Dense packings from quadratic fields and codes✩

Chaoping Xing

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

Received 7 March 2007

Available online 30 January 2008

Communicated by Vera Pless

Abstract

In the present paper, we make use of the quadratic field \( \mathbb{Q}(\sqrt{-3}) \) to construct dense packings in the Euclidean spaces. With the help from good error-correcting codes, we are able to produce several packings with the best-known densities. Furthermore, if we assume that the best upper bound in coding theory developed by Aaltonen, Ben-Haim and Litsyn could be achieved, then the Minkowski bound would be improved.

© 2008 Elsevier Inc. All rights reserved.

Keywords: Dense packings; Asymptotic bounds; Minkowski bound; Best-known packings; Quadratic fields

1. Introduction

Dense packings have been investigated for many years and various constructions have been proposed based on the subjects, such as, geometry, combinatorics, number theory and coding theory, etc. (for instance, see [15,16]). For a survey on this topic, the reader may refer to the book by Conway and Sloane [6] and Zong and Talbot [20].

A typical construction from number fields is to make use of integral ideals to obtain lattices. For instance, the well-known lattice \( \Lambda_{24} \) can be realized as an ideal in certain cyclotomic field (see [6, p. 227]). Another example is the integral ring \( \mathcal{O}_K \) of the quadratic field \( K = \mathbb{Q}(\sqrt{-3}) \). It is a packing with the highest density in \( \mathbb{R}^2 \).

✩ The research is partially supported by the Singapore MoE Tier 1 grant RG60/07 and the National Scientific Research Project 973 of China 2004CB318000.

E-mail address: xingcp@ntu.edu.sg.
Assume that $K$ has a prime ideal with the residue class field isomorphic to the finite field $\mathbb{F}_q$. Then one can concatenate $q$-ary codes with packings in $O^n_K$ (see Section 2). Using this idea, we can produce several packings with the best-known densities.

A packing in $\mathbb{R}^n$ is a set $P$ of points in $\mathbb{R}^n$ such that the Euclidean distance of $P$

\[ d_E(P) := \inf \left\{ d_E(u, v) : u, v \in \mathbb{R}^n ; u \neq v \right\} \]

is positive, where $d_E(u, v)$ denotes the Euclidean distance of two points $u, v$.

Denote the density of a packing $P$ by $\Delta(P)$. We are interested in dense packings, i.e., we want to find a packing with density close to the quantity

\[ \Delta_n := \limsup_{P} \Delta(P), \]

where $P$ is extended over all packings in $\mathbb{R}^n$.

To look at the asymptotic behavior of $\Delta_n$ as $n$ tends to $\infty$, we define

\[ \lambda := \limsup_{n \to \infty} \frac{\log_2(\Delta_n)}{n}, \]

where $\log_2$ is the logarithm with base 2.

The well-known Minkowski bound says that $\lambda \geq -1$ (see [4, p. 184], [8, p. 148], [14, p. 4]). Litsyn and Tsfasman mentioned in their paper [9] (without detailed proof) that the Minkowski bound can be improved to $\lambda \geq -0.9$ if the McEliece–Rodemich–Ramsey–Welch bound in coding theory (see Section 3 for this bound) could be achieved. In this paper, we improve the result of Litsyn and Tsfasman by showing that if the best upper bound in coding theory developed by Aaltonen, Ben-Haim and Litsyn (see [1,2]) could be achieved, then the Minkowski bound can be improved further to $\lambda \geq -0.8471$.

The paper is organized as follows. In Section 2, we introduce a concatenation rule using quadratic field $\mathbb{Q}(\sqrt{-3})$ and codes and present several good examples. In Section 3, we derive a lower bound on $\lambda$ based on asymptotic bounds from coding theory. We show some improvements on the Minkowski bound under the assumption that the best upper bound in coding theory could be achieved.

2. Constructions of dense packings

From now on, we need some basic results from algebraic number theory. The reader may refer to [18] for some background.

Throughout this paper, we fix $\omega = (-1 + \sqrt{-3})/2$. It is a third primitive root of unity. Then $\{1, \omega\}$ forms an integral basis for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-3})$. We denote by $O_K$ the integral ring of $K$.

We identify a vector $u + \omega v \in \mathbb{R}^n + \omega \mathbb{R}^n$ in $\mathbb{C}^n$ ($u, v \in \mathbb{R}^n$) with a vector $(u - \frac{1}{2}v, \frac{\sqrt{3}}{2}v)$ in $\mathbb{R}^{2n}$ through the mapping $a + bi \mapsto (a, b)$ ($a, b \in \mathbb{R}$). Thus $O^n_K$ can be viewed as a subset of $\mathbb{R}^{2n}$.

For a complex vector $c = (a_1 + b_1i, \ldots, a_n + b_ni)$ ($a_i, b_i \in \mathbb{R}$), we denote by $\|c\|$ its norm $\sqrt{\sum_{i=1}^n (a_i^2 + b_i^2)}$. Then it is clear that $\|u + \omega v\| = \|(u - \frac{1}{2}v, \frac{\sqrt{3}}{2}v)\|$ for any two vectors $u$ and $v$ in $\mathbb{R}^n$.

The following lemma contains an obvious fact from number theory, but it is useful for our purpose. The straightforward proof is omitted.

**Lemma 2.1.** For any nonzero element $\alpha \in O_K$, we have $\|\alpha\| \geq 1.$
For a packing $\mathcal{P}$ in $\mathbb{R}^n$, we introduce a new packing $\mathcal{P} + \omega \mathcal{P} := \{\mathbf{u} + \omega \mathbf{v} : \mathbf{u}, \mathbf{v} \in \mathcal{P}\}$ in $\mathbb{R}^{2n}$. Furthermore, if $n$ is even, we can define another packing as follows

$$\mathcal{P}^{(h)} := \{\mathbf{u} + \omega \mathbf{v} : \mathbf{u}, \mathbf{v} \in \mathbb{R}^{n/2}, (\mathbf{u}, \mathbf{v}) \in \mathcal{P}\}. $$

Note that $\mathcal{P}^{(h)}$ is identified with a subset of $\mathbb{R}^n$.

**Proposition 2.2.** Let $\mathcal{P} \subseteq \mathbb{Z}^n$ be a lattice packing in $\mathbb{R}^n$. Then the Euclidean distance $d_E(\mathcal{P} + \omega \mathcal{P})$ (note that $\mathcal{P} + \omega \mathcal{P}$ is a subset of $\mathcal{O}_K^n$ which is identified with a subset of $\mathbb{R}^{2n}$) is equal to the Euclidean distance $d_E(\mathcal{P})$.

**Proof.** Since $\mathcal{P}$ is a subset of $\mathcal{P} + \omega \mathcal{P}$, it is clear that $d_E(\mathcal{P} + \omega \mathcal{P}) \leq d_E(\mathcal{P})$.

Now let $\mathbf{u}_1 + \omega \mathbf{v}_1$ and $\mathbf{u}_2 + \omega \mathbf{v}_2$ ($\mathbf{u}_i, \mathbf{v}_j \in \mathcal{P}, i = 1, 2, j = 1, 2$) be two distinct elements in $\mathcal{P} + \omega \mathcal{P}$ and put

$$\mathbf{u}_1 + \omega \mathbf{v}_1 - (\mathbf{u}_2 + \omega \mathbf{v}_2) = \mathbf{a} + \omega \mathbf{b}. $$

Then $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$ and $(\mathbf{a}, \mathbf{b}) \neq (0, 0)$. We have to show that $\|\mathbf{a} + \omega \mathbf{b}\| \geq d_E(\mathcal{P})$.

If $\mathbf{b} = 0$, then $\|\mathbf{a} + \omega \mathbf{b}\| = \|\mathbf{a}\| \geq d_E(\mathcal{P})$.

Next assume that $\mathbf{b} \neq 0$.

**Case 1.** $\mathbf{b} = 2\mathbf{a}$. Then

$$\|\mathbf{a} + \omega \mathbf{b}\| = \left\| \frac{\sqrt{3}}{2} \mathbf{b} \right\| = \|\sqrt{3}\mathbf{a}\| \geq \sqrt{3}d_E(\mathcal{P}).$$

**Case 2.** $\mathbf{b} \neq 2\mathbf{a}$. Then

$$\|\mathbf{a} + \omega \mathbf{b}\|^2 = \left\| \frac{1}{2} (2\mathbf{a} - \mathbf{b}) \right\|^2 + \left\| \frac{\sqrt{3}}{2} \mathbf{b} \right\|^2 \geq \frac{1}{4} d_E(\mathcal{P})^2 + \frac{3}{4} d_E(\mathcal{P})^2 = d_E(\mathcal{P})^2,$$

i.e., $\|\mathbf{a} + \omega \mathbf{b}\| \geq d_E(\mathcal{P})$. 

For a rational prime $p$, the splitting behavior of $p$ in $K/\mathbb{Q}$ is as follows [18]:

(i) $2$ is inert (i.e., $2\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$);

(ii) $3$ is ramified (i.e., $3\mathcal{O}_K = \wp^2$ for a prime ideal $\wp$ of $\mathcal{O}_K$);

(iii) $p$ is inert (i.e., $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$) if the Legendre symbol $(\frac{\omega}{p})$ is equal to $-1$ and $p \neq 2, 3$.

(iv) $p$ splits (i.e., $p\mathcal{O}_K = \wp_1\wp_2$ for two distinct prime ideals $\wp_1$ and $\wp_2$ of $\mathcal{O}_K$) if the Legendre symbol $(\frac{\omega}{p})$ is equal to $1$ and $p \neq 2, 3$.

Let $\wp$ be a prime ideal of $\mathcal{O}_K$. Assume that its residue class field $F_\wp$ is isomorphic to the finite field $F_q$. Let $\alpha_1 = 0, \ldots, \alpha_q$ be $q$ elements of $\mathcal{O}_K$ such that $\alpha_1, \ldots, \alpha_q$ represent $q$ distinct elements in $F_\wp$.

For a $q$-ary code $C$, we take the code alphabet set of $C$ to be $\{\alpha_1, \ldots, \alpha_q\}$. Next we give a concatenation of packings with codes.
Proposition 2.3. Let \( \mathcal{P} \subseteq \mathcal{O}_K \) be a packing in \( \mathbb{R}^{2n} \). Let \( \Delta(\mathcal{P}) \) denote the density of \( \mathcal{P} \).

(i) If \( \mathfrak{P} \) is a prime ideal in \( \mathcal{O}_K \) with the residue class field \( \mathbb{F}_q \) isomorphic to \( \mathbb{F}_q \) and \( C \) is a \( q \)-ary code of length \( n \) with the Hamming distance \( d_H(C) \) and size \( M \), then the Euclidean distance of the packing \( C + t_\mathfrak{P} \mathcal{P} \) is at least \( \min\{\sqrt{d_H(C)}, \sqrt{qd_E(\mathcal{P})}\} \), where \( t_\mathfrak{P} \) is a generator of the prime ideal \( \mathfrak{P} \) (note that \( \mathcal{O}_K \) is a principal ideal ring). Furthermore, the density of \( C + t_\mathfrak{P} \mathcal{P} \) as a packing in \( \mathbb{R}^{2n} \) (i.e., the “dimension” of this packing is \( 2n \)) is at least \( \Delta(\mathcal{P})M \) if \( d_H(C) \geq q(d_E(\mathcal{P}))^2 \).

(ii) If \( \mathcal{P} \) is a lattice and \( C \) satisfies that for \( x, y \in C \), the sum \( x + y \) is equal to \( z + t_\mathfrak{P} u \) for some \( z \in C \) and \( u \in \mathcal{P} \), then \( C + t_\mathfrak{P} \mathcal{P} \) is also a lattice.

Proof. (i) Let \( u_1 + t_\mathfrak{P} v_1 \) and \( u_2 + t_\mathfrak{P} v_2 \) (\( u_i \in C, v_j \in \mathcal{P} \) for \( i = 1, 2, j = 1, 2 \)) be two distinct elements in \( C + t_\mathfrak{P} \mathcal{P} \) and put

\[
 u_1 + t_\mathfrak{P} v_1 - (u_2 + t_\mathfrak{P} v_2) = a + t_\mathfrak{P} b.
\]

Then \( (a, b) \neq (0, 0) \).

Case 1. \( a = 0 \). Then

\[
 \|a + t_\mathfrak{P} b\| = \sqrt{q}\|b\| \geq \sqrt{q} d_E(\mathcal{P}).
\]

Note that the norm of \( t_\mathfrak{P} \) is \( \sqrt{q} \).

Case 2. \( a \neq 0 \). Then the Hamming weight \( e \) of \( a \) is at least \( d_H(C) \). We may assume that \( a = (a_1, \ldots, a_e, 0) \) with \( a_i \neq 0 \) for \( 1 \leq i \leq e \), thus \( q \mathfrak{P}(a_i) = 0 \). Put \( b = (b_1, \ldots, b_n) \), then \( a_i + t_\mathfrak{P} b_i \) are nonzero elements of \( \mathcal{O}_K \) for all \( 1 \leq i \leq e \). Hence,

\[
 \|a + t_\mathfrak{P} b\| \geq \sqrt{\sum_{i=1}^{e} \|a_i + t_\mathfrak{P} b_i\|^2} \geq \sqrt{e} \geq d_H(C).
\]

Next we look at the density of \( C + t_\mathfrak{P} \mathcal{P} \). Denote by \( d \) the Euclidean distance of \( C + t_\mathfrak{P} \mathcal{P} \). Then \( d \geq \sqrt{qd_E(\mathcal{P})} \) if \( d_H(C) \geq q(d_E(\mathcal{P}))^2 \). We denote by \( V_n \) the volume of a unit ball in \( \mathbb{R}^n \). We also denote by \( B_m(b) \) the ball of radius \( b \)

\[
 \{(a_1, \ldots, a_m) \in \mathbb{R}^m : \sqrt{a_1^2 + \cdots + a_m^2} \leq b\}.
\]

Then, a point \( u \) belongs to \( \mathcal{P} \cap B_{2n}(b) \) if and only if \( t_\mathfrak{P} u \) belongs to \( t_\mathfrak{P} \mathcal{P} \cap B_{2n}(\sqrt{q} b) \). This means that \( |\mathcal{P} \cap B_{2n}(b)| = |t_\mathfrak{P} \mathcal{P} \cap B_{2n}(\sqrt{q} b)| \). Furthermore, let \( s := \max\{||c|| : c \in C\} \), then for any \( c \in C \) and \( v \in t_\mathfrak{P} \mathcal{P} \cap B_{2n}(\sqrt{q} b) \), we have \( c + v \in (c + t_\mathfrak{P} \mathcal{P}) \cap B_{2n}(\sqrt{q} b + s) \). This implies that

\[
 |(c + t_\mathfrak{P} \mathcal{P}) \cap B_{2n}(\sqrt{q} b + s)| \geq |t_\mathfrak{P} \mathcal{P} \cap B_{2n}(\sqrt{q} b)| = |\mathcal{P} \cap B_{2n}(b)|.
\]

Hence, we have

\[
 \Delta(C + t_\mathfrak{P} \mathcal{P}) = \limsup_{b \to \infty} \frac{|(C + t_\mathfrak{P} \mathcal{P}) \cap B_{2n}(\sqrt{q} b + s + d/2)|}{\text{vol}(B_{2n}(\sqrt{q} b + s + d/2))} \geq \limsup_{b \to \infty} \frac{|\mathcal{P} \cap B_{2n}(b)|}{\text{vol}(B_{2n}(\sqrt{q} b + s + d/2))}.
\]
Corollary 2.4. Let $P \subseteq O_K^n$ be a packing in $\mathbb{R}^{2n}$.

(i) Let $\{C_i = (n, M_i, \geq 3^{m-i}(d_E(P))^2)\}_{i=0}^{m-1}$ be a sequence of ternary codes, then the density of $C_0 + (\sqrt{-3})C_1 + \cdots + (\sqrt{-3})^{m-1}C_{m-1} + (\sqrt{-3})^mP$ as a packing in $\mathbb{R}^{2n}$ is at least $\Delta(P) \prod_{i=0}^{m-1} M_i$.

(ii) If $p$ is inert in $K/\mathbb{Q}$ and $\{C_i = (n, M_i, \geq p^{2(m-n)}(d_E(P))^2)\}_{i=0}^{m-1}$ be a sequence of $p^2$-ary codes, then the density of $C_0 + pC_1 + \cdots + p^{m-1}C_{m-1} + p^mP$ as a packing in $\mathbb{R}^{2n}$ is at least $\Delta(P) \prod_{i=0}^{m-1} M_i$.

(iii) Assume that $p$ splits in $K/\mathbb{Q}$. Let $P$ be a prime ideal of $K$ lying over $p$ with $F_P \simeq \mathbb{F}_p$ and let $t_P$ be a generator of $P$. If $\{C_i = (n, M_i, \geq p^{m-n}(d_E(P))^2)\}_{i=0}^{m-1}$ be a sequence of $p$-ary codes, then the density of $C_0 + t_PC_1 + \cdots + t^{m-1}_PC_{m-1} + t^m_P \mathbb{Z}$ as a packing in $\mathbb{R}^{2n}$ is at least $\Delta(P) \prod_{i=0}^{m-1} M_i$.

By induction, we get the following corollary from Proposition 2.3.

Corollary 2.5. Let $P \subseteq O_K^n$ be a lattice packing of dimension $2n+m$ in $\mathbb{R}^{2n+m}$. Let $P$ be a prime ideal in $O_K$ with $F_P \simeq \mathbb{F}_q$.

(i) If $C$ is a $q$-ary code of length $n+m$ with the Hamming distance $d_H(C)$ and size $M$, then the Euclidean distance of the packing

$$R := C + \left\{(t_Q u, q v) : u \in O_K^n, v \in \mathbb{Z}^m, (u, v) \in P\right\}$$

(note that for a codeword of $C$, the first $n$ coordinates are taken from the set $\{\alpha_1, \ldots, \alpha_q\}$, while the last $m$ coordinates are taken from the set $\{0, 1, \ldots, q-1\}$) is at least $\min\{\sqrt{d_H(C)}, \sqrt{q d_E(P)}\}$, where $t_Q$ is a generator of the prime ideal $P$. Furthermore, the density of the packing $R$ in $\mathbb{R}^{2n+m}$ is at least $\Delta(P) M/q^{m/2}$ if $d_H(C) \geq q(d_E(P))^2$.

(ii) If $C$ satisfies that for $x, y \in C$, the sum $x + y$ is equal to $z + (t_Q u, q v)$ for some $z \in C$ and $(u, v) \in P$, then $R$ is also a lattice.

Proof. By using the similar arguments as in the proof of Proposition 2.3(i), we can easily show that the Euclidean distance of the packing $R$ is at least $\min\{\sqrt{d_H(C)}, \sqrt{q d_E(P)}\}$.

Next we look at the density of $R$. Denote by $d$ the Euclidean distance of $R$. Then $d \geq \sqrt{q d_E(P)}$ if $d_H(C) \geq q(d_E(P))^2$. 
Let \(\{u_1 + iv_1, e_1\}, \ldots, (u_{2n+m} + iv_{2n+m}, e_{2n+m})\} \) with \(u_j, v_j \in \mathbb{R}^n, e_j \in \mathbb{Z}^m\) be a basis of \(\mathcal{P}\). Then the set \(\{(t q_1 u_1 + iv_1, q e_1), \ldots, (t q_1 u_{2n+m} + iv_{2n+m}, q e_{2n+m})\}\) is a basis of the lattice \(T := \{(t q_1 u, q v) : u \in \mathcal{O}_K^n, v \in \mathbb{Z}^m, (u, v) \in \mathcal{P}\}\).

Let \(t q_1 = a + ci\). Then \(a^2 + c^2 = q\) and we get the Gram matrix of \(T\)

\[
M := \begin{pmatrix}
(a u_1 - c v_1, c u_1 + a v_1, q e_1) \\
\vdots \\
(a u_{2n+m} - c v_{2n+m}, c u_{2n+m} + a v_{2n+m}, q e_{2n+m})
\end{pmatrix}
\]

\[
= \begin{pmatrix}
(u_1, v_1, e_1) \\
\vdots \\
(u_{2n+m}, v_{2n+m}, e_{2n+m})
\end{pmatrix} \times \begin{pmatrix}
a I_n & c I_n & 0 \\
-c I_n & a I_n & 0 \\
0 & 0 & q I_m
\end{pmatrix},
\]

where \(I_n\) denotes the identity matrix of size \(n\). Thus,

\[
\text{discr}(T) = \det(M^T M) = (a^2 + c^2)^{2n} q^{2m} \text{discr}(\mathcal{P}) = q^{2n+2m} \text{discr}(\mathcal{P}).
\]

This means that for a sufficiently large \(b > 0\), the ball \(B_{2n+m}(b)\) contains about \([\text{vol}(B_{2n+m}(b))]/\sqrt{\text{discr}(T)}\) points of \(\mathcal{T}\), i.e.,

\[
\lim_{b \to +\infty} \frac{|B_{2n+m}(b) \cap \mathcal{T}|}{\text{vol}(B_{2n+m}(b))} = \frac{1}{q^{n-m} \sqrt{\text{discr}(\mathcal{P})}}.
\]

Let \(s := \max\{|e| : e \in \mathcal{C}\}\). Then for any \(e \in \mathcal{C}\) and \(v \in \mathcal{T} \cap B_{2n+m}(b)\), the point \(e + v\) belongs \(R \cap B_{2n+m}(b + s)\), i.e., \(|R \cap B_{2n+m}(b + s)| \geq |C| \times |\mathcal{T} \cap B_{2n+m}(b)|\).

Finally we get

\[
\Delta(R) = \limsup_{b \to +\infty} \frac{|R \cap B_{2n+m}(b + s)|(d/2)^{2n+m} V_{2n+m}}{\text{vol}(B_{2n+m}(b + s + d/2))}
\]

\[
\geq \limsup_{b \to +\infty} \frac{|C| \cdot |\mathcal{T} \cap B_{2n+m}(b)|(\sqrt{q d_E(\mathcal{P})/2})^{2n+m} V_{2n+m}}{\text{vol}(B_{2n+m}(b + s + d/2))}
\]

\[
= \left( \limsup_{b \to +\infty} \frac{|\mathcal{T} \cap B_{2n+m}(b)|}{\text{vol}(B_{2n+m}(b))} \times \frac{\text{vol}(B_{2n+m}(b))}{\text{vol}(B_{2n+m}(b + s + d/2))} \right) 
\times M(\sqrt{q})^{2n+m} (d_E(\mathcal{P})/2)^{2n+m} V_{2n+m}
\]

\[
= M(\sqrt{q})^{2n+m} (d_E(\mathcal{P})/2)^{2n+m} V_{2n+m}
\]

\[
= \frac{\Delta(\mathcal{P}) M}{q^{m/2}}.
\]

This completes the proof of part (i). Again, part (ii) is obvious. \(\square\)

From the above concatenation, we have to find codes with large Hamming distance and dense packings \(\mathcal{P} \subseteq \mathcal{O}_K^n\). We have already some methods to construct good codes from coding theory (for instance, see \([3,5,7,10,13]\)). Next, we will concentrate on finding good packings \(\mathcal{P}\).

**Proposition 2.6.** Let \(\Lambda\) be a lattice of dimension \(n\) in \(\mathbb{R}^n\).

(i) The discriminant \(\text{discr}(\Lambda + \omega \Lambda)\) of the lattice \(\Lambda + \omega \Lambda \subseteq \mathbb{R}^{2n}\) is equal to \((\frac{3}{4})^n (\text{discr}(\Lambda))^2\). 

(ii) The volume \(\text{vol}(\Lambda + \omega \Lambda)\) of the lattice \(\Lambda + \omega \Lambda \subseteq \mathbb{R}^{2n}\) is equal to \((\frac{3}{4})^{n/2} \text{vol}(\Lambda)^2\). 

(iii) The minimal norm \(\lambda_{\min}(\Lambda + \omega \Lambda)\) of the lattice \(\Lambda + \omega \Lambda \subseteq \mathbb{R}^{2n}\) is equal to \(\lambda_{\min}(\Lambda)\).

(iv) The minimal determinant \(\Delta_{\min}(\Lambda + \omega \Lambda)\) of the lattice \(\Lambda + \omega \Lambda \subseteq \mathbb{R}^{2n}\) is equal to \(\lambda_{\min}(\Lambda)\).
(ii) If \( n \) is even, then the discriminant \( \text{discr}(A^{(h)}) \) of the lattice \( A^{(h)} \subseteq \mathbb{R}^n \) is equal to 
\[
\left( \frac{\sqrt{3}}{2} \right)^n \text{discr}(A).
\]

**Proof.** Let \( \{e_1, \ldots, e_n\} \) be a \( \mathbb{Z} \)-basis of \( A \).

(i) It is easy to see that \( \{e_1, \ldots, e_n, \omega e_1, \ldots, \omega e_n\} \) forms a \( \mathbb{Z} \)-basis of \( A + \omega A \), i.e., \( \{(e_1, 0), \ldots, (e_n, 0), (-1/2)e_1, (\sqrt{3}/2)e_1), \ldots, (-1/2)e_n, (\sqrt{3}/2)e_n\} \) is a basis of \( A + \omega A \) over \( \mathbb{Z} \). Hence, we get the Gram matrix of \( A + \omega A \)
\[
\begin{pmatrix}
(e_1, 0) \\
\vdots \\
(e_n, 0) \\
(-1/2)e_1, (\sqrt{3}/2)e_1) \\
\vdots \\
(-1/2)e_n, (\sqrt{3}/2)e_n)
\end{pmatrix}
\times
\begin{pmatrix}
(e_1, 0) \\
\vdots \\
(e_n, 0) \\
(-1/2)e_1, (\sqrt{3}/2)e_1) \\
\vdots \\
(-1/2)e_n, (\sqrt{3}/2)e_n)
\end{pmatrix}^T
= \begin{pmatrix} A & -1/2 A \\ -1/2 A & A \end{pmatrix}.
\]
where \( A \) denotes the Gram matrix \( (\langle e_i, e_j \rangle)_{1 \leq i, j \leq n} \) and \( \langle e_i, e_j \rangle \) denotes the usual inner product. Thus,
\[
\text{discr}(A + \omega A) = \det \begin{pmatrix} A & -1/2 A \\ -1/2 A & A \end{pmatrix} = \det \begin{pmatrix} A & -1/2 A \\ O & 3/4 A \end{pmatrix} = \left( \frac{3}{4} \right)^n \det(A)^2 = \left( \frac{3}{4} \right)^n (\text{discr}(A))^2.
\]
This finishes the proof of part (i).

(ii) Split \( e_i \) into \( (a_i, b_i) \) with \( a_i, b_i \in \mathbb{R}^{n/2} \). Then it is clear that \( \{(a_1 - \frac{1}{2} b_1, \frac{\sqrt{3}}{2} b_1), \ldots, (a_n - \frac{1}{2} b_n, \frac{\sqrt{3}}{2} b_n)\} \) forms a basis of \( A^{(h)} \) over \( \mathbb{Z} \). Hence, we get the Gram matrix of \( A^{(h)} \)
\[
M := \begin{pmatrix} (a_1 - \frac{1}{2} b_1, \frac{\sqrt{3}}{2} b_1) \\
\vdots \\
(a_n - \frac{1}{2} b_n, \frac{\sqrt{3}}{2} b_n) \end{pmatrix}
= \begin{pmatrix} (a_1, b_1) \\
\vdots \\
(a_n, b_n) \end{pmatrix} \times \begin{pmatrix} I_{n/2} & O \\ -\frac{1}{2} I_{n/2} & \frac{\sqrt{3}}{2} I_{n/2} \end{pmatrix},
\]
where \( I_{n/2} \) denotes the identity matrix of size \( n/2 \). Thus,
\[
\text{discr}(A^{(h)}) = \det(M^T M) = \left( \frac{\sqrt{3}}{2} \right)^n \text{discr}(A).
\]
This finishes the proof. \( \square \)

For a packing \( \mathcal{P} \in \mathbb{R}^n \), we define the center density of \( \mathcal{P} \) by \( \delta(\mathcal{P}) := \Delta(\mathcal{P})/V_n \).

**Proposition 2.7.** For every even \( n \), the center density and minimum norm of the lattice \( T_n^{(h)} \) are \( 3^{-1-n/4} \) and \( \sqrt{2} \), respectively, where
\[
T_n := \left\{ \begin{array}{l}
(a_1, \ldots, a_n) \in \mathbb{Z}^n: \sum_{i=1}^n a_i \equiv 0 \text{ (mod 3)}
\end{array} \right\}.
\]

**Proof.** We first prove that \( d_E(T_n^{(h)}) = \sqrt{2} \). Let \( (u, v) \) be a nonzero point in \( T_n \). We have to show that \( ||u + \omega v||^2 \geq 2 \).
Case 1. \( \|v\|^2 \geq 2 \). Then

\[
\|u + \omega v\|^2 = \left\| u - \frac{1}{2} v \right\|^2 + \left\| \frac{\sqrt{3}}{2} v \right\|^2 \geq \frac{3}{4} \times 2 = \frac{3}{2}.
\]

As \( \|u + \omega v\|^2 \) is an integer, we get \( \|u + \omega v\|^2 \geq 2 \).

Case 2. \( \|v\|^2 = 0 \). Then \( v = 0 \) and

\[
\|u + \omega v\|^2 = \|u\|^2 \geq (d_E(T_n))^2 = 2.
\]

Case 3. \( \|v\|^2 = 1 \). Then \( \|u\|^2 \geq 1 \). If \( \|u\|^2 = 1 \), then we must have either, \( u = (0, \ldots, 0, 1, 0, \ldots, 0) \) and \( v = (0, \ldots, 0, -1, 0, \ldots, 0) \), or \( u = (0, \ldots, 0, -1, 0, \ldots, 0) \) and \( v = (0, \ldots, 0, 1, 0, \ldots, 0) \). It is easy to verify that \( \|u + \omega v\|^2 = 2 \) or \( 3 \).

If \( \|u\|^2 \geq 2 \), then

\[
\|u + \omega v\|^2 = \left\| u - \frac{1}{2} v \right\|^2 + \left\| \frac{\sqrt{3}}{2} v \right\|^2 \geq \left( 1 - \frac{1}{2} \right)^2 + 1^2 + \frac{3}{4} = 2.
\]

Thus, by Proposition 2.6(ii), the center density of \( T_n^{(h)} \) is

\[
\delta(T_n^{(h)}) = \frac{1}{3} \times \left( \frac{\sqrt{3}}{2} \right)^n \times \left( \frac{\sqrt{3}}{2} \right)^{-n/2} = 3^{-1-n/4}.
\]

The proof is completed. \( \square \)

Example 2.8. Let \( A_{n-1} \) denote the lattice

\[
\left\{ (a_1, \ldots, a_n) \in \mathbb{Z}^n : \sum_{i=1}^n a_i = 0 \right\}.
\]

Then, the dimension, the minimum norm and the discriminant of \( A_{n-1} \) are \( n - 1 \), \( 2 \) and \( n \), respectively. Furthermore, \( A_{n-1}^{(h)} \) is a subset of \( T_n^{(h)} \) and hence the minimum norm of the lattice \( A_{n-1}^{(h)} \) is at least 2 for every even number \( n \geq 2 \). In fact, one can easily check that the minimum norm of \( A_{n-1}^{(h)} \) is 2.

Let \( e_1 = (-1 - 2\omega, -1 - 2\omega, -1 - 2\omega, 2 + \omega, 2 + \omega, 2 + \omega) \), \( e_2 = (1, -1, 0, 0, 0, 0) \), \( e_3 = (0, 1, -1, 0, 0, 0) \), \( e_4 = (0, 0, 1, -1, 0, 0) \), \( e_5 = (0, 0, 0, 1, -1, 0) \), \( e_6 = (0, 0, 0, 0, 1, -1) \), \( e_7 = (-\omega, 0, 0, 0, 0, 1) \), \( e_8 = (\omega, -\omega, 0, 0, 0, 0) \), \( e_9 = (0, 0, -\omega, 0, 0, 0) \), \( e_{10} = (0, 0, \omega, -\omega, 0, 0) \), \( e_{11} = (0, 0, 0, \omega, -\omega, 0) \). Then the set \( \{e_1, \ldots, e_{11}\} \) forms a basis of \( A_{11}^{(h)} \) (note that this basis is obtained from a basis of \( A_{11} \)).

Consider the set

\[
C := \left\{ (0, 0, 0, 0, 0, 0), (1, 1, 1, \omega, \omega, \omega), -(1, 1, 1, \omega, \omega, \omega) \right\}.
\]

Then \( C \) is in fact a trivial ternary \([6, 1, 6]-\)linear code when the coordinates of the vectors in \( C \) are viewed as elements in the residue class field of the ideal \( \sqrt{-3}\mathcal{O}_K \) of \( K \) (note that \( \omega \equiv 1 \) mod \( \sqrt{-3}\mathcal{O}_K \)).

From the fact that

\[
3(1, 1, 1, \omega, \omega, \omega) = \sqrt{-3}e_1 \in \sqrt{-3}A_{11}^{(h)},
\]

we know that the set

\[
C + \sqrt{-3}A_{11}^{(h)} := \{ c + \sqrt{-3}u : c \in C; u \in A_{11}^{(h)} \}
\]

is a lattice with a basis \( \{(1, 1, 1, \omega, \omega, \omega), \sqrt{-3}e_2, \ldots, \sqrt{-3}e_{11}\} \).
The Euclidean distance of $C + \sqrt{-3}A_{11}^{(h)}$ is $\sqrt{6}$ as we have seen in the proof of Proposition 2.3(i).

As a basis of $C + \sqrt{-3}A_{11}^{(h)}$ is given explicitly, we can compute its discriminant and it is equal to $3^{16}/2^9$ (this computation was carried out using the software Mathematica). Therefore, the center density of $C + \sqrt{-3}A_{11}^{(h)}$ is equal to

$$\left(\frac{\sqrt{6}}{2}\right)^{11} \times \frac{2^{4.5}}{3^{8}} = \frac{1}{18\sqrt{3}}.$$ 

This achieves the best-known density for lattices of dimension 11 (see [17]).

**Example 2.9.**

(i) $n = 8$. Let $C$ be a ternary [4, 2, 3]-linear code. Then by Propositions 2.3(i) and 2.6(i), the center density of $C + \sqrt{-3}O_K^4$ is at least

$$|C| \times \delta(O_K^4) = 9 \times \left(\frac{1}{2}\right)^8 \times \left(\frac{2}{\sqrt{3}}\right)^4 = \frac{1}{16}.$$ 

This achieves the best-known density for dimension 8 (see [17]). It follows from Proposition 2.3(ii) that $C + \sqrt{-3}O_K$ is a lattice.

(ii) $n = 12$. Let $C$ be a ternary [6, 1, 6]-linear code. Then by Propositions 2.3(i) and 2.7, the center density of $C + \sqrt{-3}T_{12}^{(h)}$ is at least $|C| \times 3^{-4} = 1/27$. This achieves the best-known density for dimension 12 (see [17]). In fact, this is a lattice packing.

Let $\{e_1, \ldots, e_{11}\}$ be the basis of $A_{11}^{(h)}$ defined in Example 2.8. Put $e_{12} = (0, 0, 0, 1, 1, 1)$, then $\{e_1, \ldots, e_{11}, e_{12}\}$ forms a basis of $T_{12}^{(h)}$. Thus, $\{(1, 1, 1, \omega, \omega, \omega), \sqrt{-3}e_2, \ldots, \sqrt{-3}e_{12}\}$ is a basis of $C + \sqrt{-3}T_{12}^{(h)}$.

Prof. Gabi Nebe [12] showed that this lattice is in fact the Coxeter Todd lattice up to some scaling factor.

(iii) $n = 36$. Let $C$ be a quaternary [18, 9, 8]-linear code. Then by Propositions 2.3(i) and 2.7, the center density of $C + 2T_{36}^{K}$ is at least $|C| \times 3^{-10} = 4^9/3^{10}$. This achieves the best-known density for dimension 36 (see [17]). Furthermore, if we let the code alphabet set of $C$ be $\{0, 1, \omega, 1 + \omega\}$, then it is not difficult to verify by Proposition 2.3(ii) that $C + 2T_{36}^{K}$ is a lattice.

(iv) $n = 60$. Let $C_1$ and $C_2$ be a ternary [30, 26, 3]-linear code and a quaternary [30, 15, 12]-linear code, respectively. Then by Propositions 2.3(i) and 2.6(i), the center density of $C_2 + 2C_1 + 2\sqrt{-3}O_K^{30}$ is

$$|C_1| \times |C_2| \times \left(\frac{1}{2}\right)^{60} \times \left(\frac{2}{\sqrt{3}}\right)^{30} = 3^{11}.$$ 

Note that $C_1 + \sqrt{-3}O_K^{30}$ is a lattice. However, we are not sure if $C_2 + 2C_1 + 2\sqrt{-3}O_K^{30}$ is a lattice since it is not easy to check the conditions in Proposition 2.3(ii) for $C_2$.

(v) $n = 62$. Let $C_1$ and $C_2$ be a ternary [31, 27, 3]-linear code and a quaternary [31, 15, 12]-linear code, respectively. Then by Propositions 2.3(i) and 2.6(i), the center density of $C_2 + 2C_1 + 2\sqrt{-3}O_K^{31}$ is

$$|C_1| \times |C_2| \times \left(\frac{1}{2}\right)^{62} \times \left(\frac{2}{\sqrt{3}}\right)^{31} = 3^{11.5}.$$ 

Again, for the same reason, we are not sure if $C_2 + 2C_1 + 2\sqrt{-3}O_K^{31}$ is a lattice.
Example 2.10.

(i) $n = 7$. Let $C$ be a ternary $[4, 2, 3]$-linear code and consider the lattice $O_K^3 \times \mathbb{Z}$. Then by Propositions 2.5 and 2.6(i), the center density of $C + \sqrt{-3}O_K^3 \times 3\mathbb{Z}$ is
\[
|C| \times \left(\frac{1}{2}\right)^7 \times \left(\frac{2}{\sqrt{3}}\right)^3 \times \frac{1}{\sqrt{3}} = \frac{1}{16}.
\]
This packing achieves the best-known density for dimension 7.

(ii) Consider the lattice $T_{35}$ defined in Proposition 2.7. Thus, we get a lattice $Q := \left\{ (u + \omega v, c) : u, v \in \mathbb{Z}^{17}, c \in \mathbb{Z}, (u, v, c) \in T_{35} \right\} \subset O_K^{17} \times \mathbb{Z}$. It is easy to see that the Euclidean distance of $Q$ is $\sqrt{2}$. Similar to Proposition 2.6, we can show that the discriminant of $Q$ is $\left(\frac{3}{4}\right)^{17} \text{discr}(T_{35}) = 3^{19}/4^{17}$. Thus, the center density of $Q$ is
\[
\delta(Q) = \left(\frac{\sqrt{2}}{2}\right)^{35} \times \frac{1}{\text{discr}(Q)} = \frac{1}{3^9 \sqrt{6}}.
\]
Let $C$ be a quaternary $[18, 9, 8]$-linear code.

Put $R := \left\{ (2u + 2\omega v, 4c) : (u, \omega v, c) \in Q \right\} \subset O_K^{17} \times \mathbb{Z}$.

By Proposition 2.5, the center density of $C + R$ is
\[
4^9 \times \delta(Q)/\sqrt{4} = 2^{16.5} \approx 2.719.
\]
This is close to the best-known center density 2.828 for packings in $\mathbb{R}^{35}$.

(iii) $n = 59$. Let $C_1$ and $C_2$ be a ternary $[30, 26, 3]$-linear code and a quaternary $[30, 15, 12]$-linear code, respectively. It is clear that $C_1 + \sqrt{-3}O_K^{29} \times 3\mathbb{Z}$ is a lattice. Then by Propositions 2.5 and 2.6(i), the center density of $C_2 + \{(2u, 4v) : (u, v) \in C_1 + \sqrt{-3}O_K^{29} \times 3\mathbb{Z}\}$ is
\[
|C_1| \times |C_2| \times \left(\frac{1}{2}\right)^{59} \times \left(\frac{2}{\sqrt{3}}\right)^{29} \times \frac{1}{\sqrt{12}} = \frac{3^{11}}{2}.
\]

(iv) $n = 61$. Let $C_1$ and $C_2$ be a ternary $[31, 27, 3]$-linear code and a quaternary $[31, 15, 12]$-linear code, respectively. It is clear that $C_1 + \sqrt{-3}O_K^{30} \times 3\mathbb{Z}$ is a lattice. Then by Propositions 2.5 and 2.6(i), the center density of $C_2 + \{(2u, 4v) : (u, v) \in C_1 + \sqrt{-3}O_K^{30} \times 3\mathbb{Z}\}$ is
\[
|C_1| \times |C_2| \times \left(\frac{1}{2}\right)^{61} \times \left(\frac{2}{\sqrt{3}}\right)^{30} \times \frac{1}{\sqrt{12}} = \frac{3^{11.5}}{4}.
\]

Remark 2.11.

(i) The construction in this section does not assume that the used codes are linear. Unfortunately, we cannot use nonlinear binary codes as 2 is inert in $K/\mathbb{Q}$. On the other hand, there is no much research on nonlinear nonbinary codes. One of the referees and I tried some nonlinear nonbinary codes and no new packings were found. We could also consider ternary/quaternary mixed codes for our construction.
(ii) The construction in this section can be generalized to an arbitrary number field $F$. One requirement for this generalization is that the discriminant of $F$ must be as small as possible.

3. Asymptotic result

Before talking further about packings, we need to introduce some technical notations and results from coding theory.

For a code $C$ over $\mathbb{F}_q$, we denote by $n(C), M(C),$ and $d(C)$ the length, the size, and the minimum distance of $C$, respectively. Let $U_q$ be the set of ordered pairs $(\delta, R) \in \mathbb{R}^2$ for which there exists a family $\{C_i\}_{i=1}^\infty$ of codes over $\mathbb{F}_q$ with $n(C_i) \to \infty$ and

$$\delta = \lim_{i \to \infty} \frac{d(C_i)}{n(C_i)}, \quad R = \lim_{i \to \infty} \frac{\log_q M(C_i)}{n(C_i)}.$$

The following description of $U_q$ can be found in Section 1.3.1 of [19].

**Proposition 3.1.** There exists a continuous function $R_q(\delta), \delta \in [0, 1]$, such that

$$U_q = \{(\delta, R) \in \mathbb{R}^2: 0 \leq R \leq R_q(\delta), \ 0 \leq \delta \leq 1\}.$$

Moreover, $R_q(0) = 1$, $R_q(\delta) = 0$ for $\delta \in [(q-1)/q, 1]$, and $R_q(\delta)$ decreases on the interval $[0, (q-1)/q]$.

For $0 < \delta < 1$, define the $q$-ary entropy function

$$H_q(\delta) := \delta \log_q (q-1) - \delta \log_q \delta - (1-\delta) \log_q (1-\delta),$$

and put

$$R_{GV}(q, \delta) := 1 - H_q(\delta).$$

Then the Gilbert–Varshamov bound says that

$$R_q(\delta) \geq R_{GV}(q, \delta) \quad \text{for all } \delta \in \left(0, \frac{q-1}{q}\right).$$

The above bound follows from the finite version of the Gilbert–Varshamov bound which states that one always has a $q$-ary $(n, q^n / \sum_{j=0}^{d-1} \binom{n}{j}(q-1)^j, d)$-code for any $1 \leq d \leq n$ (see [1,19]).

On the other hand, there are several upper bounds developed by Aaltonen, Ben-Haim and Litsyn, and McEliece, Rodemich, Rumsey and Welch (see [1,2,11]). Put

$$R_{LP1}(q, \delta) = H_q \left( \frac{q-1 - (q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)}}{q} \right).$$

Then the first linear programming bound (see [11]) tells us

$$R_q(\delta) \leq R_{LP1}(q, \delta) \quad \text{for all } \delta \in \left(0, \frac{q-1}{q}\right).$$

There are the second, third linear programming bounds and shortening bound [1,2]. It is quite complicated to state these bounds. Since we require only some numerical results from these bounds, we do not state these bounds in the present paper. The reader may refer to the most recent paper of Ben-Haim and Litsyn [2] on these bounds. Define the function

$$R_U(q, \delta) := \min \{R_{LP2}(q, \delta), R_{LP3}(q, \delta), R_{sho}(q, \delta)\},$$
where \( R_{LP2}(q, \delta) \), \( R_{LP3}(q, \delta) \), \( R_{sho}(q, \delta) \) stand for the second linear programming bound (see Theorem 1 of [2]), the third linear programming bound (see Theorem 7 of [2]) and the shortening bound (see Theorem 2 of [2]), respectively. Combining these three bounds, we get

\[
R_q(\delta) \leq R_U(q, \delta) \quad \text{for all } \delta \in \left(0, \frac{q-1}{q}\right).
\]

(3.1)

Theorem 3.2. If \( q \) is a prime power such that there exists a prime ideal \( \mathfrak{P} \) of \( \mathcal{O}_K \) with \( F_\mathfrak{P} \) isomorphic to \( F_q \), then we have

\[
\lambda \geq -\frac{1}{2} - \frac{1}{4} \log_2 3 + \frac{1}{2} \log_2 \pi e + \frac{1}{2} \log_2 x + \frac{1}{2} \log_2 (q) \left( \sum_{j=\lceil \log_q x \rceil}^{\infty} \left( R_q \left( \frac{x}{q^j} \right) - 1 \right) - \left\lfloor \log_q x \right\rfloor \right)
\]

for any integer \( x \geq 1 \), where \( e \) is the base for the natural logarithm.

Proof. Let \( p \) be the smallest prime such that \( p \geq x \). Let \( \{C_n\} \) be a family of \( p \)-ary \( [n, k_\chi, x] \)-linear codes such that \( \lim_{n \to \infty} k_\chi / n = 1 \). Then \( \mathcal{P}_n := (C_n + p\mathbb{Z}^n) + \omega(C_n + p\mathbb{Z}^n) \) is a lattice in \( \mathcal{O}_K^n \). It is a packing in \( \mathbb{R}^{2n} \) with minimum norm at least \( x \). The discriminant of the lattice \( C_n + p\mathbb{Z}^n \) is \( p^2 k_\chi \) (for determination of this discriminant, the reader may refer to [6] or compute it by using the similar arguments as in the proof of Proposition 2.3(i)). By Proposition 2.6(i), the discriminant of \( \mathcal{P}_n \) is

\[
\left( \frac{3}{4} \right)^n \times p^{4n-4k_\chi}.
\]

Let \( \{D_i^{(n)}\} \) be a family of \( q \)-ary \( (n, M_i^{(n)}, x \cdot q^i) \)-codes for all \( 1 \leq i \leq m := \lceil \log_q (n/x) \rceil \).

Let \( t_\mathfrak{P} \) be a generator of \( \mathfrak{P} \). Then, it follows from Proposition 2.3 and induction that the density of the packing

\[
D_m + t_\mathfrak{P} D_{m-1} + \cdots + t_\mathfrak{P}^{m-1} D_1 + t_\mathfrak{P}^m \mathcal{P}_n
\]

is at least

\[
\Delta(\mathcal{P}_n) \prod_{i=1}^{m} M_i^{(n)} \geq \left( \frac{2}{\sqrt{3}} \right)^n \times V_{2n} \times p^{2k_\chi-2n} \times \left( \frac{\sqrt{x}}{2} \right)^{2n} \prod_{i=1}^{m} M_i^{(n)}.
\]

Take \( n = q^a \) for a positive integer \( a \) and let \( a \) tend to \( \infty \).

Fix a sufficiently large integer \( \ell \) with \( \lceil \log_q x \rceil < \ell < a \). Choose the codes \( D_i^{(n)} \) such that

\[
\lim_{n \to \infty} \frac{\log_q (M_i^{(n)})}{n} = R_q \left( \frac{x \cdot q^i}{n} \right) = R_q \left( \frac{x}{q^a-i} \right)
\]

for \( i = a - \lceil \log_q x \rceil, \ldots, a - \ell \) and

\[
M_i^{(n)} \geq \frac{q^n}{\sum_{j=0}^{xq^i-1} \binom{n}{j}(q-1)^j}
\]

for all \( i = a - \ell - 1, \ldots, 1 \). Hence,
Let \( \ell \) tend to \( \infty \), we obtain the desired result. \( \Box \)

**Corollary 3.3.** If \( q \) is a prime power such that there exists a prime ideal \( \mathfrak{p} \) of \( \mathcal{O}_K \) with \( F_{\mathfrak{p}} \) isomorphic to \( \mathbb{F}_q \), then for any real number \( z \) with \( 1/q < z < 1 \), we have

\[
\lambda \geq -\frac{1}{2} - \frac{1}{4} \log_2 3 + \frac{1}{2} \log_2 \pi e + \frac{1}{2} \log_2 2 + \frac{1}{2} \log_2 q \sum_{j=0}^{\infty} \left( R_q \left( \frac{z}{q^j} \right) - 1 \right) - \left[ \log_q x \right].
\]

(3.2)

**Proof.** Let \( \{x\} \) be a family of integers with \( x \to \infty \) such that

\[
\log_2 x - \left[ \log_2 x \right] \to \log_q z
\]
as \( x \) tends to \( \infty \). Then

\[
\lim_{x \to \infty} \frac{x}{q \left[ \log_q x \right]} = z.
\]

Hence, by Theorem 3.2 we have

\[
\lambda \geq -\frac{1}{2} - \frac{1}{4} \log_2 3 + \frac{1}{2} \log_2 \pi e + \frac{1}{2} \log_2 2 + \frac{1}{2} \log_2 q \sum_{j=0}^{\infty} \left( R_q \left( \frac{z}{q^j} \right) - 1 \right) - \left[ \log_q x \right].
\]

This finishes the proof. \( \Box \)
**Theorem 3.4.**

(i) If the bound (3.1) could be achieved for ternary codes, then the Minkowski bound can be improved to $\lambda \geq -0.8892$.

(ii) If the bound (3.1) could be achieved for quaternary codes, then the Minkowski bound can be improved to $\lambda \geq -0.8589$.

(iii) If the bound (3.1) could be achieved for 7-ary codes, then the Minkowski bound can be improved to $\lambda \geq -0.8471$.

(iv) We have an unconditional lower bound, i.e., $\lambda \geq -1.2653$.

**Proof.** Define the function

$$f(q, z) := -\frac{1}{2} - \frac{1}{4} \log_2 3 + \frac{1}{2} \log_2 \pi e + \frac{1}{2} \log_2 z + \frac{1}{2} \log_2(q) \sum_{j=0}^{\infty} \left( R_U \left( \frac{z}{q^j} \right) - 1 \right).$$

By Corollary 3.3, if $F_q$ is isomorphic to the residue class field $\mathbb{F}_p$ for some prime ideal $p$ in $K$ and the bound (3.1) could be achieved for $q$-ary codes, then we have

$$\lambda \geq f(q, z) \quad \text{for any } 1/q < z < (q - 1)/q.$$

The desired results follow from the facts that 2 is inert, 3 is ramified, 7 splits in $K$, and

$$f(3, 0.351) \approx -0.8892; \quad f(4, 0.352) \approx -0.8589; \quad f(7, 0.334) \approx -0.8471.$$

Put

$$g(q, z) := -\frac{1}{2} - \frac{1}{4} \log_2 3 + \frac{1}{2} \log_2 \pi e + \frac{1}{2} \log_2 z + \frac{1}{2} \log_2(q) \sum_{j=0}^{\infty} \left( R_{GV} \left( \frac{z}{q^j} \right) - 1 \right).$$

By Corollary 3.3, we have

$$\lambda \geq g(4, 0.305) \approx -1.2653.$$

This finishes the proof. $\square$

**Remark 3.5.**

(i) By using the same idea with the lattice $\mathbb{Z}^n$, Litsyn and Tsfasman obtained an unconditional bound $\lambda \geq -1.29$ in [9].

(ii) From Theorem 3.4, one can conjecture that the currently known upper bounds for nonbinary codes are far from being accurate, and most probably can be improved.

**Acknowledgments**

The author is very grateful to the two anonymous referees for their very careful reading of the first version and many invaluable suggestions and comments. Without these suggestions and comments, the paper would not have appeared in the current form. The author also thanks one of the referees for providing me Ref. [2] which is very useful for Section 3. The author thanks Dr. Lanju Xu for many discussions and providing me the numerical results for Theorem 3.4.
References