \( p \) for increasingly large primes \( p \). In order to facilitate discussion and comparison with previous results, we will state a more abstract and flexible version of the main averaging result and later explain the most convenient choices of parameters.

Assume we are given for a fixed integer \( t \geq 2 \) a family of surjective homomorphisms \( \phi_{p} : \mathcal{O}_K^t \rightarrow \mathcal{R}_p^t \), indexed by primes \( p \), where \( \mathcal{R}_p \) is a finite \( \mathbb{F}_p \)-algebra of fixed \( \mathbb{F}_p \)-rank \( d_R \) and where the sizes of \( p, \mathcal{R}_p \) are unbounded in the family. We also fix an embedding \( i : A \hookrightarrow \mathbb{R}^{n^2m} \) which identifies \( \mathcal{O}_K^t \) with a lattice in \( \mathbb{R}^{n^2m} \). Assume we are given subsets \( U_p \subset \mathcal{R}_p^t \) and sets of \( \mathcal{R}_p \)-submodules \( \mathcal{C}_k \) of \( \mathcal{R}_p^t \) of fixed \( \mathbb{F}_p \)-dimension \( d(k) < t \cdot d_R \) (which we refer to as generalized \( k \)-dimensional codes) such that the following two conditions hold:

1) (\( U \)-balancedness): For any fixed \( p \) in the family and \( x \in U_p \), the number of \( k \)-dimensional codes in \( \mathcal{C}_k \) containing \( x \) is constant (we denote this constant \( L_{U_p} \)).
2) (non-degeneracy): There exists a constant \( c_U > 0 \) and \( s > \frac{d_R \cdot \text{max}_{k}(d(k))}{mn^2t} \) such that \( ||i(x)|| \geq c_U \cdot p^s \) for any nonzero \( x \in \phi_{p}^{-1}(\mathcal{R}_p^t \setminus U_p) \).

We also require the mild condition that \( \lim_{p \to \infty} |U_p| = 1 \).

We can then prove an averaging result for lifts in this general setup. Denote within this setup the set of scaled lattices \( L_p = \{ \beta \phi_{p}^{-1}(C) : C \in \mathcal{C}_k \} \), where \( \beta \) is chosen such that all the lattices in \( L_p \) have volume \( V := \text{Vol}(\mathcal{O}_K^t) \), \( \beta \geq (\frac{p}{|\mathcal{R}_p|})^{1/n^2mt} \). Finally, we define following [18, Def 2]:

**Definition 15:** A function \( f : \mathbb{R}^d \rightarrow \mathbb{R} \) is called semi-admissible if \( f \) is Riemann-integrable and there exist positive constants \( b, \delta > 0 \) such that \( |f(x)| \leq \frac{b}{(1 + \|x\|)^{d+\delta}} \) for all \( x \in \mathbb{R}^d \).

We then have the following:

**Theorem 16:** Let \( \mathcal{C}_k \) be the set of codes of fixed \( \mathbb{F}_p \)-dimension \( d(k) \) and let \( f : \mathbb{R}^{m^2t} \rightarrow \mathbb{R} \) be a semi-admissible function for \( t \geq 2 \). Under the setup and notations above, assume the \( U \)-balancedness and non-degeneracy conditions are satisfied. Then, provided \( d_R \cdot t > d(k) > t \cdot (d_R - s(n^2m)) \), we have:

\[
\lim_{p \to \infty} \mathbb{E}_{\mathcal{O}_p} \left( \sum_{x \in (\beta \phi_{p}^{-1}(C))^t} f(i(x)) \right) \leq \frac{\int_{\mathbb{R}^{n^2mt}} f(x)dx}{\zeta(n^2mt) \cdot V}.
\]

where \( p \) ranges over the primes in the family and where for \( \Lambda \in \mathbb{L}_p \) we denote by \( \Lambda' \) the primitive vectors in \( \Lambda \) (=shortest vectors of the lattice on the real line they span).

We note that we set up the non-degeneracy condition so that in the very least the largest dimension \( d(k) \) possible for the appropriate notion of \( k \)-dimensional code which is strictly contained in \( \mathcal{R}_p^t \) satisfies the condition \( d_R \cdot t > d(k) > t \cdot (d_R - s(n^2m)) \) and so the result is not vacuous. **Proof:** We split the expected value of the lattice sum into two parts: First, we show that the expected value of the term

\[
\sum_{x \in (\beta \phi_{p}^{-1}(C))^t, \phi_{p}(x/\beta) \in (\mathcal{R}_p^t \setminus U_p)} f(i(x)) \]

which we may rewrite as

\[
\sum_{x \in (\phi_{p}^{-1}(C))^t, \phi_{p}(x) \in (\mathcal{R}_p^t \setminus U_p)} f(\beta i(x))
\]

tends to zero in absolute value as \( p \to \infty \). By the non-degeneracy condition, we can bound

\[
||i(x)|| \geq \beta \cdot c_U \cdot p^s \geq c_u \cdot p^{(d(k) - d_R \cdot t)/(mn^2t)} \cdot p^s
\] (13)
which under our assumption on \( d(k) \) becomes arbitrarily large as \( p \to \infty \). Since \( f \) decays rapidly at infinity we get for each individual lattice in \( \mathbb{L}_p \) that the sum converges to 0 as \( p \to \infty \) by dominated convergence, and therefore idem for the average.

The remaining terms can be bounded on average via \( U \)-balancedness. Indeed, let \( g : R_p^t \to \mathbb{R}^+ \) denote any function. We have that

\[
\mathbb{E}_\mathbb{C} \left[ \sum_{c \in \mathbb{C} \cap U_p} g(c) \right] = \sum_{x \in U_p} \mathbb{E}_\mathbb{C}[g(x) \mathbf{1}_\mathbb{C}(x)]
= \sum_{x \in U_p} g(x) \frac{|U_p|}{|\mathbb{C}|} \\
\leq \sum_{x \in U_p} g(x) \frac{p^{d(k)}}{|\mathbb{p}|},
\]

where we use \( U \)-balancedness as well as a counting argument for the inequality and where the expected value is taken as average over all codes in \( \mathbb{C} \). We deduce the inequality

\[
\mathbb{E} \left[ \sum_{x \in (\phi^{-1}(C))' \cap \phi(x) \in U_p} f(\beta i(x)) \right] \leq \frac{p^{d(k)}}{|\mathbb{p}|} \sum_{x \in (\mathbb{O}^t)'} f(\beta i(x)).
\]

By the Möbius inversion formula (and exchanging summation and limits by dominated convergence when \( f \) does not have bounded support), the latter equals

\[
\sum_{r = 1}^{\infty} \mu(r) \sum_{x \in \mathbb{O}^t \setminus \{0\}} \frac{p^{d(k)}}{|\mathbb{p}|} r^{n^2 mt} f(r \beta i(x)).
\]

The result now follows: first, note that we have for fixed \( r \in \mathbb{N} \) by approximation of the Riemann integral of \( f \) that

\[
\lim_{p \to \infty} \sum_{x \in \mathbb{O}^t \setminus \{0\}} (r \beta)^{n^2 mt} f(r \beta i(x)) = V^{-1} \int_{\mathbb{R}^{n^2 mt}} f(x)dx
\]

since \( \beta \to 0^+ \) as \( p \) becomes large. Moreover, by the second part of the non-degeneracy assumption the ratio \( \frac{|\mathbb{p}|}{|\mathbb{p}|} \to 1 \), so that \( \frac{p^{d(k)}}{|\mathbb{p}|} \) approaches \( \beta^{n^2 mt} \) as \( p \to \infty \). Finally, switching the limit in \( p \) and summation in \( r \) is allowed by dominated convergence, as \( f \) decays rapidly.

We now turn to examples of such a setup.

**Example 17:** In the case where \( n = 1 \) and \( \mathbb{O} \) is just the ring of integers \( \mathbb{O}_K \) of a number field \( K \), we can for example take \( \phi_p \) to be the reduction map modulo a prime \( p | \mathbb{O} \) for (the infinitely many) primes \( p \) that split completely in \( \mathbb{O}_K \). In this case, we get \( \mathbb{R}_p = \mathbb{F}_p \) and take \( U_p \) to be the complement in \( \mathbb{R}^t \) of \( \mathbb{F}_p \setminus \mathbb{F}_p^t \). With the usual definition of \( k \)-dimensional codes as free rank \( k \mathbb{F}_p \)-submodules of \( \mathbb{F}_p^t \), the balancedness condition is satisfied (see e.g., \([15, \text{Lemma } 1]\)), and moreover the non-degeneracy result is straightforward in this case: nonzero elements \( x \in \mathbb{O}_K \) have algebraic norm

\[
N_{\mathbb{O}_K / \mathbb{Q}}(x) \in \mathbb{P} \setminus \{0\},
\]

but the norm is just the product of the \( n \) embedded coordinates of \( i(x) \), so by the geometric/arithmetic mean inequality we obtain

\[
\|i(x)\| \gg p^{1/n}
\]

and non-degeneracy is satisfied. The condition on \( k \) in Theorem 16 simply becomes \( k > 0 \) and this recovers the construction of \([18]\) in the number field case.

**Example 18:** Let now \( n > 1 \) so that we are in the non-commutative situation. The most straightforward generalization to division algebras \( A \) with center \( K \) of the number field results is the following: consider primes \( p \mid \mathbb{O}_K \) that split \( A \). Let \( \mathbb{F}_p \cong \mathbb{O}_K/p \) denote the residue field. We then have an infinite family of ring isomorphisms

\[
\phi_p : \mathbb{O} / p\mathbb{O} \to M_n(\mathbb{F}_p)
\]

for a maximal order \( \mathbb{O} \) in \( A \). We take \( t \) copies of these to build our reduction map. In order to make sure the multiplicative structure is preserved as well, it makes sense to set \( \mathbb{R}_p := M_n(\mathbb{F}_p) \) and to consider codes which are free \( \mathbb{R}_p \)-submodules of \( \mathbb{R}_p^t \) of rank \( k \). It also seems natural to define \( U_p \) to be the complement in \( \mathbb{R}_p^t \) of

\[
\left( \mathbb{R}_p^t \setminus U_p \right) := ((M_n(\mathbb{F}_p) \setminus GL_n(\mathbb{F}_p))^t.
\]

It then follows that the \( U \)-balancedness condition is again satisfied (see the proof of \([18, \text{Lemma } 2]\)). We get a non-degeneracy result from Lemma 13: indeed we obtain for a nonzero vector \( a \in \mathbb{O}^t \) that maps to \( \mathbb{R}_p^t \setminus U_p \) the lower bound

\[
\|i(a)\| \gg q^{\frac{t}{n}}
\]

Moreover, as \( |GL_n(\mathbb{F}_p)| = \prod_{i=0}^{t-1}(q^n-q^i) \) we also have that \( \frac{|U_p|}{|\mathbb{R}_p^t|} \to 1 \) as \( p \to \infty \). Since the largest possible \( q \)-dimension of a code is \( n^2(t - 1) \), tracing through the definitions we have non-degeneracy exactly when \( t > n \), in which case via Theorem 16 we obtain the averaging result by pulling back codes which are free \( \mathbb{M}_n(\mathbb{F}_p) \)-modules of rank \( k \) for \( t > k > t - t/n \). In particular, when \( n = 2 \) we recover in the special case of the quaternion algebra \( A = \left( \mathbb{Q} \langle -1, -1 \rangle \right) \) the results of \([18, \text{Theorem } 3]\) for the Lipschitz integers as well as for the maximal order of Hurwitz integers. We note that we recover the condition \( k > t/2 \) appearing in \([18, \text{Theorem } 3]\). So this does give a generalization to arbitrary \( \mathbb{Q} \)-division algebras when \( t > n \), however it would be more convenient to obtain results that work for arbitrary \( t \geq 2 \).

In order to obtain averaging results that do not require the condition \( t > n \), one would have to obtain a stronger non-degeneracy lower bound on the norm or relax the condition that the codes be free \( \mathbb{M}_n(\mathbb{F}_p) \)-modules. Since the norm-trace inequality and the lower bound are sharp, we focus on the latter. However, when relaxing the definition of codes, one has to be careful to preserve the \( U \)-balancedness condition and to preserve enough multiplicative structure so that the units \( \mathbb{O}^\times \) act on the lattices and we obtain improved bounds on the packing density. This is achieved by taking as \( k \)-dimensional codes \( k \) copies of the simple left \( \mathbb{M}_n(\mathbb{F}_p) \)-module \( V = \mathbb{F}_p^n \) for \( n < k < t/n \). This carries enough structure through to the lattices in \( \mathbb{L}_p \) for the intended applications. Moreover, the \( U \)-balancedness result is a special case of the following, which we formulate in representation-theoretic terms:

**Lemma 19:** Let \( k \) be a 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

$$U = \{ v \in V \oplus n_3 \mid Ru \simeq V \oplus n_1 \}$$

$C_{n_2,n_3} = \{ C \subseteq V \oplus n_3 \mid C \text{ is an } R\text{-submodule, } C \simeq V \oplus n_2 \}$.

Assuming that $U$ is non-empty, for each $u \in U$ there is a bijection

$$\{ C \subseteq C_{n_2,n_3} \mid u \in C \} \rightarrow C_{n_2-n_1,n_3-n_1}$$

**Proof:** Observe that for any $u \in U$

$$u \in C \iff Ru \subseteq C \subseteq V \oplus n_3$$

$$\iff \frac{C}{Ru} \subseteq \frac{V \oplus n_3}{Ru} \simeq \frac{V \oplus (n_3-n_1)}{}.$$

Hence, if we identify $V \oplus n_3/Ru$ with $V \oplus (n_3-n_1)$, the proposed bijection is simply $C \mapsto C/Ru$.

**Corollary 20:** In the previous lemma, if $k$ is a finite field, then the number $\# \{ C \subseteq C_{n_2,n_3} \mid u \in C \}$ is independent of $u$.

Setting $R = M_n(F_q)$, $V = F_q^n$, $n_3 = nt$, $n_2 = k$ and $n_1 = n$, we deduce our $U$-balancedness condition. We summarize our results in this case as a consequence of Theorem 16 in easily accessible form:

**Theorem 21:** Let $A$ be a $\mathbb{Q}$-division algebra whose center is a number field $K$. Let $n = \sqrt{|A : K|}$ and $m = [K : \mathbb{Q}]$. Let $O$ be an order in $A$ and for an integer $t \geq 2$ we consider an infinite family of surjective reductions

$$\phi : O^t \rightarrow M_n(F_q)^t$$

as given in each coordinate by Lemma 9. Let $i : A^t \rightarrow (A \otimes \mathbb{Q} \mathbb{R})^t$ denote the coordinate-wise embedding and let $f : \mathbb{R}^{nt} \rightarrow \mathbb{R}$ be a semi-admissable function. For a fixed $n \leq k < nt$, set

$$C_{k,p} = \{ C \subseteq M_n(F_q)^{\oplus t} \mid C \cong (F_q^{\oplus k})^{\oplus k} \text{ as } M_n(F_q)\text{-module} \}$$

$$\mathbb{L}_{k,p} = \{ \beta_\phi \phi \cdot (C) \mid C \in C_{k,p} \},$$

where the constant $\beta_\phi$ normalizes the covolume of lattices in $\mathbb{L}_{k,p}$ to $V := \text{Vol}(O^t)$ is given by $\beta_\phi = q^{\frac{n_2-n_1}{2}}$. Then if $(n-1)t < k < nt$, we have that

$$\lim_{p \to \infty} \mathbb{E}_{L_{k,p}} \left( \sum_{x \in (\beta_\phi \phi \cdot (C))'} f(i(x)) \right) \leq \frac{\int_{\mathbb{R}^{nt}} f(x)dx}{\zeta (n^2 mt) \cdot V},$$

where the limit is taken over primes in the family and $(\beta_\phi \phi \cdot (C))'$ denotes the primitive vectors in $\beta_\phi \phi \cdot (C)$.

**Proof:** This readily follows from our discussions above as a special case of Theorem 16: indeed we set

$$U_p = \{ v \in M_n(F_q)^{\oplus t} \mid \dim_{F_q} (M_n(F_q)v) = n^2 \}.$$  

Moreover, we take $R_p = M_n(F_q)$ and the $U$-balancedness condition is satisfied by Corollary 20. Finally, the non-degeneracy condition is again satisfied as in Example 18, since if $a \in \mathcal{O}^{\oplus t} \setminus \{0\}$ is such that $\phi_p(a) \notin U_p$, then $a$ has to have one coordinate which is non-trivial and is a non-invertible matrix modulo $p$. Thus we obtain the bound in equation (14) and obtain non-degeneracy as before. Finally, the condition on $d(k)$ in Theorem 16 then just becomes $tn - t < k < tn$.

In particular, we obtain in this way a valid result as soon as $t \geq 2$.

**IV. IMPROVED BOUNDS**

Keeping the notation from the previous section, we now show how to leverage the extra symmetries under finite groups $G_0 \subseteq \mathcal{O}^\times$ of the lattices obtained in $\mathbb{L}_0$ in order to obtain sphere packings of density exceeding the Minkowski–Hlawka bound. We first present a result based on the approach in [18, Corollary 1] which in turn is inspired by Vance [11] and Rogers’ [8] work.

For a central $K$-division algebra $A$, we recall that $A_\mathbb{R}$ denotes the real vector space $A \otimes \mathbb{Q} \mathbb{R}$ of dimension $n^2 m$. We also recall that the space $A_\mathbb{R}$ is endowed with a norm coming from the quadratic form as defined in Equation 2 for some positive definite and symmetric $a \in A_\mathbb{R}$. Such a norm will be chosen and fixed permanently in Lemma 24.

Given a lattice $\Lambda \subseteq A_\mathbb{R}$, 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 $B_{A_\mathbb{R}}(r)$ of radius $r$ contains $k$ $A_\mathbb{R}$-linearly independent lattice vectors (under the $A_\mathbb{R}$-action on $A_\mathbb{R}$).

In particular, $\min_1(\Lambda)$ is the shortest vector length $\lambda_1(\Lambda)$ in $\Lambda$. We begin by remarking that a lemma of Minkowski [31] which was extended by Vance [11, Theorem 2.2] holds even more generally:

**Proposition 22:** Let $t \geq 2$ and $\Lambda$ denote an $O$-lattice in $A_\mathbb{R}$.

Then $\Lambda$ contains a left $A_\mathbb{R}$-module basis $\{ v_1, \ldots, v_t \}$ such that $\| v_i \| = \min_i(\Lambda)$. Moreover, if $\text{Vol}(\Lambda) = 1$, there exists an $O$-lattice of covolume one in $A_\mathbb{R}$ such that

$$\lambda_1(\Lambda) = \left( \prod_{i=1}^{t} \min_i(\Lambda) \right)^{1/t}.$$

**Proof:** Essentially the same proof goes through as in [11, Theorem 2.2] replacing $4$ by the appropriate dimension $mn^2$.

To proceed, we select

$$v_1 = \text{argmin}_{v \in A_\mathbb{R}\{0\}} \| i(v) \|$$

$$v_2 = \text{argmin}_{v \in A_\mathbb{R}v_1} \| i(v) \|$$

$$v_3 = \text{argmin}_{v \in A_\mathbb{R}(v_1 + A v_2)} \| i(v) \|$$

$$v_4 = \text{argmin}_{v \in A_\mathbb{R}(v_1 + A v_2 + A v_3)} \| i(v) \|$$

and we can argue inductively that they are linearly independent with respect to $A_\mathbb{R}$-action and satisfy $\| v_i \| = \min_i(\Lambda)$.

We now generate vectors $x_1, x_2, \ldots, x_k$ using a Gram-Schmidt process (see Appendix ) on $v_1, v_2, \ldots, v_k$. Since $\{ v_i \}_{i=1}^t$ is free with respect to left-$A_\mathbb{R}$ action, we get that $x_1, x_2, \ldots, x_k$ freely generate $A_\mathbb{R}$ as a left-$A_\mathbb{R}$ module.

Now consider the $R$-linear map given by

$$T : y \mapsto \frac{y_1}{\lambda_1} x_1 + \frac{y_2}{\lambda_2} x_2 + \cdots + \frac{y_k}{\lambda_k} x_k,$$

for $y = y_1 x_1 + y_2 x_2 + \cdots + y_k x_k \in A_\mathbb{R}$.
Define a lattice $\hat{\Lambda}$ by:

$$\hat{\Lambda} = (\lambda_1 \lambda_2 \ldots \lambda_k)^{1/k} T(\Lambda).$$

We observe that $\det(\hat{\Lambda}) = \det(\Lambda)$. For any $y' \in \hat{\Lambda} \setminus \{0\}$, we can now find $y = y_1 x_1 + \cdots + y_k x_k \in \Lambda$ such that $y' = (\lambda_1 \cdots \lambda_k)^{1/k} T(y)$. Furthermore, there must be a smallest $i_0 \geq 1$ such that $y_{i_0} \neq 0$ and $y_{i_0+1} = y_{i_0+2} = \cdots = y_k = 0$. Then $y \in \Lambda \cap (A_R v_1 + A_R v_2 + \cdots + A_R v_{i_0-1})$. Therefore $\|i(y')\| \geq \lambda_{i_0}$. This implies that

$$\|i(y')\|^2 = (\lambda_1 \lambda_2 \cdots \lambda_k)^{2/k} \sum_{i=1}^{i_0} \left| \frac{i(y_i)}{\lambda_i} \right|^2 \geq \lambda_{i_0} \left( \frac{1}{\lambda_{i_0}^2} \sum_{i=1}^{i_0} \|i(y_i)\|^2 \right) \geq \frac{(\lambda_1 \lambda_2 \cdots \lambda_k)^2}{\lambda_{i_0}^2},$$

using orthogonality as in Appendix. This lower bound is tight, since we can set $y_1 = 1_{K_0}$ and $y_i = 0$ for $i \geq 2$.

Remark 23: This version of Minkowski’s lemma given above is effective in the sense that for an explicit lattice $\Lambda$, the lattice $\hat{\Lambda}$ can also be computed algorithmically. The only important step here is to find the successive minima vectors $v_i$, and then $\hat{\Lambda}$ is easily seen to be computable.

When $A = \mathbb{Q}$ (so $A_R = \mathbb{R}$), finding the $v_i$ can be achieved by the so-called SLP algorithm, which will have an exponential running time of $O(2^{2^n})$. Details can be found in [32]. The division algebra case requires only slight modifications of the algorithm and should have a running time of $O(2^{2mn^2})$.

We also record the lemma:

**Lemma 24:** Let $\mathcal{O}$ denote an order in a $K$-division algebra $A$ and let $G_0 \subset \mathcal{O}^\times$ denote a finite group. Then $G_0$ acts on vectors in any $\mathcal{O}$-lattice $\Lambda \in \mathbb{L}_p$ obtained as in the construction of Theorem 16. Furthermore, we may choose a symmetric positive definite element $a \in A_R$ such that for all such $\Lambda$ the induced norm satisfies

$$\|i(x')\|^2 = \sum_{i=1}^{t} T(x_i^*ax_i) = \|i(g \cdot x')\|^2 \forall g \in G_0, x \in \Lambda.$$

**Proof:** The lattices obtained in $\mathbb{L}_p$ via our construction are easily seen to be preserved under the $\mathcal{O}$-action when the morphisms $\phi_p$ preserve the multiplicative structure and the codes in $C$ we are pulling back are $\phi_p(\mathcal{O})$-modules. Therefore the units act as well.

For the second part, we may set

$$a = \sum_{g \in G_0} g^*g.$$

One can easily check that the induced quadratic form then has the required $G_0$-invariance.

From now on, we may and will assume a norm as in Lemma 24 has been chosen on $A_R$. Using the methods from [8], [11], [18] we apply Theorem 16 to a specific function $f : \mathbb{R}^{mn^2t} \rightarrow \mathbb{R}$ in order to obtain improved bounds.

**Theorem 25:** Let $A$ be a central simple division algebra over a number field $K$. 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 $\Lambda$ in dimension $n^2mt$ achieving

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

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

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

which can be constructed. Indeed, $\Lambda_\varepsilon$ is obtained by applying Proposition 22 to a suitable sublattice of $\mathcal{O}^\times$ obtained as a pre-image via reduction modulo primes $p$ of $\mathcal{O}_K$ of large enough norm of a code isomorphic to $k$ copies of simple left $\mathcal{O}/p\mathcal{O}$-modules for $nt - t < k < nt$ as in Theorem 21.

**Proof:**

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

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

This function is indeed semi-admissible and we have that

$$\int_{\mathbb{R}^{mn^2t}} f_r(y) dy = V_{mn^2t} \cdot r^{mn^2t} \cdot e^{(1-e^{-t})},$$

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

$$V_{mn^2t} \cdot r^{mn^2t} \cdot e^{(1-e^{-t})} = (1 - \varepsilon) \cdot \frac{|G_0| \|\text{Vol}(\mathcal{O}^\times)\| \zeta(mn^2t)}{mn^2}.$$
From proposition 22 we deduce the (constructive) existence of a lattice $\Lambda$ with volume equal to $\text{Vol}(\Lambda)$ and shortest vector length $\lambda_1(\Lambda) > r$. We thus obtain for all such $\varepsilon$ the existence of a lattice $\hat{\Lambda}_\varepsilon$ of volume $\text{Vol}(O^t)$ and packing density

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

Letting $\varepsilon \to 0$, it thus also follows by Mahler compactness that the sequence $\hat{\Lambda}_\varepsilon$ has a converging subsequence (in the quotient topology on $\text{GL}_{mn^2t}(\mathbb{R})/\text{GL}_{mn^2t}(\mathbb{Z})$). Since the packing density is a continuous function with respect to this topology, we also get the existence of a lattice with density $\Delta(\hat{\Lambda}) \geq \frac{|G_0| \zeta(mn^2t) \cdot t}{2mn^2t \cdot (1 - e^{-t})}$.

**Remarks 26:**

1) First note that the zeta factor quickly approaches one as $n^2 mt$ increases and thus can be ignored for the purpose of giving asymptotic bounds for large dimensions.

2) The lower bounds on the density in Theorem 25 have the advantage of producing a factor $t$ in the numerator for lattices constructed from $O^t$. Via a simpler approach, taking $f$ to be the indicator function of a ball one finds an $O$-lattice $\Lambda$ which outperforms the bound above (slightly) only when $t = 2$. We record this below.

**Proposition 27:** With the notations of Theorem 25, there exists a $n^2 mt$-dimensional sub-lattice $\Lambda_\varepsilon \subset O^t$ with packing density

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

in the set of scaled pre-images of codes $\mathbb{L}_p$ for $p$ large enough. Moreover, there exists a $n^2 mt$-dimensional lattice $\Lambda$ with density $\Delta(\Lambda) \geq \frac{|G_0| \zeta(mn^2t) \cdot t}{2mn^2t}$ for all $t \geq 2$.

**Proof:** Take $f$ to be the indicator function of a ball of radius $r$ and let $r$ be chosen so that $\text{Vol}(B(r)) = (1 - \varepsilon)|G_0| \zeta(mn^2t) \text{Vol}(O^t)$. Applying Theorem 21, there must be for large enough $p$ a lattice $\Lambda_\varepsilon \subset \mathbb{L}_p$ (with the notations of the theorem) such that

$$|B(r) \cap \Lambda_\varepsilon| \leq (1 - \varepsilon)|G_0|.$$ 

Having arranged for $f$ to be $G_0$-invariant, the left hand side of (17) must be a multiple of $|G_0|$ and thus is forced to equal 0. This gives a lower bound on the shortest vector leading to the desired packing density for $\Lambda_\varepsilon$, while the second statement follows again by Mahler compactness.

Taking $t = 2$ is often the most advantageous in view of optimizing the packing density in relation to the dimension of the lattice. Nevertheless, having improved bounds for arbitrary $t \geq 2$ allows for more flexibility in terms of the parameters of the lattices and codes used (see also Table I and related notes).

Theorem 25 and Proposition 27 in particular recover the results of [13] such as those discussed in Section II-B for lattices obtained via lifts of codes. One of the main advantages of such constructive proofs is that, at least theoretically, dense lattices can then be explicitly found by searching a finite set of parameters. We conclude by a discussion of such effectiveness questions.

**V. Notes on Effectivity**

Our results such as Theorem 21 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 $(1 - \varepsilon) \frac{|G_0|}{2mn^2t}$ is found, with $G_0 < O^*$ designating the units of finite order in $O$.

**A. Varying the Division Ring**

We first focus on the case of $t = 2$ in Theorem 25 when in fact the better bounds are obtained by taking the simpler indicator function $f = 1_{B(0)}$ of a ball of appropriate radius as in Proposition 27.

**Theorem 28:** Let $A$ denote central simple division $K$-algebras for number fields $K$ and denote $[A : K] = n^2$ and $[K : \mathbb{Q}] = m$. Let $O$ denote a maximal order in such $A$. Fix $0 < \varepsilon < 1$. Assume the prime $p | q$ in $O_K$ is chosen large enough with respect to $m, n$ so that the size of the residue field $|O_K/p| = q$ satisfies:

1) we have as $m, n$ increase the relation:

$$n^2(m^2)^{2/(mn)^2}|G_0|^{1/2} < (q^{1/ln}),$$

2) the ratio

$$\frac{\text{Vol}(O^t)}{\text{Vol}(O)} < (1 + \varepsilon/3).$$

Then there exists an effective constant $C_\varepsilon > 0$ such that in dimension $2n^2m > C_\varepsilon$ there exists a lattice $\Lambda \subset \mathbb{L}_p$ with packing density

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

Here $\mathbb{L}_p$ denotes the set of scaled preimages of generalized codes of $F_p$-dimension $2n^2 - n$ via the reduction map $\phi_p : O^t \to (O/pO)^2$ as in Theorem 21.

**Proof:**

Tracing through the proof of Theorem 21 for $t = 2$ and $k = 2n - 1$ (the only sensible choice), we find that the term

$$\sum_{x \in (\phi_p^{-1}(C))'} f(3t(x))$$

is trivial for $f = 1_{B(r)}$ and some $C \subset C_{k,p}$ as soon as

$$r < \left(\frac{N(a)^{1/2n^2m}}{n\sqrt{m}}\right) q^{\frac{1}{2n^2}},$$

via Lemma 13 and (13), where $a = \sum_{g \in G_0} g^*g$. Since $N(g^*g) = 1$ for $g \in G_0$, it is easy to give a uniform lower bound $N(a)^{1/2n^2m} \geq 1$ or even $N(a)^{1/2n^2m} \geq \sqrt{|G_0|}$ by the Minkowski determinant inequality. In particular, it suffices to ensure the parameter $r$ satisfies

$$r < \left(\sqrt{m}\right) q^{\frac{1}{2n^2}}.$$ 

(19)
The expected value for the remaining terms for fixed characteristic \( p \) can then be seen by balancedness to be bounded by:

\[
E \leq \frac{q^{n(2n-1)}}{q^{2n^2} - (q^{n^2} - \prod_{i=0}^{n-1} (q^n - q^i))^2} \sum_{x \in (\mathcal{O}^2)^r} \mathbb{I}_{B(r)}(\beta_p(x)) \tag{20}
\]

Now by a classical geometry of numbers result (see [18, Lemma 4] or [23, Lemma 3.2]) we can bound

\[
\sum_{x \in (\mathcal{O}^2)^r} \mathbb{I}_{B(r)}(\beta_p(x)) \leq (r + \beta_p \tau(\mathcal{O}^2)^2) 2^{n^2 m} \frac{V_{2n^2 m}}{\beta_p 2^{n^2 m} \text{Vol}(\mathcal{O}^2)} \tag{21}
\]

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 \( S_n(q) := \frac{q^{n(2n-1)}}{q^{2n^2} - (q^{n^2} - \prod_{i=0}^{n-1} (q^n - q^i))^2} \beta_p 2^{n^2 m} \) we arrive at:

\[
E \leq \frac{S_n(q)}{\beta_p 2^{n^2 m}} 2^{n^2 m} \frac{V_{2n^2 m}}{\text{Vol}(\mathcal{O}^2)} \left( 1 + \frac{\tau(\mathcal{O}^2) \beta_p}{r} \right)^{2n^2 m} \tag{22}
\]

Observe now that

\[
S_n(q) = \frac{|M_{2n}(\mathbb{F}_q)|^2}{|M_n(\mathbb{F}_q)|^2} \frac{|M_n(\mathbb{F}_q)|^2}{|G_{m}(\mathbb{F}_q)|^2} \tag{21}
\]

so that we can assume \( q \) is large enough so that \( \frac{S_n(q)}{\beta_p 2^{n^2 m}} < (1 + \varepsilon/3) \).

Moreover, for a radius \( r \) that yields the density bound, we should have that the volume of the ball of radius \( r \) is around \( |G_0|(1 - \varepsilon) \text{Vol}(\mathcal{O}^2) \). By the Stirling formula, we may estimate as the dimension grows

\[
r \sim \frac{n \sqrt{m}}{\sqrt{2\pi}} (|G_0| \text{Vol}(\mathcal{O}^2))^{1/2n^2 m},
\]

which under our assumptions on \( q \) satisfies the inequality (19) using a trivial bound like \( |G_0| = o((n^2 m)^{nm}) \). It now suffices to show that under the parameters above, we can bound

\[
(1 + \frac{\tau(\mathcal{O}^2) \beta_p}{r})^{2n^2 m} < (1 + \varepsilon/3)
\]

for large enough dimension, since then we get from the inequality (22) the existence of a lattice in \( \mathbb{L}_p \) with the desired lower bound on the packing density. Recall that \( \beta_p = q^{-1/2n^2 m} \) with our parameters and we have from Lemma 14 that

\[
\tau(\mathcal{O}^2) / r = \sqrt{2} \cdot \tau(\mathcal{O}) \leq \text{Vol}(\mathcal{O})^{1/2n^2 m} \cdot (n \sqrt{m} + 6) / (\sqrt{2\pi}).
\]

We thus have

\[
\frac{\tau(\mathcal{O}^2) \beta_p}{r} \leq \text{Vol}(\mathcal{O})^{1/2n^2 m} |G_0|^{1/2n^2 m} q^{-1/2n^2 m}.
\]

But under the assumptions of the theorem on \( q \), the result now follows since as \( mn^2 \) goes to infinity the term \( 2n^2 m \cdot \tau(\mathcal{O}^2) \beta_p \) becomes arbitrarily small. Assuming \( p \) and \( q \) chosen large enough for each \( n, m \) as in the assumptions of the theorem, we may thus view \( (1 + \frac{\tau(\mathcal{O}^2) \beta_p}{r})^{2n^2 m} \) as a function in \( n, m \) which approaches 1 for large enough dimension \( n^2 m \). This easily yields an effective constant \( C_\varepsilon \) guaranteeing

\[
(1 + \frac{\tau(\mathcal{O}^2) \beta_p}{r})^{2n^2 m} < (1 + \varepsilon/3)
\]

for \( n^2 m > C_\varepsilon \).

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 ([19]). Moreover, the computation of the volume \( \text{Vol}(\mathcal{O}) \) 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 \( \{ \det(tr_{\mathcal{O}/\mathcal{O}} \mathfrak{a} \mathfrak{b}) \mid \mathfrak{a}, \mathfrak{b} \leq A \} \) for \( \mathfrak{a}, \mathfrak{b} \in \mathcal{O} \) a \( \mathbb{Z} \)-basis. Equivalently it is the norm of the \( \mathbb{Q} \)-algebra different \( N_{A/\mathcal{O}}(\mathcal{O}(\mathcal{O}/\mathbb{Z})) \). We may then write ([27, Ex 25.1]):

\[
d(\mathcal{O}/\mathbb{Z}) = N_{K/\mathbb{Q}}(d(\mathcal{O}/\mathcal{O})) \cdot d(\mathcal{O}/\mathcal{K}/\mathbb{Z})^n,
\]

where \( d(\mathcal{O}/\mathcal{K}) \) is just the regular discriminant of the central simple \( K \)-algebra \( A \) and \( d(\mathcal{O}/\mathcal{K}/\mathbb{Z}) \) is the discriminant of the central number field. In particular, when there is some control of the ramification behavior of \( A/K \) and we have some upper bounds for the discriminant of \( K \), the conditions of Theorem 28 become entirely explicit.

Example 29: When \( K = \mathbb{Q}(\zeta_m) \) is a cyclotomic field, one has that

\[
d(\mathcal{O}/\mathcal{K}/\mathbb{Z}) = \prod_{l \mid p} l^{\varphi(m)/((l - 1)/l)}. \tag{23}
\]

When \( n = 1 \), by considering cyclotomic fields \( \mathbb{Q}(\zeta_m) \) Moustrou thus finds via a version of Theorem 28 in this case 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 [23, Theorem 1, Prop 3.1].

Example 30: Similarly, fixing \( n = 2 \), varying \( K = \mathbb{Q}(\zeta_m) \) and considering the quaternion algebra over \( K \)

\[
A = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}
\]

when 2 has odd order modulo \( m \), we can use that \( d(\mathcal{O}/\mathcal{K}/\mathbb{Z}) \leq m^\varphi(m) \) and that the discriminant of the Hurwitz integers \( d(\mathcal{H}/\mathbb{Z}) = 2 \) to obtain an effective version of Proposition 6 via Theorem 28. We record this below.

Proposition 31: Let \( m_k = \prod_{p \mid k} p \) prime \( p \) and set \( n_k := 8\varphi(m_k) \). Then for any \( \varepsilon > 0 \) there is an effective constant \( c_\varepsilon \) such that for \( k > c_\varepsilon \) a lattice \( A \) in dimension \( n_k \) with density

\[
\Delta(A) \geq (1 - \varepsilon) \frac{24 \cdot m_k}{2n_k}
\]

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

\[
\Delta(A) \geq (1 - e^{-n_k}) \frac{3 \cdot n_k \log \log n_k}{24} \tag{24}
\]

dimension \( n_k \).

Proof: We consider the quaternion algebras \( A_k = \left( \frac{-1, -1}{\mathbb{Z}} \right) \) and exhibit a large enough residue field size \( q \) so that the conditions of Theorem 28 are satisfied. From the discriminant relation (23) we obtain that the first condition amounts to

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

It is convenient to as in [23, Prop 3.1] search for large primes which split completely in \( \mathbb{Q}(\zeta_{m_k}) \), and this happens
When $p \equiv 1 \mod m_k$, using an effective version of the \v Cebotarev density theorem (see e.g., [33]), one sees that an interval of size, say, $(1/m_k)(m_k)^6\varphi(m_k)$ must contain such a prime for large enough $m_k$. Such a prime then satisfies $(m_k\varphi(m_k)^2)^2\varphi(m_k) = o(p)$ for our choice of $m_k$. Finding a suitable prime $p$ can thus be done in at most around $e^{3/4n_k\log n_k}$ steps. Moreover, for such primes, we have that

$$\left|\frac{M_2(F_p)}{\left|M_2(F_p)\right|^2 - \left|M_2(F_p)\right| \cdot \text{GL}_2(F_p)\right| - 1\right| = o(e^{-n_k}),$$

which deals with the second condition of Theorem 28. The time estimate for enumerating the lattice family is then of $e^{1.5\cdot n_k\log(n_k)(1+o(1))}$ binary operations since the number of codes we consider in Theorem 28 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. We thus obtain an effective version of the bounds in Proposition 6, as claimed.

The density lower bounds above outperform the best known effective lower bounds on the density from cyclotomic fields

$$\text{Vol}(B(r)) = (1 - \varepsilon)\frac{2^t\text{Vol}(\mathcal{H}) \cdot \zeta(4t)}{e^{1-e^{-t}}},$$

(see also [13, Fig. 1]).

**Example 32:** Consider the case when $k = 2$ and $m_k = 7 \cdot 23 = 161$. A suitable prime $p$ is then for instance

$$p = (161 \cdot \varphi(161)^2)^2\varphi(161) + 223147$$

of size about $10^{1072}$ and satisfying $p \equiv 1 \mod 161$. Using this prime in Theorem 28 yields a lattice $\Lambda$ in $8 \cdot \varphi(161) = 1056$ dimensions such that

$$\Delta(\Lambda) \geq (1 - \varepsilon)\frac{3864}{21056},$$

for $\varepsilon \leq 10^{-1000}$ in about $10^{10^8}$ bit-operations. Even with the best computers, it is currently far out of reach to enumerate a basis for such a lattice. Nevertheless, this gives a very explicit construction of such a random lattice that achieves a good packing.

Finally, we note that similarly an effective version of Proposition 7 can be obtained. It seems plausible for such results that as long as only the degree of the center of the division algebras over $\mathbb{Q}$ is unbounded as in Proposition 31, the family size of $n$-dimensional lattices to be searched should be $e^{C \cdot n \log(n)(1+o(1))}$ for some constant $C > 0$.

**B. 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 [11]. 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 33:** 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

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

where $r$ is defined by $\text{Vol}(B(r)) = (1 - \varepsilon)\frac{2^{t}\text{Vol}(\mathcal{H}) \cdot \zeta(4t)}{e^{1-e^{-t}}}$, and which, provided the odd prime $p$ satisfies $t^2 = o(p)$ and $t$ is large enough, lies in the set of (rescaled) lifts

$$L_p = \{\phi_p^{-1}(C) : C \in \mathcal{C}_{t+1}\},$$

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

**Proof:** Consider the proof of Theorem 25. 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

$$\text{Vol}(B(r)) = (1 - \varepsilon)\frac{2^{t}\text{Vol}(\mathcal{H}) \cdot \zeta(4t)}{e^{1-e^{-t}}}$$

(24)

Via Stirling’s formula, we get from (24) and the discriminant $d(\mathcal{H}) = 2$ the asymptotic

$$r \sim t^{1/(4t) + 1/2} \cdot \frac{2^{5/8}}{\sqrt{\pi t}}.$$  

(25)

First consider any $t < k < 2t$. Pulling back codes of $F_t$-dimension $2k$ as in Theorem 21, 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

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

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 16 (and ignoring for simplicity the Möbius inversion step since the zeta factor quickly approaches 1 for large $t$), we have that

$$\mathbb{E} \leq \frac{p^{d(k)}}{|U_p|} \cdot \frac{\beta_{p}^{4t}}{\beta_{p}^{4t}} \cdot \sum_{x \in \mathcal{O} \setminus \{0\}} \beta_{p}^{4t} f_r(\beta_{p} x)$$

$$= \frac{p^{4t}}{p^{4t}} \cdot \frac{\beta_{p}^{4t}}{\beta_{p}^{4t}} \cdot \sum_{x \in \mathcal{O} \setminus \{0\}} \beta_{p}^{4t} f_r(\beta_{p} x)$$

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

$$\Delta(p,t) = \beta_{p}^{4t} \cdot \sum_{x \in \mathcal{O} \setminus \{0\}} f_r(\beta_{p} x) - V^{-1} \int_{R_{4t}} f_r(x) dx$$  

(26)

recalling here that $f_r$ is the radial function given by

$$f_r(y) = \begin{cases} \frac{1}{e^{r \log(y/r)}} & \text{if } 0 \leq \|y\| \leq r & \left(1-1/e^r\right)4t \\ 0 & \text{if } r \\ & \leq \|y\| \leq r & \left(1-1/e^r\right)4t \\ & \text{else.} \\ \end{cases}$$

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
We note that in particular $f_r$ has derivative bounded by $C_r = e^{1/4}/r$. Tiling the support of $f_r$ by Voronoi cells of diameter the packing radius $\tau(\beta O^4)$, we can bound the error in approximating the Riemann integral via the lattice sum on each individual cell by $\Vol(O^4)/\beta^4 \cdot C_r \cdot 2\tau(\beta O^4)$. For large enough $p, t$, we may estimate that the support of $f_r$ is covered by $\beta^{-4t}e^{-\Vol(B(r))/\Vol(O^4)}$ cells (with an error that is $o(\Vol(O^4))$ as $t \to \infty$), so that we arrive at the total error estimate

$$
\Delta(p, t) \leq 2eC_r \cdot \beta_p \Vol(B(r)) \Vol(O^4) \cdot \sqrt{t} \cdot \tau(O) \tag{27}
$$

We therefore obtain for $r$ satisfying (24) the bound as $p, t$ become large of

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

It now seems most convenient to take $k = t + 1$ and we see that in particular the condition $t^2 = o(p)$ suffices to guarantee for any given $\varepsilon > 0$ that $\Delta(p, t) < \varepsilon$ for large enough rank $t$. We have thus shown that for any $\varepsilon$ we can find $t$ large enough so that under our assumptions on $p$ there exists $\Lambda \in \mathbb{L}_p$ with $\sum_{j \in \Lambda} f_r(\gamma) \leq (1 - \varepsilon) \cdot 6$. The result now follows as in the proof of Theorem 25.

We therefore conclude:

**Corollary 34**: Given any $0 < \varepsilon < 1$, for large enough $t$ a lattice $\Lambda$ in dimension $4t$ whose packing density satisfies

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

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

**Proof**: Given $\varepsilon$ and large enough $t$, it is easy to find a large enough prime $p$ so that the construction of Proposition 33 applies. The corresponding family of lattices has $|c_{t+1}|$ elements in Proposition 33’s notation. They are generated by vectors with coefficients polynomial in $t$. The cost of computing their density or shortest vector as well as of computing their successive quaternionic minima (see remark 23) is thus small compared to the cost of enumerating the family and we find by applying the effective version of 22 the desired lattice.

In conclusion, we provide in Table I for the reader’s convenience a comparison of the parameters of various effective constructions of dense lattices in terms of rank of the lattice, code parameters, alphabet size and log of the family size, expanding on [18, Table 1]. We note that this is neither an exhaustive list of the constructions in the literature nor of the constructions that can be achieved from lifting codes to division rings.

## APPENDIX

### GRAM–SCHMIDT PROCESS FOR REAL SEMISIMPLE ALGEBRAS WITH POSITIVE INVOLUTIONS

Let $A$ be a real semisimple algebra and let $(\cdot)^* : A \to A$ be a positive involution.

**Orthogonality in $A_k$**

Let $k \geq 1$. Fix a positive definite symmetric element $a \in A$. Let us define

$$
\langle x, y \rangle A : A^k \times A^k \to A,
$$

$$
\langle x, y \rangle A = \sum_{i=1}^{k} x_i a y_i^*.
$$

This form is $\mathbb{R}$-bilinear but not necessarily $A$-bilinear, since $A$ may not be commutative. We can however define a real positive definite symmetric bilinear form on $A_k$ given by

$$
\langle x, y \rangle = \mathbb{T}(\langle x, y \rangle A).
$$

We assume that $A_k$ carries this real inner product.

**Lemma 35**: The following properties are satisfied by $\langle \cdot, \cdot \rangle_A$.

1. For $x, y \in A^k$, we have

$$
\langle x, y \rangle_A = \langle y, x \rangle_A.
$$

2. For $x \in A^k \setminus \{0\}$, $\langle x, x \rangle_A$ is a symmetric and positive definite in $A$, and hence is a unit in $A$.

3. For $x, y \in A^k$ and $\alpha \in A$, we have

$$
\langle \alpha x, y \rangle_A = \alpha \langle x, y \rangle_A,
$$

$$
\langle x, \alpha y \rangle_A = \langle x, y \rangle_A \alpha^*.
$$

4. Suppose $x \in A^k \setminus \{0\}$. Then there exists some $b \in A$ such that $\langle bx, bx \rangle = 1_A$.

**Proof**: All of them are trivial verifications. For the last one, we must find a $b \in A$ such that $\langle x, x \rangle_A^{-1} = b^*b$. See [13, Corollary 46].

**Definition 36**: We say two vectors in $A^k$ are orthogonal if the above given product between them is 0. We call a set of
vectors \( \{x_1, x_2, \cdots, x_m\} \in A^k \) orthonormal if \( \langle x_i, x_j \rangle_A = \delta_{ij} 1_A. \)

Note that if \( \langle x, y \rangle = 0 \), then \( \langle \alpha_1 x_1, \alpha_2 y \rangle = 0 \) for each \( \alpha_1, \alpha_2 \in A \) and \( x, y \in A^k. \)

**Proposition 37:** Suppose \( x_1, x_2, \cdots, x_m \in A^k \) is an orthonormal set of vectors. Then \( m \leq k \) and \( x_1, x_2, \cdots, x_m \) are free under the left action of \( A. \) If \( m = k \), then the vectors \( x_1, \cdots, x_k \) freely generate \( A^k \) as a left \( A \)-module.

**Proof:** Observe that if \( a_1, a_2, \cdots, a_m \in A \) are such that

\[
 a_1 x_1 + a_2 x_2 + \cdots + a_m x_m = 0,
\]

then we can just evaluate

\[
 \langle a_1 x_1 + a_2 x_2 + \cdots + a_m x_m, x_i \rangle = a_i \langle x_i, x_i \rangle = a_i 1_A = 0.
\]

Hence, we have that each \( a_i = 0 \). Using this, we get that

\[
 A^m \rightarrow A^k
\]

\[
 (a_1, a_2, \cdots, a_m) \mapsto a_1 x_1 + \cdots + a_m x_m.
\]

is an injective \( \mathbb{R} \)-linear map. Hence, for dimensional constraints, \( m \leq k \) and \( m = k \) will imply that it is an isomorphism.

**Remark 38:** If we were to define

\[
 \langle \cdot, \cdot \rangle_A : A^k \times A^k \rightarrow A
\]

\[
 \langle x, y \rangle = \sum_{i=1}^{k} x_i^* y_i,
\]

we would reach the same proposition above, but for right actions instead of left.

**Corollary 39:** Suppose \( x_1, x_2, \cdots, x_k \in A^k \) is an orthonormal set of vectors. Then for any \( v = a_1 x_1 + a_2 x_2 + \cdots + a_k x_k \) for \( \{a_i\}_{i=1}^k \subseteq A \), we have

\[
 (v, v)_A = T((v, v)_A) = \sum_{i=1}^{k} T(a_i^* a_i),
\]

**Gram-Schmidt Algorithm**

The following algorithm is an analogue of Gram-Schmidt. Suppose \( v_1, v_2, \cdots, v_k \in A^k \) are some vectors that freely generate \( A^k \) as a left \( A \)-module. We claim that using these vectors, it is possible to create a set of orthonormalized basis vectors \( x_1, x_2, \cdots, x_k \).

First, we do the following. Define for \( u, v \in A^k \),

\[
 \text{proj}(u, v) = \begin{cases} 
 (u, v)_A (u, u)_A^{-1} u & \text{if } u \neq 0 \\
 0 & \text{if } u = 0.
\end{cases}
\]

This has the property that \( \langle \text{proj}(u, v), u \rangle_A = (v, v)_A \).

Generate vectors \( x_1', x_2', \cdots, x_k' \) as follows.

\[
 x_1' = v_1,
\]

\[
 x_2' = v_2 - \text{proj}(x_1', v_2)
\]

\[
 x_3' = v_3 - \text{proj}(x_1', v_3) - \text{proj}(x_2', v_3)
\]

\[
 x_i' = v_i - \text{proj}(x_1', v_i) - \text{proj}(x_2', v_i) - \text{proj}(x_3', v_i)
\]

We can prove that \( (x_i', x_j') = 0 \) for \( i > j \) by first induction via ordering \((i, j)\) as \((2, 1), (3, 1), \cdots, (k, 1), (2, 2), (4, 2), \cdots, (k, 2), (4, 3), \cdots \) Now choose \( b_i \) such that \( x_i = b_i x_i' \) has \( \langle x_i, x_j \rangle = 1_A. \) Hence, we are done.

**Definition 40:** Given a real semisimple algebra \( A \) with a positive involution \( (\cdot)^* \), we call the above method of generating \( x_1, x_2, \cdots, x_m \) from vectors \( v_1, v_2, \cdots, v_m \) the Gram-Schmidt algorithm. If \( \{v_j\}_{j=1}^m \) are free under left \( A \) multiplication, then so are \( \{x_i\}_{i=1}^m \).

**Acknowledgment**

The authors would like to thank Gauthier Leterrier, Martin Stoller, and Maryna Viazovska for helpful conversations on the topics of this article. They would also like to thank Matthew De Courcy-Ireland for insightful comments on a previous version of this manuscript. Finally, they thank the referees for valuable suggestions that helped us improve the article.

**References**

[1] J. Conway and N. Sloane, *Sphere Packings, Lattices, and Groups* (Grundlehren der Mathematischen Wissenschaften), vol. 290. Cham, Switzerland: Springer, 1988.

[2] H. Cohn and A. Kumar, ”Optimality and uniqueness of the Leech lattice among lattices,” *Ann. Math.*, vol. 170, no. 3, pp. 1003–1050, Nov. 2009.

[3] T. C. Hales, ”A proof of the Kepler conjecture,” *Ann. Math.*, vol. 162, pp. 1063–1143, 2005.

[4] M. S. Viazovska, ”The sphere packing problem in dimension,” *Ann. Math.*, vol. 185, no. 3, pp. 991–1015, 2017. [Online]. Available: http://eudml.org/doc/26395748

[5] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska, ”The sphere packing problem in dimension 24,” *Ann. Math.*, vol. 185, no. 3, pp. 1017–1033, May 2017. [Online]. Available: http://arxiv.org/abs/2001.00242

[6] H. Cohn, ”A conceptual breakthrough in sphere packing,” *Notices Amer. Math. Soc.*, vol. 64, no. 2, pp. 102–115, Feb. 2017.

[7] E. Hlawka, ”Zur Geometrie der Zahlen,” *Math. Zeitschrift*, vol. 49, no. 1, pp. 285–312, Dec. 1943. [Online]. Available: http://eudml.org/doc/169025

[8] C. A. Rogers, ”Existence theorems in the geometry of numbers,” *Ann. Math.*, vol. 48, no. 4, pp. 994–1002, 1947.

[9] H. Cohn and C. A. Rogers, ”Hlawka’s theorem in the geometry of numbers,” *Duke Math. J.*, vol. 14, no. 2, pp. 367–375, Jun. 1947.

[10] K. Ball, ”A lower bound for the optimal density of lattice packings,” *Int. Math. Res. Not. IMRN*, vol. 1992, no. 10, pp. 217–221, 1992. doi: 10.1155/1992/217

[11] S. Vance, ”Improved sphere packing lower bounds from Hurwitz lattices,” *Adv. Math.*, vol. 227, no. 5, pp. 2144–2156, Aug. 2011.

[12] A. Venkatesh, ”A note on sphere packings in high dimension,” *Int. Math. Res. Notices*, vol. 2013, no. 7, pp. 1628–1642, 2013. doi: 10.1093/imrn/rns096.

[13] N. P. Gargava, ”Lattice packings through division algebras,” 2021, arXiv:2107.04844.

[14] C.-L. Siegel, ”A mean value theorem in geometry of numbers,” *Ann. Math.*, vol. 46, no. 2, pp. 340–347, Apr. 1944.

[15] H.-A. Loeliger, ”Averaging bounds for lattices and linear codes,” *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1767–1773, Nov. 1997.

[16] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska, ”Universal optimality of the E8 and Leech lattices and interpolation formulas,” *Ann. Math.*, vol. 196, no. 3, pp. 983–1082, 2022. doi: 10.4007/annals.2022.196.3.3

[17] S. N. Litsyn and M. A. Tsfasman, ”Constructive high-dimensional sphere packings,” *Duke Math. J.*, vol. 54, no. 1, pp. 147–161, Jan. 1987.

[18] A. Campbell, ”Random ensembles of lattices from generalized reductions,” *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 5211–5239, Jul. 2018.

[19] S. A. Amitsur, ”Finite subgroups of division rings,” *Trans. Amer. Math. Soc.*, vol. 80, no. 2, pp. 361–386, 1955.

[20] J. A. Rush, ”A lower bound on packing density,” *Invent. Math.*, vol. 98, no. 3, pp. 499–510, 1989. [Online]. Available: http://eudml.org/doc/143740
[21] J. A. Rush and N. J. A. Sloane, “An improvement to the Minkowski–Hiawka bound for packing superballs,” *Mathematika*, vol. 34, no. 1, pp. 8–18, Jun. 1987.

[22] P. Gaborit and G. Zémor, “On the construction of dense lattices with a given automorphisms group,” *Ann. Inst. Fourier*, vol. 57, no. 4, pp. 1051–1062, 2007. [Online]. Available: http://eudml.org/doc/10250

[23] P. Moustrou, “On the density of cyclotomic lattices constructed from codes,” *Int. J. Number Theory*, vol. 13, no. 5, pp. 1261–1274, 2017.

[24] G. Berhuy and F. Oggier, *An Introduction to Central Simple Algebras and Their Applications to Wireless Communication*. Providence, RI, USA: American Mathematical Society, 2013.

[25] F. Oggier and J. Ducoat, “On skew polynomial codes and lattices from quotients of cyclic division algebras,” *Adv. Math. Commun.*, vol. 10, no. 1, pp. 79–94, Mar. 2016.

[26] R. Vehkalahti and L. Luzzi, “The DMT of real and quaternionic lattice codes and DMT classification of division algebra codes,” *IEEE Trans. Inf. Theory*, vol. 68, no. 5, pp. 2999–3013, May 2022.

[27] I. Reiner, *Maximal Orders* (London Mathematical Society Monographs). Oxford, U.K.: Clarendon Press, 2003. [Online]. Available: https://books.google.ch/books?id=0liBQgAACAAJ

[28] E. B. Fluckiger, “Upper bounds for Euclidean minima of algebraic number fields,” *J. Number Theory*, vol. 121, no. 2, pp. 305–323, Dec. 2006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022314X0600062X

[29] S. D. Miller and N. Stephens-Davidowitz, “Kissing numbers and transference theorems from generalized tail bounds,” *SIAM J. Discrete Math.*, vol. 33, no. 3, pp. 1313–1325, Jan. 2019.

[30] W. Banaszczyk, “New bounds in some transference theorems in the geometry of numbers,” *Math. Ann.*, vol. 296, no. 4, pp. 625–636, 1993. [Online]. Available: http://eudml.org/doc/165105

[31] H. Minkowski, *Geometrie der Zahlen*. Sonnewalde, Germany: Benedictus Gotthelf Teubner, 1910. [Online]. Available: https://books.google.ch/books?id=MasGAAAAAYAAJ

[32] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective* (The Springer International Series in Engineering and Computer Science), vol. 671. Cham, Switzerland: Springer, 2002.

[33] J. Thorner and A. Zaman, “A unified and improved Chebotarev density theorem,” *Algebra Number Theory*, vol. 13, no. 5, pp. 1039–1068, Jul. 2019.

Nihar Gargava received the bachelor’s degree in mathematics from the Indian Institute of Technology Kanpur in 2017 and the master’s degree from the École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, in 2019, where he is currently pursuing the Ph.D. degree with the Chair of Number Theory. His master’s thesis was titled “Asymptotic Bounds on Error-Correcting Codes.” He is also a Researcher at the Error-Correction Division, Quantumurn, Cambridge. His research interests include number theory, sphere packings, error-correcting codes, and quantum computing.

Vlad Serban received the Ph.D. degree from Northwestern University in 2016. He was a Post-Doctoral Researcher at The Fields Institute for Research in Mathematical Sciences, Toronto, in 2017. From 2017 to 2019, he was a Post-Doctoral Researcher at the University of Vienna. He is currently a Post-Doctoral Assistant at the Chair of Number Theory, Institute of Mathematics, École Polytechnique Fédérale de Lausanne (EPFL). He is an algebraic number theorist by training and interested in the Langlands program as well as in applying ideas from arithmetic to optimization problems, such as the sphere packing problem and related questions in coding theory and cryptography.