Canad. Math. Bull. Vol. **54** (4), 2011 pp. 645–653
doi:10.4153/CMB-2011-038-7

An Extension of Craig's Family of Lattices

André Luiz Flores, J. Carmelo Interlando,
and Trajano Pires da Nóbrega Neto

Abstract. Let p be a prime, and let ζ_p be a primitive p-th root of unity. The lattices in Craig's family are $(p-1)$-dimensional and are geometrical representations of the integral $\mathbb{Z}[\zeta_p]$-ideals $\langle 1-\zeta_p\rangle^i$, where i is a positive integer. This lattice construction technique is a powerful one. Indeed, in dimensions $p-1$ where $149 \le p \le 3001$, Craig's lattices are the densest packings known. Motivated by this, we construct $(p-1)(q-1)$-dimensional lattices from the integral $\mathbb{Z}[\zeta_{pq}]$-ideals $\langle 1-\zeta_p\rangle^i\langle 1-\zeta_q\rangle^j$, where p and q are distinct primes and i and j are positive integers. In terms of sphere-packing density, the new lattices and those in Craig's family have the same asymptotic behavior. In conclusion, Craig's family is greatly extended while preserving its sphere-packing properties.

1 Introduction

In this section we briefly review the construction of lattices from number fields and give a summary of our contribution. The main goal is to establish notation. More details on this background material can be found in [1,3] and the references therein.

Let K be a number field of degree d, and let $\sigma_1,\dots,\sigma_d$ be the embeddings ($\mathbb{Q}$-monomorphisms) of K into $\mathbb{C}$, the field of complex numbers. As usual, σ_i is real for $1 \le i \le r$, and σ_{j+s} is the complex conjugate of σ_j for $r+1 \le j \le r+s$. Hence, $d = r+2s$. The canonical embedding $\sigma_K\colon K \to \mathbb{R}^d$ is the injective ring homomorphism defined by

$$\sigma_K(x) = \big(\sigma_1(x),\dots,\sigma_r(x),\Re\sigma_{r+1}(x),\Im\sigma_{r+1}(x),\dots,\Re\sigma_{r+s}(x),\Im\sigma_{r+s}(x)\big),$$

where $\Re z$ and $\Im z$ are the real and imaginary parts of the complex number z, respectively.

Let $\mathfrak{O}_K$ be the ring of algebraic integers of K, and let $\mathfrak{a}$ be a nonzero $\mathfrak{O}_K$-ideal of absolute norm $N_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$. The set $\sigma_K(\mathfrak{a}) = \{\sigma_K(\alpha) \mid \alpha \in \mathfrak{a}\}$, also called the geometric representation of $\mathfrak{a}$, is a d-dimensional point lattice (or lattice, for short) whose fundamental region has volume

$$V(\sigma_K(\mathfrak{a})) = 2^{-s}\sqrt{|\operatorname{Disc}(K)|}\cdot N_{K/\mathbb{Q}}(\mathfrak{a}), \tag{1.1}$$

where $|\operatorname{Disc}(K)|$ is the absolute value of the discriminant of K, see [3, p. 107]. We also say that $\sigma_K(\mathfrak{a})$ is the lattice associated with $\mathfrak{a}$.

Given $\alpha \in \mathfrak{a}$, the squared Euclidean distance between the point $\sigma_K(\alpha) \in \mathbb{R}^d$ and the origin is equal to $|\sigma_K(\alpha)|^2 = c_K \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\bar{\alpha})$, where $c_K = 1$ if K is totally

Received by the editors October 20, 2008.
Published electronically March 10, 2011.
AMS subject classification: **11H31**, 11H55, 11H50, 11R18, 11R04.
Keywords: geometry of numbers, lattice packing, Craig's lattices, quadratic forms, cyclotomic fields.

real, $c_K = \frac{1}{2}$ if K is totally complex, $\operatorname{Tr}_{K/\mathbb{Q}}(\,\cdot\,)$ denotes trace, and $\bar{\alpha}$ is the complex conjugate of α; see [1, p. 225]. The parameter

$$\rho = \tfrac{1}{2}\min\{|\sigma_K(\alpha)| \mid \alpha \in \mathfrak{a}, \alpha \neq 0\}$$

is called the packing radius of $\sigma_K(\mathfrak{a})$.

The center density $\delta(\Lambda)$ of a d-dimensional lattice Λ is equal to $\rho^d/V(\Lambda)$, where $V(\Lambda)$ is the volume of a fundamental region for Λ. The sphere-packing density of Λ is $\Delta = V_d\delta(\Lambda)$, where V_d is the volume of a d-dimensional sphere of radius 1; see [1, pp. 6–13]. In view of (1.1), the center density of the lattice $\sigma_K(\mathfrak{a})$ is given by

$$\delta(\sigma_K(\mathfrak{a})) = \frac{2^s\rho^d}{\sqrt{|\operatorname{Disc}(K)|}\, N_{K/\mathbb{Q}}(\mathfrak{a})}. \tag{1.2}$$

Let F be the field $\mathbb{Q}(\zeta_p)$, and let $\mathfrak{p}$ be the integral $\mathfrak{O}_F$-ideal $\langle 1-\zeta_p\rangle$. The $(p-1)$-dimensional Craig lattice ([1, Ch. 8]) is defined as $A^{(i)}_{p-1} = \sigma_F(\mathfrak{p}^i)$. For $i \leq (p-3)/2$, the packing radius of $A^{(i)}_{p-1}$ is lower bounded by $\sqrt{pi}/2$; see [2]. Moreover, for large $n = p-1$, these lattice packings satisfy

$$\tfrac{1}{n}\log_2\Delta_n \gtrsim -\tfrac{1}{2}\log_2\log_2 n, \tag{1.3}$$

where Δ_n represents the density of the n-dimensional packing; see [1, p. 17].

The contribution of the present work is to extend Craig's technique as follows. Let L be the cyclotomic field $\mathbb{Q}(\zeta_{pq})$, where p and q are distinct primes. Let $\mathfrak{I}_{ij} = \mathfrak{P}^i\mathfrak{Q}^j$ be an integral $\mathfrak{O}_L$-ideal where $\mathfrak{P} = \langle 1-\zeta_p\rangle$ and $\mathfrak{Q} = \langle 1-\zeta_q\rangle$ are also $\mathfrak{O}_L$-ideals, and i and j are positive integers. The new lattices are defined as $\sigma_L(\mathfrak{I}_{ij})$. Note that for each i and j, $\sigma_L(\mathfrak{I}_{ij})$ is an n-dimensional lattice, where $n = (p-1)(q-1)$. In Section 2, we show that the packing radius of $\sigma_L(\mathfrak{I}_{ij})$ is lower bounded by $\sqrt{2pqij}/2$ for $i \leq (p-1)/2$ and $j \leq (q-1)/2$. In Section 3 we calculate the center density of $\sigma_L(\mathfrak{I}_{ij})$ and show that similar to Craig's lattices, the new lattices are asymptotically good with respect to their densities Δ_n; that is, (1.3) holds for large $n = (p-1)(q-1)$.

2 The Packing Radius of $\sigma_L(\mathfrak{I}_{ij})$

In this section we will prove that $\operatorname{Tr}(\xi\bar{\xi}) \geq 4pqij$ for any element $\xi \neq 0$ in $\mathfrak{I}_{ij}$. This is the statement of Theorem 2.6, which will immediately provide a lower bound for the packing radius of $\sigma_L(\mathfrak{I}_{ij})$. A few definitions, observations, and lemmas preceding that result are in order.

Any $x \in \mathbb{Z}[\zeta_{pq}]$ can be expressed as $x = \sum_{k=0}^{p-2} x_k\zeta_p^k$ where $x_k \in \mathbb{Z}[\zeta_q]$ for $k = 0,\dots,p-2$, or as $x = \sum_{k=0}^{q-2} y_k\zeta_q^k$, where $y_k \in \mathbb{Z}[\zeta_p]$ for $k = 0,\dots,q-2$. With this notation in mind, define the mappings

$$\lambda_p\colon \mathbb{Z}[\zeta_{pq}] \to \mathbb{Z}[\zeta_p] \quad \text{by} \quad x = \sum_{k=0}^{q-2} y_k\zeta_q^k \mapsto \sum_{k=0}^{q-2} y_k,$$

and

$$\lambda_q\colon \mathbb{Z}[\zeta_{pq}] \to \mathbb{Z}[\zeta_q] \quad \text{by} \quad x = \sum_{k=0}^{p-2} x_k \zeta_p^k \mapsto \sum_{k=0}^{p-2} x_k.$$

Observe that λ_p (respectively, λ_q) is a homomorphism from the additive group of $\mathbb{Z}[\zeta_{pq}]$ into the additive group of $\mathbb{Z}[\zeta_p]$ (respectively, $\mathbb{Z}[\zeta_q]$). The next two lemmas follow by direct inspection, hence their proofs are omitted.

Lemma 2.1 *Let $w = \sum_{k=0}^{p-2} w_k \zeta_p^k \in \mathbb{Z}[\zeta_p]$. Then*

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(w\bar{w}) = p\Big(\sum_{k=0}^{p-2} w_k^2\Big) - \Big(\sum_{k=0}^{p-2} w_k\Big)^2 = (p-1)\Big(\sum_{k=0}^{p-2} w_k^2\Big) - 2\sum_{k<s} w_k w_s.$$

Lemma 2.2 *Let $x = \sum_{k=0}^{p-2} x_k \zeta_p^k \in \mathbb{Z}[\zeta_{pq}]$. Then*

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\bar{x}) = p\Big(\sum_{k=0}^{p-2} \mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_k\overline{x_k})\Big) - \mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}\Big(\sum_{k=0}^{p-2} x_k\Big)\Big(\sum_{k=0}^{p-2} \overline{x_k}\Big).$$

Lemma 2.3 *Let $x = \sum_{k=0}^{p-2} x_k \zeta_p^k \in \mathbb{Z}[\zeta_{pq}]$. Then $\lambda_q(\zeta_p^a x) = \lambda_q(x) - p x_{p-1-a}$ for any integer a such that $1 \le a < p-1$.*

Proof Write

$$\begin{aligned}\zeta_p^a x &= \zeta_p^a(x_0 + x_1\zeta_p + \cdots + x_{p-2}\zeta_p^{p-2})\\ &= -x_{p-1-a} + (x_0 - x_{p-1-a})\zeta_p + (x_1 - x_{p-1-a})\zeta_p^2 + \cdots + (x_{p-3} - x_{p-1-a})\zeta_p^{p-2}\end{aligned}$$

and calculate λ_q of the latter expression using the definition of the mapping. ■

Lemma 2.4 *Let $x = \sum_{k=0}^{p-2} x_k \zeta_p^k \in \mathbb{Z}[\zeta_{pq}]$, and let $f(X) = \sum_{k=0}^{p-2} x_k X^k \in \mathbb{Z}[\zeta_q][X]$. Let $f^{(k)}(X)$ denote the k-th derivative of f for $0 \le k \le p-1$. If $x \in \mathfrak{p}^i$, where $1 \le i \le p$, then*

$$f(1) \equiv f(1) \equiv \cdots \equiv f^{(i-1)}(1) \equiv 0 \pmod{p\mathbb{Z}[\zeta_q]}.$$

Proof Note that $x \in \mathfrak{p}^i$ if and only if there are polynomials $g(X), h(X) \in \mathbb{Z}[\zeta_q][X]$ such that

$$f(X) = x_0 + x_1 X + \cdots + x_{p-2}X^{p-2} = g(X)(X-1)^i + h(X)(X^p - 1).$$

The proof is completed by successively differentiating both sides with respect to X and evaluating them at $X = 1$. ■

Lemma 2.5 ([2, Lemma 2, p. 149]) *Let $\eta \ne 0$ be an element of $\mathfrak{p}^i$ with $1 \le i \le \frac{p-1}{2}$. Then $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\eta\bar{\eta}) \ge 2pi$.*

Theorem 2.6 *Let $\xi \neq 0$ be an element of $\mathfrak{I}_{ij} = \mathfrak{P}^i\mathfrak{Q}^j$, where $1 \leq i \leq \frac{p-1}{2}$ and $1 \leq j \leq \frac{q-1}{2}$. Then $\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\xi\bar{\xi}) \geq 4pqij$.*

Proof Let $\mathcal{M} = \{\mu \in \mathfrak{I}_{ij} \mid \mu \neq 0 \text{ and } \mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\mu\bar{\mu}) \text{ is minimum}\}$. We can express $\mathcal{M}$ as the disjoint union $\mathcal{M}_0 \cup \mathcal{M}_1$, where $\mathcal{M}_0 = \{\mu \in \mathcal{M} \mid \lambda_p(\mu) = \lambda_q(\mu) = 0\}$ and $\mathcal{M}_1 = \mathcal{M} \setminus \mathcal{M}_0$. The proof is carried out by showing the following claims.

Claim 2.7 *If $\mathcal{M}_0 = \varnothing$, then $\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\xi\bar{\xi}) \geq 4pqij$ for all $\xi \neq 0$ in $\mathfrak{I}_{ij}$.*

Claim 2.8 *If $\mathcal{M}_0 \neq \varnothing$, then $\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\xi\bar{\xi}) \geq 4pqij$ for all $\xi \neq 0$ in $\mathfrak{I}_{ij}$.*

In preparation for the proofs of Claims 2.7 and 2.8, observe that an element $x \in \mathfrak{Q}^j$ can be written as $x = (1-\zeta_q)^j z$, where $z = \sum_{k=0}^{p-2} z_k\zeta_p^k$ is in $\mathbb{Z}[\zeta_{pq}]$. Hence, $x = \sum_{k=0}^{p-2} x_k\zeta_p^k$, where $x_k \in (1-\zeta_q)^j\mathbb{Z}[\zeta_q]$ for $k = 0, \dots, p-2$. Similarly, $x = \sum_{k=0}^{p-2} y_k\zeta_q^k$, where $y_k \in (1-\zeta_q)^j\mathbb{Z}[\zeta_p]$ for $k = 0, \dots, q-2$.

Proof of Claim 2.7 Define

$$T = \{t \in \mathbb{Z}[\zeta_q] \mid \exists\, \xi' \in \mathcal{M}_1 \text{ with } \lambda_q(\xi') = tp\}$$

and $t_0 \in T$ by

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0\overline{t_0}) = \min\{\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t\bar{t}) \mid t \in T\}.$$

Further, let $\xi \in \mathcal{M}_1$ be such that $\lambda_q(\xi) = t_0p$. During the rest of the proof, we will use the representation

$$\xi = x_0 + x_1\zeta_p + \cdots + x_{p-2}\zeta_p^{p-2},$$

where $x_k = \sum_{\ell=0}^{q-2} a_{k,\ell}\zeta_q^\ell$ and $t_0 = \sum_{\ell=0}^{q-2} h_\ell\zeta_q^\ell$. We have

$$\lambda_q(\xi) = \sum_{m=0}^{p-2} x_m = \sum_{m=0}^{p-2}\sum_{\ell=0}^{q-2} a_{m,\ell}\zeta_q^\ell = \sum_{\ell=0}^{q-2}\sum_{m=0}^{p-2} a_{m,\ell}\zeta_q^\ell. \tag{2.1}$$

On the other hand,

$$\lambda_q(\xi) = t_0p = \left(\sum_{\ell=0}^{q-2} h_\ell\zeta_q^\ell\right)p. \tag{2.2}$$

From (2.1) and (2.2), it follows that

$$\sum_{m=0}^{p-2} a_{m,\ell} = ph_\ell. \tag{2.3}$$

For $y = \zeta_p^a\xi$ with $a \geq 1$, observe that $\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(y\bar{y}) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\xi\bar{\xi})$ is also minimum, that is, $y \in \mathcal{M}$. Since $\mathcal{M}_0 = \varnothing$, we can assume that $\lambda_q(y) \neq 0$. The last statement can be seen as follows:

(i) If $\lambda_q(\xi) \neq 0$ and $\lambda_p(\xi) = 0$, then $\lambda_p(y) = \lambda_p(\zeta_p^a \xi) = \zeta_p^a \lambda_p(\xi) = 0$, whence $\lambda_q(y) \neq 0$.

(ii) If $\lambda_q(\xi) \neq 0$ and $\lambda_p(\xi) \neq 0$, it is no loss of generality to assume that $\lambda_q(y) \neq 0$. Otherwise, $\lambda_p(y) \neq 0$ and $\lambda_q(y) = 0$, and we would reverse the roles of ξ and y.

By Lemma 2.3,

$$\lambda_q(y) = \lambda_q(\zeta_p^a \xi) = \lambda_q(\xi) - p x_{p-1-a} = p(t_0 - x_{p-1-a}) \neq 0.$$

From the fact that $y \in \mathcal{M}$ and the definition of t_0, we have

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}((x_m - t_0)(\overline{x_m - t_0})) \geq \mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0 \overline{t_0}) \tag{2.4}$$

for $m = 0, \dots, p-2$. The left-hand-side of (2.4) is equal to

$$q \sum_{\ell=0}^{q-2} (a_{m,\ell} - h_\ell)^2 - \Big(\sum_{\ell=0}^{q-2} a_{m,\ell} - \sum_{\ell=0}^{q-2} h_\ell \Big)^2,$$

which in turn is equal to

$$q\Big(\sum_{\ell=0}^{q-2} {a_{m,\ell}}^2 - 2 \sum_{\ell=0}^{q-2} a_{m,\ell} h_\ell + \sum_{\ell=0}^{q-2} {h_\ell}^2 \Big) - \Big(\sum_{\ell=0}^{q-2} a_{m,\ell} \Big)^2 + 2 \Big(\sum_{\ell=0}^{q-2} a_{m,\ell} \Big) \Big(\sum_{\ell=0}^{q-2} h_\ell \Big) - \Big(\sum_{\ell=0}^{q-2} h_\ell \Big)^2.$$

The right-hand-side of (2.4) is equal to

$$q\Big(\sum_{\ell=0}^{q-2} {h_\ell}^2 \Big) - \Big(\sum_{\ell=0}^{q-2} h_\ell \Big)^2.$$

From

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_m \overline{x_m}) = q\Big(\sum_{\ell=0}^{q-2} a_{wv}^2 \Big) - \Big(\sum_{\ell=0}^{q-2} a_{wv} \Big)^2,$$

we obtain

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_m \overline{x_m}) \geq 2q\Big(\sum_{\ell=0}^{q-2} a_{m,\ell} h_\ell \Big) - 2\Big(\sum_{\ell=0}^{q-2} a_{m,\ell} \Big) \Big(\sum_{\ell=0}^{q-2} h_\ell \Big).$$

Therefore,

$$\begin{aligned} \sum_{m=0}^{p-2} \mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_m \overline{x_m}) &\geq \sum_{m=0}^{p-2} 2q\Big(\sum_{\ell=0}^{q-2} a_{m,\ell} h_\ell \Big) - 2 \sum_{m=0}^{p-2} \Big(\sum_{\ell=0}^{q-2} a_{m,\ell} \Big) \Big(\sum_{\ell=0}^{q-2} h_\ell \Big) \\ &= 2q\Big(\sum_{\ell=0}^{q-2} \sum_{m=0}^{p-2} a_{m,\ell} h_\ell \Big) - 2\Big(\sum_{\ell=0}^{q-2} \sum_{m=0}^{p-2} a_{m,\ell} \Big) \Big(\sum_{\ell=0}^{q-2} h_\ell \Big). \end{aligned}$$

https://doi.org/10.4153/CMB-2011-038-7 Published online by Cambridge University Press

From (2.3),

$$\begin{aligned}\sum_{m=0}^{p-2} \operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_m\overline{x_m}) &\geq 2q\Big(\sum_{\ell=0}^{q-2}(ph_\ell)h_\ell\Big) - 2\Big(\sum_{\ell=0}^{q-2} ph_\ell\Big)\Big(\sum_{\ell=0}^{q-2} h_\ell\Big)\\ &= 2p\left(q\Big(\sum_{\ell=0}^{q-2} h_\ell^2\Big) - \Big(\sum_{\ell=0}^{q-2} h_\ell\Big)^2\right);\end{aligned}$$

that is,

$$\sum_{m=0}^{p-2} \operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_m\overline{x_m}) \geq 2p\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0\overline{t_0}).$$

Observe also that

$$\begin{aligned}\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}\left(\Big(\sum_{m=0}^{p-2} x_m\Big)\overline{\Big(\sum_{m=0}^{p-2} x_m\Big)}\right) &= \operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}\Big(\lambda(\xi)\overline{\lambda(\xi)}\Big)\\ &= \operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}\big((t_0p)(\overline{t_0p})\big) = p^2\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0\overline{t_0}).\end{aligned}$$

Lemma 2.1 and the latter equality yield

$$\begin{aligned}\operatorname{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\xi\bar{\xi}) &= p\Big(\sum_{m=0}^{p-2}\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_m\overline{x_m})\Big) - \operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}\left(\Big(\sum_{m=0}^{p-2} x_m\Big)\overline{\Big(\sum_{m=0}^{p-2} x_m\Big)}\right)\\ &\geq p\big(2p\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0\overline{t_0})\big) - p^2\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0\overline{t_0}) = p^2\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0\overline{t_0}).\end{aligned}$$

For $i \leq \frac{p-1}{2}$, we obtain

$$\operatorname{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(x_0\overline{x_0}) \geq p(p-1)\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0\overline{t_0}) \geq 2pi\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(t_0\overline{t_0}) \geq 4pqij,$$

where the latter inequality follows from Lemma 2.5. ■

Proof of Claim 2.8 Let $\xi' \in \mathcal{M}_0$, and consider the representations

$$\xi' = \sum_{m=0}^{p-2} x_m\zeta_p^m \text{ and } \xi' = \sum_{\ell=0}^{q-2} y_\ell\zeta_q^\ell$$

where $x_m = \sum_{\ell=0}^{q-2} a_{m,\ell}\zeta_q^\ell$ and $y_\ell = \sum_{m=0}^{p-2} a_{m,\ell}\zeta_p^m$. From Lemma 2.2,

$$\begin{aligned}\operatorname{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\xi\bar{\xi}) &= p\Big(\sum_{m=0}^{p-2}\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_k\overline{x_k})\Big) - \operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}\left(\Big(\sum_{m=0}^{p-2} x_m\Big)\overline{\Big(\sum_{m=0}^{p-2} x_m\Big)}\right)\\ &= p\Big(\sum_{m=0}^{p-2}\operatorname{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_m\overline{x_m})\Big)\end{aligned}$$

https://doi.org/10.4153/CMB-2011-038-7 Published online by Cambridge University Press

as $\lambda_q(x) = 0$. Regarding the latter summation, observe that

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_m\overline{x_m}) = q\Big(\sum_{\ell=0}^{q-2} a_{m,\ell}^2\Big) - \Big(\sum_{\ell=0}^{q-2} a_{m,\ell}\Big)^2 = q\Big(\sum_{\ell=0}^{q-2} a_{m,\ell}^2\Big)$$

because

$$\lambda_q(\xi') = \sum_{m=0}^{p-2} x_m = \sum_{m=0}^{p-2}\sum_{\ell=0}^{q-2} a_{m,\ell}\zeta_q^\ell = \sum_{\ell=0}^{q-2}\Big(\sum_{m=0}^{p-2} a_{m,\ell}\Big)\zeta_q^\ell = 0$$

implies that $\sum_{m=0}^{p-2} a_{m,\ell} = 0$. Thus, we obtain the following expression:

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\xi\bar{\xi}) = pq\Big(\sum_{\ell=0}^{q-2}\sum_{m=0}^{p-2} a_{m,\ell}^2\Big).$$

By way of contradiction, suppose that $\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\bar{x}) < 4pqij$. This is equivalent to

$$\sum_{\ell=0}^{q-2}\sum_{m=0}^{p-2} a_{m,\ell}^2 < 4ij. \tag{2.5}$$

Therefore, for the matrix of coefficients $A = (a_{m\ell})$, exactly one of the following two statements is true:

(i) There is a row with fewer than $2j$ nonzero elements.
(ii) There is a column with fewer than $2i$ nonzero elements.

If that were not the case, then each row and each column of $(a_{m\ell}^2)$ would have at least $2i$ and $2j$ strictly positive entries, respectively. We would conclude that the sum of the entries is greater than or equal to $4ij$; that is, $\sum_{\ell=0}^{q-2}\sum_{m=0}^{p-2} a_{m,\ell}^2 \geq 4ij$, which contradicts (2.5).

In what follows, we assume that (i) occurs. If (ii) occurs, the proof is analogous. Let m_0 be an integer with $0 \leq m_0 \leq p-2$, and $x_{m_0} = \sum_{\ell=0}^{q-2} a_{m_0,\ell}\zeta_q^\ell$, where the number ν of nonzero coefficients $a_{m_0,\ell}$ satisfies $\nu \leq 2j-1$. Since $\sum_{\ell=0}^{q-2} a_{m_0,\ell} = 0$, a parity verification shows that $\nu \neq 2j-1$. Hence, $\nu \leq 2e$ for some $e \leq j-1$. Consider the polynomial $f(X) \in \mathbb{Z}[X]$ such that $x_{m_0} = f(\zeta_q)$. We can write $f(X)$ as:

$$f(X) = X^{s_1} + X^{s_2} + \cdots + X^{s_e} - (X^{t_1} + X^{t_2} + \cdots + X^{t_e}),$$

where s_k and $t_k \in \{0,\dots,q-2\}$ for $k = 1,\dots,e$. The exponents s_k and t_k may eventually repeat.

Since $x_{m_0} \in \mathfrak{Q}^j$, applying Lemma 2.4 to $f(X)$, the successive derivatives satisfy $f^{(k)}(1) \equiv 0 \pmod{q}$ for $k = 0,\dots,j-1$. These congruences imply that

$$\sum_{k=1}^{e} s_k^u \equiv \sum_{k=1}^{e} t_k^u \pmod{p}$$

https://doi.org/10.4153/CMB-2011-038-7 Published online by Cambridge University Press

for $u = 0, \dots, j-1$. It follows that the elementary symmetric functions of the s_k and t_k of degree less than j coincide modulo q. Hence,

$$\prod_{k=1}^{e}(X - s_k) \equiv \prod_{k=1}^{e}(X - t_k) \pmod{q}.$$

These polynomials have the same roots modulo q, so after reordering, we have $s_k \equiv t_k \pmod{q}$. Recalling that $s_k, t_k \in \{0, \dots, q-2\}$, we conclude that $s_k = t_k$ and, consequently, $f(X) \equiv 0$. This is impossible since $x_{m_0} \neq 0$. Therefore, $\mathrm{Tr}_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\xi\bar{\xi}) \geq 4pqij$ holds true in this case. ■

3 Asymptotic Center Density of the Lattices $\sigma_L(\Im_{ij})$

We start out by obtaining a lower bound for the center density of $\sigma_L(\Im_{ij})$. This is easy now that we know that the packing radius ρ of $\sigma_L(\Im_{ij})$ is lower bounded by $\sqrt{pqij/2}$; see Theorem 2.6. Together with elementary results concerning cyclotomic fields in [4], the formula in (1.2) yields

$$(3.1)\quad \delta(\sigma_L(\Im_{ij})) \geq \frac{2^{(p-1)(q-1)/2} \cdot \left(\frac{pqij}{2}\right)^{(p-1)(q-1)/2}}{\frac{(pq)^{(p-1)(q-1)/2}}{p^{(q-1)/2}q^{(p-1)/2}} \cdot p^{(q-1)i}q^{(p-1)j}} = (ij)^{\frac{(p-1)(q-1)}{2}} p^{\frac{(q-1)(1-2i)}{2}} q^{\frac{(p-1)(1-2j)}{2}}.$$

For fixed p and q, the latter expression is maximized when $i = [(p-1)/(2\ln(p))]$ and $j = [(q-1)/(2\ln(q))]$, where $[\,\cdot\,]$ represents the nearest integer function. Knowing the optimal values of i and j, now we can determine Δ_n, the density of $\sigma_L(\Im_{ij})$, for large n.

Theorem 3.1 *If i and j are chosen as above, we have*

$$\tfrac{1}{n}\log_2 \Delta_n \gtrsim -\tfrac{1}{2}\log_2 \log_2, n$$

where $n = (p-1)(q-1)$ is sufficiently large.

Proof The proof is carried out assuming that both p and q approach infinity independently. We remark that, in a similar manner, one can prove the theorem's statement in the case where p (respectively, q) is kept constant while q (respectively, p) approaches infinity.

Let $\delta_n = \delta(\sigma_L(\Im_{ij}))$. From $\Delta_n = V_n\delta_n$, it follows that $\log_2 \Delta_n = \log_2 V_n + \log_2 \delta_n$ where $\log_2 V_n = -\frac{n}{2}\log_2 \frac{n}{2\pi e} - \frac{1}{2}\log_2(n\pi) - \epsilon$ with $0 < \epsilon < \frac{\log_2 e}{6n}$; see [1, p. 9]. Thus

$$\frac{1}{n}\log_2 V_n = -\frac{1}{2}\log_2 \frac{n}{2\pi e} - \frac{1}{2n}\log_2(n\pi) - \frac{\epsilon}{n}.$$

Since $n = (p-1)(q-1)$, we have from (3.1) that

$$\frac{1}{n}\log_2 \delta_n \geq$$
$$\frac{1}{n}\Big(\frac{(p-1)(q-1)}{2}\log_2(ij) + \frac{(q-1)(1-2i)}{2}\log_2 p + \frac{(p-1)(1-2j)}{2}\log_2 q\Big).$$

Therefore,

$$\frac{1}{n}\log_2 \Delta_n \geq$$
$$\frac{1}{2}\log_2\Big(\frac{ij}{n}\Big) + \frac{1-2i}{2(p-1)}\log_2 p + \frac{1-2j}{2(q-1)}\log_2 q - \frac{1}{2n}\log_2(n\pi) - \frac{\epsilon}{n} + \frac{1}{2}\log_2(2\pi e).$$

By substituting the optimal values of i and j in the latter expression, one can show that for sufficiently large p and q,

$$\tfrac{1}{n}\log_2 \Delta_n \geq -\tfrac{1}{2}\log_2\log_2 n + \kappa,$$

where κ is a positive constant. ∎

References

[1] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups.* Third edition, Grundlehren der Mathematischen Wissenschaften, 290, Springer-Verlag, New York, 1999.

[2] J. C. Interlando, A. L. Flores, and T. P. da Nóbrega Neto, *A family of asymptotically good lattices having a lattice in each dimension*. Int. J. Number Theory **4**(2008), no. 1, 147–154. doi:10.1142/S1793042108001262

[3] R. A. Mollin, *Algebraic number theory*. CRC Press Series on Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, FL, 1999.

[4] L. C. Washington, *Introduction to cyclotomic fields.* Second edition, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997.

Departamento de Matemática, Universidade Federal de Alagoas, Arapiraca, AL, Brazil
e-mail: andreflores_br@yahoo.com.br

Department of Mathematics and Statistics, San Diego State University, San Diego, CA, U.S.A.
e-mail: carmelo.interlando@sdsu.edu

Departamento de Matemática, Universidade Estadual Paulista, São José do Rio Preto, SP, Brazil
e-mail: trajano@ibilce.unesp.br