Abstract. A Gilbert-Varshamov-type bound for Euclidean packings was recently found by Nebe and Xing. In this present paper, we derive a Gilbert-Varshamov-type bound for lattice packings by generalizing Rush’s approach of combining $p$-ary codes with the lattice $p\mathbb{Z}^n$. Specifically, we will exploit suitable sublattices of $\mathbb{Z}^n$ as well as lattices of number fields in our construction. Our approach allows us to compute the center densities of lattices of moderately large dimensions which compare favorably with the best known densities given in the literature as well as the densities derived directly via Rush’s method.

1. Introduction

The classical problem of packing balls densely and uniformly in an $n$-dimensional Euclidean space has baffled numerous mathematicians for centuries. Recall that a ball in an $n$-dimensional Euclidean space $\mathbb{R}^n$ refers to the set of points in $\mathbb{R}^n$ whose Euclidean distance from a given point does not exceed a fixed positive real number $r$. Indeed, apart from its inherent mathematical and geometric appeal, such dense packings as well as their related problems have found useful applications in diverse fields, such as engineering, astronomy and physics, just to name a few. Though many beautiful discoveries surrounding this fascinating subject have been made over the years, there remains a wide spectra of open unsolved problems continue to inspire active research among the different mathematical disciplines. We refer interested readers to the books of Cassels [1], Rogers [6] and Conway and Sloane [2] for background reading and developments in this topic.

A particularly useful class of packings is the so-called lattice packings in which the centers of the balls form a discrete additive group (or lattice) in $\mathbb{R}^n$. In order for any packing to be meaningful, it is necessary for the minimum distance between any two points of the lattice to be positive so that balls with diameters equal to this distance can be packed together without any overlaps.

2000 Mathematics Subject Classification: 05B40 11H31, 52C17, 11H71.

The first author is partially supported by Singapore MOE-ARF Tier 2 research grant T208B2206.

Date of initial submission: Jan 17, 2009.

The first author is the corresponding author.
We can then define a quantity to measure the density of the packing as the proportion of the space filled up by these balls. More specifically, let $\mathcal{L}$ be the lattice of points representing the centers of the balls. If $d(x, y)$ denotes the Euclidean distance between any two points $x, y \in \mathbb{R}^n$, then the minimum distance of the lattice $\mathcal{L}$ is defined as

$$d(\mathcal{L}) = \inf_{x, y \in \mathcal{L}, x \neq y} d(x, y).$$

Thus, the density of $\mathcal{L}$, denoted by $\Delta(\mathcal{L})$, is given by

$$\Delta(\mathcal{L}) = \frac{(d(\mathcal{L})/2)^n V_n}{\det(\mathcal{L})},$$

where $V_n$ is the volume of a ball of radius 1 and $\det(\mathcal{L})$ is the determinant of $\mathcal{L}$ or the volume of the fundamental domain of $\mathcal{L}$. Similarly, we often consider the center density of $\mathcal{L}$, denoted by $\delta(\mathcal{L})$, that measures the average number of points in a fundamental domain, that is, $\delta(\mathcal{L}) = \Delta(\mathcal{L}) / V_n$.

For any positive integer $n$, we are interested in the maximum density (respectively center density) that can possibly be achieved by some lattice. We will write $\Delta_n$ (respectively $\delta_n$) to represent these respective quantities. For small values of $n$, say $n \leq 9$ and $n = 24$, $\Delta_n$ is explicitly known (refer to [2]) but as $n$ increases, only general upper and lower bounds on $\Delta_n$ are presently available. For instance, the celebrated Minkowski bound, which is often quoted as the benchmark for good lattices, states that

$$\lim_{n \to \infty} \frac{\log_2 \Delta_n}{n} \geq -1.$$  

However, this bound is an existence bound and it remains an interesting problem to construct families of explicit lattices that attain this bound. In fact, if $n$ is large, it is difficult to construct lattices with good densities.

Due to the many similarities between error-correcting codes and lattices, it is not surprising that a great number of results in lattice packings are inspired by corresponding results from its counterpart, and vice versa. For example, the Leech and Sloane’s “construction A” concatenates binary codes and standard lattices to produce new lattices (refer to [2]). In [7], Rush extended this approach to non-binary codes via an equivalent distance-metric in the vector space $\mathbb{F}_p^n$ for some odd prime $p$, thereby exhibiting an explicit (though computationally infeasible) method to construct a family of lattices achieving the Minkowski bound asymptotically. In [5], the authors built on these ideas and based on a restricted family of double circulant codes, they presented a family of lattice packings which achieve, up to a multiplicative constant, the best known densities of at least $cn2^{-n}$.

In this paper, we generalize Rush’s approach to concatenate codes with arbitrary sublattices of $\mathbb{Z}^n$. We further apply the construction to sublattices of $O_K^n$, where $O_K$ is the ring of integers in an imaginary quadratic field $K$. 
Based on the determination of the Gilbert-Varshamov bound for linear codes, we derive an analogous bound for our construction.

This paper is organized as follows. In the next section, we will describe our main construction and obtain a Gilbert-Varshamov-type bound for the center densities of lattices. We then consider two specific examples in Section 3, and we derive an analogous bound for our construction. Based on the determination of the Gilbert-Varshamov bound for linear codes, we will compare favorably with the center densities given in [2] as well as those derived from Rush’s bound.

2. THE GENERAL CONSTRUCTION

First, we introduce some notations which will be useful in the following construction.

Let $\mathcal{L} \subseteq \mathbb{Z}^n$ be a lattice of rank $n$. Note that $\mathbb{Z}^n / \mathcal{L}$ is a finite abelian group and we denote its order by $\det(\mathcal{L})$, the determinant of $\mathcal{L}$. Denote by $B_{\mathcal{L}}^n(d)$ the ball of radius $\sqrt{d}$ centered at the origin, that is, $B_{\mathcal{L}}^n(d) = \{ \mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{L} : ||\mathbf{x}||^2 = \sum_{i=1}^n x_i^2 \leq d \}$. We will denote the theta series for a lattice $\mathcal{L}$ (see [2]), we have the following obvious formula for $B_{\mathcal{L}}^n(d)$.

**Lemma 2.1.** Let $\theta_{\mathcal{L}}(x) = \sum_{i=0}^{\infty} A_i x^i$ be the theta series for a lattice $\mathcal{L} \subseteq \mathbb{Z}^n$. Then $B_{\mathcal{L}}^n(d) = \sum_{i=0}^{d} A_i$.

For an odd prime $p$, we identify the Galois field $\mathbb{F}_p$ with the set $\mathcal{P} = \{0, \pm 1, \pm 2, \ldots, \pm (p - 1)/2\}$. Given any integer $a$, let $a \langle p \rangle$ be the representative in $\mathcal{P}$ for the equivalence class of $a$. Thus, $|a \langle p \rangle| \leq |a|$ for any $a \in \mathbb{Z}$. Similarly, for a vector $\mathbf{x} \in \mathbb{Z}^n, \mathbf{x} \langle p \rangle$ will denote the vector in which all the components are reduced modulo $p$ to elements in $\mathcal{P}$. In addition, let $B_{\mathcal{L},p}^n(d)$ denote the set $\{ \mathbf{x} \langle p \rangle = (x_1 \langle p \rangle, \ldots, x_n \langle p \rangle) : \mathbf{x} = (x_1, \ldots, x_n) \in B_{\mathcal{L}}^n(d) \}$ and let $B_{\mathcal{L},p}^n(d)$ be its cardinality.

**Remark 2.2.**

(i) It is clear that $B_{\mathcal{L},p}^n(d) \subseteq B_{\mathcal{L}}^n(d)$ for any prime number $p$ and any positive integers $n$ and $d$.

(ii) If $\mathcal{L}$ is the standard lattice $\mathbb{Z}^n$, then $B_{\mathcal{L},p}^n(d) = \{ \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{P}^n : \sum_{i=1}^n x_i^2 \leq d \}$. For any lattice $\mathcal{L} \subseteq \mathbb{Z}^n$, we have $B_{\mathcal{L},p}^n(d) \subseteq B_{\mathbb{Z}^n,p}^n(d)$, and hence, $B_{\mathcal{L},p}^n(d) \leq B_{\mathbb{Z}^n,p}^n(d)$.

(iii) For a sublattice $\mathcal{L}$ of $\mathbb{Z}^n$, let $\mathcal{L} \langle p \rangle = \{ \mathbf{x} \langle p \rangle : \mathbf{x} \in \mathcal{L} \}$.

1. For a sublattice $\mathcal{L}$ of $\mathbb{Z}^n$, let $\mathcal{L} \langle p \rangle = \{ \mathbf{x} \langle p \rangle : \mathbf{x} \in \mathcal{L} \}$. Then it follows easily from the fact that $\det(\mathcal{L}) = |\mathbb{Z}^n / \mathcal{L}|$ that $\mathcal{L} \langle p \rangle = \mathbb{F}_p^n$ if and only if $p \nmid \det(\mathcal{L})$. 


The next lemma suggests how we may construct a sublattice of a certain lattice of \( Z^n \) having a prescribed minimum Euclidean distance.

**Lemma 2.3.** Let \( L \) be a lattice of \( Z^n \) such that \( L(p) \) is the whole space \( \mathbb{F}_p^n \) for an odd prime \( p \). Suppose that there exists a \( k \times n \) matrix \( H \) over \( \mathbb{F}_p \) such that \( Hc^T \neq 0 \) for every nonzero \( c \in B_{L,p}(d) \), where \( c^T \) refers to the transpose of \( c \). Then we can construct a sublattice \( L_H \) of \( L \) such that the rank of \( L_H \) is \( n - k \) and its Euclidean distance \( d(L_H) \geq \sqrt{d+1} \).

**Proof.** By linear algebra, there exist at least \( n - k \) linearly independent vectors \( c_1, \ldots, c_{n-k} \) over \( \mathbb{F}_p \) such that \( Hc_i^T = 0 \) for \( i = 1, \ldots, n - k \). Since \( L(p) = \mathbb{F}_p^n \), we can find vectors \( x_i \in L, i = 1, \ldots, n - k \) with \( x_i(p) = c_i \). Let \( L_H \) be the lattice with basis \( \{x_1, \ldots, x_{n-k}\} \). It is clear that the rank of \( L_H \) is \( n - k \). To show its minimum distance, let \( x \) be a nonzero vector of \( L_H \). First, assume that \( x(p) \neq 0 \). Write \( x = a_1x_1 + \cdots + a_{n-k}x_{n-k} \). Then

\[
Hx(p)^T \equiv a_1Hx_1(p)^T + \cdots + a_{n-k}Hx_{n-k}(p)^T \mod p
\]

\[
= a_1Hc_1^T + \cdots + a_{n-k}Hc_{n-k}^T \mod p
\]

\[
= 0.
\]

By our construction of \( H \), it follows that \( x(p) \notin B_{L,p}(d) \), that is, \( x \notin B_L(d) \). This means that \( ||x||^2 > d \) and since, all norms of \( L \) are integers, \( ||x||^2 \geq d+1 \).

On the other hand, if \( x(p) = 0 \), it follows from the linear independence of \( c_1, \ldots, c_{n-k} \) that \( x = p^ty \), for some \( t \geq 1 \) and \( y \in L_H \) such that \( y(p) \neq 0 \). From above, \( ||x||^2 = ||p^ty||^2 = p^{2t}||y||^2 \geq p^{2t}(d + 1) \geq d + 1 \). \( \square \)

Now, let \( L \) be a lattice of \( Z^n \) with \( L(p) = \mathbb{F}_p^n \) and minimum Euclidean distance \( d(L) \). Further, assume that the other conditions in Lemma 2.3 are satisfied. In particular, suppose that there exists a \( k \times n \) matrix \( H \) over \( \mathbb{F}_p \) such that \( Hc^T \neq 0 \) for all nonzero \( c \in B_{L,p}(d) \). Assume further that \( H \) has rank \( k \). As in the proof, let \( L_H \) be the lattice with basis \( \{x_1, \ldots, x_{n-k}\} \), where \( \{x_1(p), \ldots, x_{n-k}(p)\} \) is a basis for the null space of \( H \). Note that \( L_H \) is not unique, depending on the choice of the \( x_i \)’s.

We construct a new lattice \( R_{L,H} \subseteq Z^n \) defined by

\[
R_{L,H} = L_H + pL.
\]

The following theorem gives the parameters of \( R_{L,H} \).

**Theorem 2.4.**

(i) The rank of \( R_{L,H} \) is \( n \).

(ii) The minimum Euclidean distance of \( R_{L,H} \) satisfies \( d(R_{L,H}) \geq \min\{\sqrt{d+1}, pd(L)\} \).

(iii) The determinant of \( R_{L,H} \) is \( p^k \det(L) \).

**Proof.**

(i) This is clear.

(ii) Let \( c = x + py \) be a nonzero vector of \( R_{L,H} \) with \( x \in L_H \) and \( y \in L \).

If \( x = 0 \), then

\[ ||c|| = ||py|| = p||y|| \geq pd(L). \]
If \( \mathbf{x} \neq \mathbf{0} \), then \( \mathbf{c}(p) = \mathbf{x}(p) \) and we can follow the proof of Lemma 2.3 to conclude that \(|\mathbf{c}| \geq \sqrt{d + 1} \).

(iii) We have

\[
\det(\mathcal{R}_{\mathcal{L},H}) = \frac{\det(p\mathcal{L})}{|\mathcal{R}_{\mathcal{L},H} : p\mathcal{L}|} = \frac{p^n \det(\mathcal{L})}{p^{n-k}} = p^k \det(\mathcal{L}).
\]

\[\square\]

Remark 2.5. Observe that the lattice \( \mathcal{R}_{\mathcal{L},H} \) depends on the choice of the matrix \( H \) we begin with. Indeed, the definition of \( H \) is analogous to the definition of a parity-check matrix in coding theory. As such, we will call the matrix \( H \) which satisfies the condition in Lemma 2.3 a parity-check matrix.

To complete our construction, it remains to find a matrix \( H \) with \( k \) as small as possible. We will use the ideas analogous to those employed in the determination of the Gilbert-Varshamov bound for linear codes to construct our \( H \), thereby giving an upper bound for \( k \).

Theorem 2.6.  

(i) Let \( u = \min\{\sqrt{d}, (p-1)/2\} \). For \( \ell = 1, \ldots, u, i = 1, \ldots, n \), let \( B^n_{\mathcal{L}}(d; x_i = \ell) := \{|(c_1, \ldots, c_{i-1}, \ell, 0, \ldots, 0) \in \mathcal{B}^n(d) : c_1, \ldots, c_{i-1} \in \mathbb{Z}\} \). Suppose that for all \( i = 1, \ldots, n-1 \) and \( \ell = 1, \ldots, u \), \( B^n_{\mathcal{L}}(d; x_i = \ell) \leq B^n_{\mathcal{L}}(d; x_{i+1} = \ell) \) and

\[ p^k > \sum_{\ell=1}^{u} B^n_{\mathcal{L}}(d; x_n = \ell). \tag{2.1} \]

Then, we can construct a \( k \times n \) matrix \( H \) over \( \mathbb{F}_p \) such that \( H\mathbf{c}^T \neq 0 \) for all nonzero \( \mathbf{c} \in \mathcal{B}^n_{\mathcal{L}}(d) \).

(ii) Let \( u = \min\{\sqrt{d}, (p-1)/2\} \). For \( \ell = 1, \ldots, \), \( i = 1, \ldots, n \), let \( B^n_{\mathcal{L},p}(d; x_i = \ell) := \{|(c_1, \ldots, c_{i-1}, \ell, 0, \ldots, 0) \in \mathcal{B}^n_{\mathcal{L}}(d) : c_1, \ldots, c_{i-1} \in \mathbb{F}_p\} \). Suppose that for all \( i = 1, \ldots, n-1 \) and \( \ell = 1, \ldots, u \), \( B^n_{\mathcal{L},p}(d; x_i = \ell) \leq B^n_{\mathcal{L},p}(d; x_{i+1} = \ell) \) and

\[ p^k > \sum_{\ell=1}^{u} B^n_{\mathcal{L},p}(d; x_n = \ell). \tag{2.2} \]

Then, we can construct a \( k \times n \) matrix \( H \) over \( \mathbb{F}_p \) such that \( H\mathbf{c}^T \neq 0 \) for all nonzero \( \mathbf{c} \in \mathcal{B}^n_{\mathcal{L},p}(d) \).

Proof. As both parts are very similar, we will only show the proof for (ii). We construct the columns of \( H \) recursively. Pick any nonzero column vector of \( \mathbb{F}_p^k \) as \( \mathbf{h}_1 \), the first column of \( \mathbf{h}_1 \). Suppose that \( \mathbf{h}_1, \ldots, \mathbf{h}_i \) have been constructed, \( 1 \leq i \leq n-1 \). For \( 1 \leq \ell \leq u \), consider the set \( \mathcal{X}^n_{\mathcal{L},p}(d; x_{i+1} = \ell) := \{\ell^{-1}(c_1\mathbf{h}_1 + c_2\mathbf{h}_2 + \ldots + c_i\mathbf{h}_i) \mod p : (c_1, c_2, \ldots, c_i, \ell, 0, \ldots, 0) \in \mathcal{B}^n_{\mathcal{L},p}(d), c_1, \ldots, c_i \in \mathbb{F}_p\} \)

\[ \quad \]
and $\mathcal{X}[i] := \bigcup_{\ell=1}^u \mathcal{X}_{\mathcal{L},p}^n(d; x_{i+1} = \ell)$. Let $h_{i+1}$ be any nonzero vector in $\mathbb{F}_p^k \setminus \mathcal{X}[i]$. This is possible since

$$|\mathcal{X}[i]| = \left| \bigcup_{\ell=1}^u \mathcal{X}_{\mathcal{L},p}^n(d; x_{i+1} = \ell) \right| \leq \sum_{\ell=1}^u |\mathcal{X}_{\mathcal{L},p}^n(d; x_{i+1} = \ell)| = \sum_{\ell=1}^u B_{\mathcal{L},p}^n(d; x_{i+1} = \ell) \leq \sum_{\ell=1}^u B_{\mathcal{L},p}^n(d; x_n = \ell) < p^k = |\mathbb{F}_p^k|.$$

It remains to show that for all nonzero $c = (c_1, \ldots, c_n) \in B_{\mathcal{L},p}^n(d)$, we have $Hc^T \not\equiv 0 \mod p$. Suppose to the contrary that there is a nonzero $c \in \mathcal{L}$ such that $Hc^T \equiv 0 \mod p$ and $||c||^2 \leq d$. Let $r$ be the largest index for which $c_r$ is nonzero. Thus, we have

$$c_1 h_1 + \cdots + c_r h_r \equiv 0 \mod p.$$

We may assume that $c_r > 0$ (otherwise we can multiply by $-1$). Then $h_r = c_r^{-1} (-c_1 h_1 - \cdots - c_{r-1} h_{r-1}) \in \mathcal{X}_{\mathcal{L},p}^n(d; x_r = c_r) \subseteq \mathcal{X}[r-1]$, contradicting our choice of $h_r$. \hfill $\square$

3. Explicit constructions

We now proceed to apply the above construction to some well-known lattices.

3.1. The standard lattice $\mathbb{Z}^n$. As a first example, we let $\mathcal{L}$ be the standard lattice $\mathbb{Z}^n$. Recall that $d(\mathbb{Z}^n) = 1$ and $\det(\mathbb{Z}^n) = 1$. Since for any prime $p$, $\mathcal{R}(p) = \mathbb{F}_p^n$, we can construct $\mathcal{L}_{\mathbb{Z}^n,H}$ as described in the preceding section. In order to facilitate our computations, we modify our condition in Equation 2.2 as follows.

**Lemma 3.1.** For any positive integers $m$ and $d$ and odd prime number $p$, let $\phi_{m,d}(x) = \left( 1 + 2 \sum_{i=1}^{(p-1)/2} x^2 \right)^m \mod x^{d+1}$, where the modulo is taken in the polynomial ring $\mathbb{Z}[x]$. Then, there exists a $k \times n$ matrix $H$ over $\mathbb{F}_p$ such that $Hc^T \not\equiv 0 \mod p$ for all nonzero $c \in B_{\mathbb{Z}^n,p}^n(d)$ if

$$p^k > \frac{\phi_{n,d}(1) - \phi_{n-1,d}(1)}{2}.$$

**Proof.** For all $\ell = 1, \ldots, (p-1)/2$ and $i = 1, \ldots, n$, we have $B_{\mathbb{Z}^n,p}^n(d; x_i = \ell) \leq B_{\mathbb{Z}^n,p}^n(d; x_n = \ell)$. Hence, it suffices to show that $\sum_{\ell=1}^{(p-1)/2} B_{\mathbb{Z}^n,p}^n(d; x_n = \ell) = (\phi_{n,d}(1) - \phi_{n-1,d}(1))/2$. Recall the theta series for $\mathbb{Z}^n$ is

$$\theta(x) = \left( 1 + 2 \sum_{i=1}^{\infty} x^2 \right)^n.$$
Now, since \( B_{\mathbb{Z}^n,p}^n(d) = \{ c \in \mathbb{F}_p^n : ||c||^2 \leq d \} \), the equivalent theta series for \( \mathbb{Z}^n/p \) is

\[
\phi(x) = \left( 1 + 2 \sum_{i=1}^{(p-1)/2} x^2 \right)^n.
\]

Thus \( B_{\mathbb{Z}^n,p}^n(d) = \phi_{n,d}(1) \). Further, we have \( B_{\mathbb{Z}^n,p}^n(d; x_n = \ell) = B_{\mathbb{Z}^n,p}^n(d; x_n = -\ell) \) for any \( \ell = 1, \ldots, (p-1)/2 \). Consequently,

\[
\phi_{n,d}(1) = \sum_{\ell=-(p-1)/2}^{(p-1)/2} B_{\mathbb{Z}^n,p}^n(d; x_n = \ell)
\]

\[
= B_{\mathbb{Z}^n,p}^n(d; x_n = 0) + 2 \sum_{\ell=1}^{(p-1)/2} B_{\mathbb{Z}^n,p}^n(d; x_n = \ell)
\]

\[
= B_{\mathbb{Z}^{n-1},p}^{n-1}(d) + 2 \sum_{\ell=1}^{(p-1)/2} B_{\mathbb{Z}^n,p}^n(d; x_n = \ell)
\]

\[
= \phi_{n-1,d}(1) + 2 \sum_{\ell=1}^{(p-1)/2} B_{\mathbb{Z}^n,p}^n(d; x_n = \ell),
\]

and the result follows.

**Corollary 3.2.** For any positive integer \( n \), odd prime \( p \) and positive integer \( d \) with \( d + 1 \leq p^2 \), the lattice \( \mathcal{R}_{\mathbb{Z}^n,H} \) has center density

\[
\delta(\mathcal{R}_{\mathbb{Z}^n,H}) \geq \frac{(d+1)^{n/2}}{2^n p^k},
\]

where \( k \) is the largest integer satisfying Equation (3.1). Hence, for an odd prime \( p \), one has

\[
\delta_n \geq \max \left\{ \frac{(d+1)^{n/2}}{2^n p^k} : 0 \leq d \leq p^2 - 1 , \ k \text{ satisfies (3.1)} \right\}.
\]

**Proof.** This is an immediate consequence of Theorem 2.4 and Lemma 3.1. \( \square \)

**Remark 3.3.** Observe that in this case where \( \mathcal{L} = \mathbb{Z}^n \), our construction is just the construction of Rush [7] applied to \( p \)-ary linear codes, which is in turn a generalization of “Construction A” of Leech and Sloane [2]. Nonetheless, by making use of the parity-check matrix \( H \), we are able to derive an expression for the center densities which slightly improves (in computational terms) the expression given in [7] (as can be seen in the values presented in the appendix). More specifically, the size of Rush’s ball has cardinality \( \frac{p-1}{2p} \cdot B_{\mathbb{Z}^n,p}^n(d) \approx \frac{B_{\mathbb{Z}^n,p}^n(d)}{2} \) while in our expression, we subtract a ball of the same radius in dimension \( n-1 \). Evidently, our results converge asymptotically.
3.2. The root lattice \(D_n\). We next consider the root lattice \(D_n = \{ (x_1, \ldots, x_n) \in \mathbb{Z}^n : \sum_{i=1}^n x_i \equiv 0 \mod 2 \}\). Then, \(d(D_n) = \sqrt{2}\) and \(\det(D_n) = 2\). Since \(p \nmid \det(D_n)\) for any odd prime \(p\), we have \(D_n(p) = \mathbb{F}_p^n\).

As it is not easy to define \(B_{D_n,p}^n(d)\) directly, we apply Equation (2.1) to find \(k\). In particular, we have the following result. Note again that we have \(B_{D_n}(d; x_i = \ell) \leq B_{D_n}(d; x_n = \ell)\) for \(1 \leq i \leq n - 1\).

**Lemma 3.4.** For a positive integer \(m\), let \(\sigma_{m,d}(x) = (1+2 \sum_{i=1}^n x^2)^m \mod x^{d+1}\), where \(u = \min\{\sqrt{d}, (p-1)/2\}\). Then for \(1 \leq \ell \leq (p-1)/2\),

\[
B_{D_n}(d; x_n = \ell) = \begin{cases} 
(\sigma_{n-1,d-\ell}(1) \pm \sigma_{n-1,d-\ell}(1)) / 2, & \text{if } \ell \text{ is even}, \\
(\sigma_{n-1,d-\ell}(1) - \sigma_{n-1,d-\ell}(1)) / 2, & \text{if } \ell \text{ is odd}.
\end{cases}
\]

**Proof.** The result follows from the theta series of \(D_n\) and the fact that for \((x_1, \ldots, x_n) \in D_n, x_n\) is even if and only if \(x_1 + \cdots + x_{n-1}\) is even. \(\square\)

**Corollary 3.5.** For any positive integer \(n\), odd prime number \(p\) and integer \(d\) with \(d+1 \leq 2p^2\), the lattice \(R_{D_n,H}\) constructed in the previous section has center density given by

\[
\delta(R_{D_n,H}) \geq \frac{(d+1)^{n/2}}{2^{n+1}p^k},
\]

where \(k\) is the largest integer satisfying Equation (2.1). Hence, for an odd prime \(p\), one has

\[
\delta_n \geq \max \left\{ \frac{(d+1)^{n/2}}{2^{n+1}p^k} : 0 \leq d \leq 2p^2 - 1, k \text{ satisfies (2.1)} \right\}.
\]

4. Number Fields

In this section, we generalize our approach to quadratic fields. We refer the reader to [8] for some fundamental results on quadratic fields that are used here without proof. Let \(K/\mathbb{Q}\) be an imaginary quadratic field, that is, \(K = \mathbb{Q}(\sqrt{d})\) for some square-free negative integer \(d\). Let \(\mathcal{O}_K\) denote the integral ring of \(K\). In particular,

\[
\mathcal{O}_K = \begin{cases} 
\mathbb{Z} + \frac{1+i\sqrt{d}}{2}\mathbb{Z}, & \text{if } d \equiv 1 \mod 4, \\
\mathbb{Z} + \sqrt{d}\mathbb{Z} & \text{otherwise}
\end{cases}
\]

Recall that for any \(x \in \mathcal{O}_K, ||x||^2 = xx^*\) is an integer. Note that we identify \(\mathcal{O}_K\) with \(\mathbb{R}^2\) by the identification \(x = a + bi \mapsto (a,b)\). Then, \(||x||^2 = a^2 + b^2\).

Fix a prime ideal \(\wp\) of \(\mathcal{O}_K\) with norm \(N(\wp) = q\), i.e., \(|K_\wp| = q\), where \(K_\wp\) denotes the residue class field \(\mathcal{O}_K/\wp\). Fix a set \(Q\) of \(q\) representatives \(Q = \{\alpha_1, \ldots, \alpha_q\}\) for \(K_\wp\) such that \(||\alpha_i||^2 \leq ||\alpha_i + \beta||^2\) for all \(\beta \in \wp\).

Denote by \(B_K^n(d)\) the set \(\{x = (x_1, \ldots, x_n) \in \mathcal{O}_K^n : ||x||^2 = \sum_{i=1}^n ||x_i||^2 \leq d\}\) and let \(B_{K,\wp}^n(d)\) denote the cardinalities of \(B_K^n(d)\) and \(B_{K,\wp}^n(d)\), respectively.
Assume that $H$ is a $k \times n$ matrix over $K_\wp$ such that for any nonzero element $c \in B_{K,\wp}^n(d)$, we have $HC^T \neq 0 \mod \wp$. The null space $C$ over $K_\wp$ of $H$ has dimension at least $n - k$. It is clear that $C \cap B_{K,\wp}^n(d) = \{0\}$.

Now for any point $y$ in $\mathcal{O}_K^n$ with $y \mod \wp \in C \setminus \{0\}$, then $y \mod \wp \notin B_{K,\wp}^n(d)$. This implies that $y \notin B_{K}^n(d)$, i.e., $\|y\|^2 \geq d + 1$.

We consider the lattice $\mathcal{R}_{K,H} = C + \wp^n$, where $\wp^n$ denotes the direct product $\wp \times \cdots \times \wp$.

**Theorem 4.1.**

(i) $d(C + \wp^n) \geq \min\{\sqrt{d+1},q\}$;

(ii) The rank of this lattice is $2n$;

(iii) $\det(C + \wp^n) = \frac{q^n\det(\mathcal{O}_K)^n}{|C|} \leq q^k \det(\mathcal{O}_K)^n$.

**Proof.** Let $x + y$ be a point in the lattice with $x \in C$ and $y \in \wp^n$. If $x = 0$, then $\|y\|^2 \geq N(\wp) = q$. If $x \neq 0$, then $x + y \mod \wp$ is a nonzero codeword of $C$. Hence, $\|x+y\|^2 \geq d + 1$.

As $|C| \geq q^k$, the determinant of the lattice is clear. □

By mimicking the proof of Theorem 2.6, we have the following analogous bound on $k$.

**Theorem 4.2.** Let $I = \{\alpha_1, \ldots, \alpha_i\}$ be a subset of $\mathcal{Q}$ such that the sets 
$$\{|\alpha_1|, \ldots, |\alpha_i|\}, \quad \{|\alpha| : \alpha \in \mathcal{Q}, 0 < |\alpha|^2 \leq d\}$$
are equal, and moreover, $|\alpha_1|, \ldots, |\alpha_i|$ are pairwise distinct. Then there is a $k \times n$ matrix over $K_\wp$ such that $HC^T \neq 0 \mod \wp$ for all nonzero $c$ of $B_{K,\wp}^n(d)$ provided that

$$q^k > \sum_{\alpha \in I} B_{K,\wp}^n(d; x_n = \alpha),$$

where $B_{K,\wp}^n(d; x_i = \alpha)$ denotes the cardinality of the set $\{(x_1, \ldots, x_i-1, \alpha, 0, \ldots, 0) \in B_{K,\wp}^n(d) : x_j \in \mathcal{Q}, 1 \leq j \leq i-1\}$.

Note that we have $B_{K,\wp}^n(d; x_i = \alpha) \leq B_{K,\wp}^n(d; x_{i+1} = \alpha)$ for all $1 \leq i \leq n - 1$.

Let’s take a look at a particular example, namely $K = \mathcal{Q}(\sqrt{-3})$. We state some basic facts about $\mathcal{Q}(\sqrt{-3})$.

(i) $2$ is inert in $K$ while $3$ is ramified in $K$. For any odd prime $p \geq 5$, $p$ splits in $K$ if $p \equiv 1 \mod 3$ and $p$ is inert in $K$ otherwise.

(ii) For any ideal $\wp$ with norm $q$, the determinant is $\det(\wp) = q\sqrt{3}/2$.

**Theorem 4.3.** For any $n$, if $\wp$ is a prime ideal of $\mathcal{Q}(\sqrt{-3})$ with norm $q \geq d+1$, the center density of the lattice $\mathcal{R}_{K,H} \subseteq \mathbb{R}^{2n}$ is given by

$$\delta(\mathcal{R}_{K,H}) \geq \frac{(d+1)^n}{2^{n}3^n/2^{k}},$$

where $k$ is the largest integer satisfying Equation (4.1). In particular,

$$\delta_{2n} \geq \max \left\{ \frac{(d+1)^n}{2^{n}3^n/2^{k}} : k \text{ satisfies Equation (4.1)} \right\}.$$
As in the previous section, we need to compute the theta function of $O_K$ in order to utilize Equation (4.1).

**Lemma 4.4.** For $k \geq 1$, let $N_k$ be the number of the Eisenstein integers of $O_K$ with norm equal to $k$, i.e., $N_k = |\{\alpha \in O_K : ||\alpha||^2 = k\}|$. Let $k$ have a canonical factorization into a product of primes

$$k = 3^e \prod_{i=1}^r p_i^{e_i} \prod_{j=1}^s q_j^{d_j}$$

with $e \geq 0$, $e_i, d_i \geq 1$, $p_i \equiv 1 \mod 3$ for all $1 \leq i \leq r$ and $q_j \equiv 2 \mod 3$ for all $1 \leq j \leq s$. Then, $N_k$ is equal to

$$N_k = \begin{cases} 0 & \text{if } d_j \text{ is odd for some } j, \\ 6 \prod_{i=1}^r (1 + e_i) & \text{otherwise}. \end{cases}$$

**Proof.** First of all, there are altogether 6 roots of unity in $O_K$, i.e., $N_1 = 6$. Now let $\alpha$ be an integer in $O_K$ with $||\alpha||^2 = k > 1$. Then $\alpha O_K$ has a factorization as a product of prime ideals

$$\alpha O_K = \wp_1^{a_1} \wp_1^{b_1} \prod_{j=1}^s \Re_j^{c_j},$$

where $\wp$ is the prime ideal lying over 3, $\wp_i$ are splitting prime ideals with conjugate $\bar{\wp}_i$ and $\Re_j$ are inert prime ideals. Then the norm of $\alpha$ is

$$||\alpha||^2 = 3^e \prod_{i=1}^r p_i^{a_i + b_i} \prod_{j=1}^s q_j^{2c_j}$$

with $N(\wp_i) = p_i$ and $N(\Re_j) = q_j^2$. This implies that $N_k = 0$ if $d_j$ is odd for some $j$. If $d_j$ are even for all $j$, we can see that for each $i$, there are $1 + e_i$ possible ideals $\wp_i^{a_i} \wp_i^{e_i-a_i}$ ($0 \leq a_i \leq e_i$) with norm equal to $p^{e_i}$ (note that $O_K$ is a principal ideal domain). This implies the desired result. \hfill $\square$

Consider the lattice $O_K^n$. It has rank $2n$ and can be viewed as a lattice in $\mathbb{R}^{2n}$. Let $S_{n,k}$ denote the number of lattice points on the sphere of radius $k$, i.e.,

$$S_{n,k} := \left| \{ (\alpha_1, \ldots, \alpha_n) \in O_K^n : \sum_{i=1}^n ||\alpha_i||^2 = k \} \right|.$$ 

Note that if we identify a point $(a_1+ib_1, \ldots, a_n+ib_n) \in \mathbb{C}^n$ with $(a_1, b_1, \ldots, a_n, b_n) \in \mathbb{R}^{2n}$, then $\sum_{j=1}^n ||a_j + ib_j||^2 = \sum_{j=1}^n (a_j^2 + b_j^2)$.

By considering the theta function of $O_K$, we are able to determine $S_{n,k}$ in terms of $N_k$. More specifically, we have
Lemma 4.5. One has the following identity of power series

\[ \sum_{k=0}^{\infty} S_{n,k} x^k = \left(1 + \sum_{k=1}^{\infty} N_k x^k\right)^n. \]

Finally, we obtain

\[ B_n^K(d) = \sum_{k=0}^{d} S_{n,k}. \]

Likewise, we can compute \( B_{n,\varphi}^K(d) \) as

\[ B_{n,\varphi}^K(d) = \sum_{k=0}^{d} S_{n,k,\varphi}, \]

where

\[ \sum_{k=0}^{\infty} S_{n,k,\varphi} x^k = \left(\sum_{\alpha \in \mathbb{Q}} x||\alpha||^2\right)^n. \]

Remark 4.6. (i) We remark that the work in this present paper can be further explored in various directions. First of all, in the previous section, we applied our construction to two particular examples of lattices, namely \( \mathbb{Z}^n \) and \( D_n \). It is interesting to consider other families of lattices in which the theta series are explicitly known as well. We will leave these considerations as a future project.

(ii) In addition, we may attempt to construct new lattices by concatenating codes to other lattices of \( \mathcal{O}_K^n \). For instance, we may consider the lattice \( \mathcal{L} = \{(x_1, \ldots, x_n) \in \mathcal{O}_K^n : \sum_{i=1}^{n} x_i \equiv 0 \pmod{\varphi}\} \), where \( \varphi \) is the unique prime lying over 3. However, we did not get any new lattices from this construction.

(iii) Last but not least, we can generalize the construction in this section from quadratic fields to arbitrary number fields. Once again, we will leave this problem for future research.

5. Appendix: A table of densities

We carry out the above computations using the Magma computer algebra system [4] for some large dimensions of \( n \). We compare our results with those of Rush’s construction [7], which gives the following bound for the center density in dimension \( n \), namely,

\[ \delta(L_{\text{Rush}}) \geq \max_{d>0} \frac{\sqrt{d+1}}{2^n p^k}, \]

where \( p \geq \sqrt{d+1} \) and

\[ p^k > \frac{p-1}{2p} \times B_{\mathbb{Z}^n,p}^n(d). \]
Table of center densities of lattices from $\mathbb{Z}^n, D_n, K = \mathbb{Q}(\sqrt{-3})$ and Rush’s construction, respectively

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\log_2(\delta(R_{\mathbb{Z}^n,H}))$</th>
<th>$\log_2(\delta(R_{D_n,H}))$</th>
<th>$\log_2(\delta(R_{K,H}))$</th>
<th>$\log_2(\delta(L_{\text{Rush}}))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>752.20</td>
<td>753.29</td>
<td>753.48</td>
<td>750.97</td>
</tr>
<tr>
<td>520</td>
<td>769.64</td>
<td>770.74</td>
<td>770.92</td>
<td>768.44</td>
</tr>
<tr>
<td>1020</td>
<td>1997.74</td>
<td>1998.70</td>
<td>1999.00</td>
<td>1996.6</td>
</tr>
<tr>
<td>1030</td>
<td>2024.49</td>
<td>2025.44</td>
<td>2025.76</td>
<td>2023.36</td>
</tr>
<tr>
<td>1440</td>
<td>3175.15</td>
<td>3176.06</td>
<td>3176.42</td>
<td>3174.04</td>
</tr>
<tr>
<td>1442</td>
<td>3181.00</td>
<td>3181.91</td>
<td>3182.26</td>
<td>3179.89</td>
</tr>
<tr>
<td>1444</td>
<td>3186.85</td>
<td>3187.73</td>
<td>3188.10</td>
<td>3185.74</td>
</tr>
<tr>
<td>1446</td>
<td>3192.69</td>
<td>3193.59</td>
<td>3193.95</td>
<td>3191.57</td>
</tr>
<tr>
<td>1448</td>
<td>3198.54</td>
<td>3199.45</td>
<td>3199.80</td>
<td>3197.43</td>
</tr>
<tr>
<td>1450</td>
<td>3204.39</td>
<td>3205.30</td>
<td>3205.64</td>
<td>3203.29</td>
</tr>
<tr>
<td>1452</td>
<td>3210.24</td>
<td>3211.15</td>
<td>3211.50</td>
<td>3209.13</td>
</tr>
<tr>
<td>1454</td>
<td>3216.10</td>
<td>3217.01</td>
<td>3217.35</td>
<td>3214.98</td>
</tr>
<tr>
<td>1456</td>
<td>3221.95</td>
<td>3222.86</td>
<td>3223.20</td>
<td>3220.84</td>
</tr>
<tr>
<td>1458</td>
<td>3227.81</td>
<td>3228.71</td>
<td>3229.07</td>
<td>3226.72</td>
</tr>
<tr>
<td>1460</td>
<td>3233.67</td>
<td>3234.58</td>
<td>3234.92</td>
<td>3232.56</td>
</tr>
<tr>
<td>1462</td>
<td>3239.53</td>
<td>3240.44</td>
<td>3240.78</td>
<td>3238.42</td>
</tr>
<tr>
<td>1464</td>
<td>3245.40</td>
<td>3246.30</td>
<td>3246.66</td>
<td>3244.3</td>
</tr>
<tr>
<td>1512</td>
<td>3386.72</td>
<td>3387.61</td>
<td>3387.97</td>
<td>3385.6</td>
</tr>
<tr>
<td>1560</td>
<td>3529.14</td>
<td>3530.01</td>
<td>3530.39</td>
<td>3528.03</td>
</tr>
<tr>
<td>1608</td>
<td>3672.62</td>
<td>3673.51</td>
<td>3673.88</td>
<td>3671.51</td>
</tr>
<tr>
<td>1656</td>
<td>3817.14</td>
<td>3818.03</td>
<td>3818.39</td>
<td>3816.03</td>
</tr>
<tr>
<td>2052</td>
<td>5045.29</td>
<td>5046.15</td>
<td>5046.54</td>
<td>5044.21</td>
</tr>
<tr>
<td>4098</td>
<td>12111.88</td>
<td>12112.66</td>
<td>12113.13</td>
<td>12110.85</td>
</tr>
<tr>
<td>8190</td>
<td>28287.70</td>
<td>28288.41</td>
<td>28288.94</td>
<td>28286.71</td>
</tr>
<tr>
<td>16380</td>
<td>64755.96</td>
<td>64756.63</td>
<td>64757.21</td>
<td>64755.03</td>
</tr>
</tbody>
</table>

Remark 5.1. (i) It can be verified that the corresponding densities in [2] are much weaker than those in the above table. For instance, for dimensions $n = 512, 1020, 1030, 4098, 8190$ and 16380, the corresponding center densities in [2] are 698, 1922, 1947, 11279, 26154 and 59617, respectively.

(ii) From the above numerical results, we observe that the center densities of our lattices from $\mathbb{Z}^n, D_n$ and $K = \mathbb{Q}(\sqrt{-3})$ are all bigger than the ones from Rush’s construction.

(iii) It seems that the quadratic field $K = \mathbb{Q}(\sqrt{-3})$ gives lattices with the best densities among all three, while $D_n$ produces lattices with bigger densities than $\mathbb{Z}^n$. 
(iv) For odd dimensions, we can get lattices using $\mathbb{Z}^n$ or $D_n$. For instance, for $n = 1441$, the center densities of the lattices from $\mathbb{Z}^n$, $D_n$ and Rush’s construction are 3178.08, 3178.98 and 3176.98, respectively.

**Acknowledgement**

We are grateful to Prof. G. Nebe for giving us some useful comments and suggestions.

**References**


Division of Mathematical Sciences, School of Physical & and Mathematical Sciences, Nanyang Technological University, Singapore 637616, Republic of Singapore.

E-mail address: xingcp@ntu.edu.sg

Cryptography Department, Institute for Infocomm Research (I²R), Singapore 119613, Republic of Singapore.

Division of Mathematical Sciences, School of Physical & and Mathematical Sciences, Nanyang Technological University, Singapore 637616, Republic of Singapore.

E-mail address: slyeo@i2r.a-star.edu.sg