ON AVERAGE COHERENCE OF CYCLOTOMIC LATTICES

LENNY FUKSHANSKY AND DAVID KOGAN

Abstract. We introduce maximal and average coherence on lattices by analogy with these notions on frames in Euclidean spaces. Lattices with low coherence can be of interest in signal processing, whereas lattices with high orthogonality defect are of interest in sphere packing problems. As such, coherence and orthogonality defect are different measures of the extent to which a lattice fails to be orthogonal, and maximizing their quotient (normalized for the number of minimal vectors with respect to dimension) gives lattices with particularly good optimization properties. While orthogonality defect is a fairly classical and well-studied notion on various families of lattices, coherence is not. We investigate coherence properties of a nice family of algebraic lattices coming from rings of integers in cyclotomic number fields, proving a simple formula for their average coherence. We look at some examples of such lattices and compare their coherence properties to those of the standard root lattices.

1. Introduction

Let $L \subset \mathbb{R}^d$ be a lattice of full rank $d \geq 1$ in the Euclidean space $\mathbb{R}^d$, where we will always write $\| \ \|$ for the corresponding Euclidean norm. Define the (squared) *minimum* of L to be

$$|L| := \min\left\{\|\boldsymbol{x}\|^2 : \boldsymbol{x} \in L \setminus \{\mathbf{0}\}\right\},$$

and the set of *minimal vectors* of L to be

$$S(L) := \left\{\boldsymbol{x} \in L : \|\boldsymbol{x}\|^2 = |L|\right\}.$$

The lattice L is called *well-rounded* (abbreviated WR) if $\operatorname{span}_{\mathbb{R}} S(L) = \mathbb{R}^d$. There is a stronger condition for L to be *generated by minimal vectors* if $\operatorname{span}_{\mathbb{Z}} S(L) = L$ (see [16]), and an even stronger condition for L to have a *basis of minimal vectors*, i.e. for $S(L)$ to contain a basis for L (see [14]). We can associate a sphere packing to the lattice L by placing maximal non-overlapping spheres of equal radius at the lattice points, then the radius of these spheres, called the *packing radius* of L will be $\sqrt{|L|}/2$ and the density of this lattice packing will be

$$\delta(L) := \frac{v_d |L|^{\frac{d}{2}}}{2^d \det(L)},$$

where v_d is the volume of a unit ball in $\mathbb{R}^d$ and $\det(L)$ is the determinant of L, i.e., $\det(L) := |\det(B)|$ for any choice of a $d \times d$ matrix B, called *basis matrix* for L, such that $L = B\mathbb{Z}^d$. The determinant of L is precisely the volume of any fundamental

2010 *Mathematics Subject Classification.* Primary: 11H06, 11H31, 11R18; Secondary: 42C15.

Key words and phrases. cyclotomic lattices, average coherence, orthogonality defect, coherence.

Fukshansky was partially supported by the Simons Foundation grant #519058.

domain of L, such as the parallelepiped spanned by the column vectors of B. Given a basis matrix $B = \begin{pmatrix} \boldsymbol{b}_1 & \dots & \boldsymbol{b}_d \end{pmatrix}$ for L, we define the *orthogonality defect* of B as

$$\nu(B) := \frac{\prod_{j=1}^{d} \|\boldsymbol{b}_j\|}{\det(L)},$$

i.e. the ratio of the volume of a rectangular box with sides $\|\boldsymbol{b}_1\|, \dots, \|\boldsymbol{b}_d\|$ to the volume of the parallelepiped spanned by the column vectors of B. Naturally, the Hadamard inequality $\nu(B) \geq 1$ holds with equality if and only if B is an orthogonal basis. If $B \subseteq S(L)$, then

$$\nu(B) = \frac{|L|^{\frac{d}{2}}}{\det(L)} = \frac{2^d}{v_d}\delta(L) \tag{1}$$

is an invariant of the lattice L, which we will call the orthogonality defect of L and denote by $\nu(L)$. Hence for a lattice with a basis of minimal vectors the packing density is proportionate to the orthogonality defect, i.e. to maximize the packing density one wants a lattice with a "least orthogonal" minimal basis. Orthogonality defect figures prominently in lattice theory, especially in connection with algorithmic lattice problems (see [15]). See also [6] and [13] for detailed authoritative expositions of the theory of lattices and its fundamental connections to optimization problems, such as sphere packing and others.

Another measure of orthogonality for a collection of vectors is given by coherence and comes from signal processing. Given a finite set of vectors $S \subset \mathbb{R}^d$, we define its *maximal coherence* as

$$\mathcal{C}(S) := \max\left\{ \frac{|\langle \boldsymbol{x}, \boldsymbol{y}\rangle|}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} : \boldsymbol{x} \neq \boldsymbol{y} \in S \right\},$$

where $\langle\ ,\ \rangle$ stands for the usual Euclidean inner product, and its *average coherence* as

$$\mathcal{A}(S) := \frac{1}{|S|-1} \max\left\{ \sum_{\boldsymbol{y} \in S \setminus \{\boldsymbol{x}\}} \frac{|\langle \boldsymbol{x}, \boldsymbol{y}\rangle|}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} : \boldsymbol{x} \in S \right\}.$$

It is easy to see that $\mathcal{A}(S) = 0$ if and only if S is an orthogonal collection of vectors, which in particular implies $|S| \leq d$. An important problem in signal processing is the construction of sufficiently large sets S ($|S| > d$) with sufficiently low coherence. Special attention among such low-coherence sets is usually given to frames, which are overdetermined spanning sets with certain additional properties, especially to the uniform tight frames: a finite set $S \subset \mathbb{R}^d$ is called a *uniform tight frame* if all vectors in S have the same norm and there exists a real constant $\gamma > 0$ such that

$$\|\boldsymbol{v}\| = \gamma \sum_{\boldsymbol{x} \in S} \langle \boldsymbol{v}, \boldsymbol{x}\rangle^2,$$

for every $\boldsymbol{v} \in \mathbb{R}^d$ (see [18] for a comprehensive exposition of tight frame theory).

We can extend the notion of coherence to lattices as follows. Notice that minimal vectors of a lattice L come in $\pm$ pairs: $\boldsymbol{x} \in S(L)$ if and only if $-\boldsymbol{x} \in S(L)$. Then define $S'(L)$ to be a subset of $S(L)$ constructed by selecting one vector out of each such pair, and define maximal and average coherence of L to be

$$\mathcal{C}(L) := \mathcal{C}(S'(L)),\ \mathcal{A}(L) := \mathcal{A}(S'(L)),$$

respectively. These values do not depend on the specific choice of vectors in $S'(L)$ out of each $\pm$ pair. If L has a basis of minimal vectors, then $\mathcal{A}(L)$ becomes a certain

alternative measure of its "non-orthogonality": $\mathcal{A}(L) \geq 0$ with equality if and only if $S'(L)$ is an orthogonal basis for L. Maximal coherence on lattices has previously been introduced in [8] and studied on nearly orthogonal lattices in [7], but average coherence has not previously been extended to lattices, as far as we know. Average coherence for frames was introduced in [2]. Our definition of average coherence slightly differs from the one introduced in [2]: in their definition, the absolute value is outside of the sum. We choose to move absolute value inside to ensure that the average coherence does not depend on the choice of the vectors in $S'(L)$: it does not matter which vector from each $\pm$ pair in $S(L)$ is selected.

While there can be a relation between average coherence and orthogonality defect in some special cases, there does not appear to be a general dependence. On the other hand, it is interesting to understand which lattices with relatively large sets of minimal vectors simultaneously have small average coherence and large orthogonality defect. To this end, given a lattice $L \subset \mathbb{R}^d$ with a basis of minimal vectors, we define its *orthogonality product measure* (referred to from here on simply as *product measure*) to be

$$\Pi(L) := \frac{|S'(L)|\nu(L)}{d\mathcal{A}(L)}. \tag{2}$$

Then a lattice L with large $|S'(L)|$ (as compared to the dimension d), small $\mathcal{A}(L)$ and large $\nu(L)$ will have large $\Pi(L)$. We can then ask which lattices have large $\Pi(L)$. In this note, we investigate average coherence and product measure on the family of cyclotomic lattices, a special family of ideal lattices. We start out by introducing the ideal lattices.

Let K be a number field of degree d over $\mathbb{Q}$, and let $\mathcal{O}_K$ be its ring of integers. Let

$$\sigma_1, \ldots, \sigma_{r_1}, \tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2} : K \hookrightarrow \mathbb{C}$$

be its embeddings into the field of complex numbers, where $r_1 + 2r_2 = d$ and $\sigma_1, \ldots, \sigma_{r_1}$ are real embeddings, whereas $\tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2}$ are pairs of complex conjugate embeddings. The *Minkowski embedding* of K into $\mathbb{R}^d$ is then defined as

$$\Sigma_K := (\sigma_1, \ldots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \ldots, \Re(\tau_{r_2}), \Im(\tau_{r_2})) : K \hookrightarrow \mathbb{R}^d,$$

and the image of $\mathcal{O}_K$ under this embedding, $\Lambda_K := \Sigma_K(\mathcal{O}_K)$ is a Euclidean lattice of full rank in $\mathbb{R}^d$. Furthermore,

$$\det(\Lambda_K) = 2^{-r_2}|\Delta_K|^{1/2}, \tag{3}$$

where Δ_K stands for the discriminant of K. Such lattices are called *number field lattices*; they form a special case of the more general *ideal lattices* (of trace type), which are given by the same construction on an arbitrary fractional ideal in K. This construction of ideal lattices is classical: it can be found, for instance, in [5] (pp. 94–99) or [17] (Chapter 5.3), as well as in [4].

We focus specifically on cyclotomic fields. Let $\zeta_n = e^{\frac{2\pi i}{n}}$ for $n > 2$ be the n-th primitive root of unity and $K = \mathbb{Q}(\zeta_n)$ be the corresponding n-th cyclotomic number field, then $d = [K : \mathbb{Q}] = \varphi(n)$ and the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. Then the group of n-th roots of unity

$$\mathcal{R}_n := \left\{\zeta_n^k : 1 \leq k \leq n\right\}$$

is precisely the set of all roots of unity contained in $\mathcal{O}_K$. We refer to the lattice Λ_K as the *n-th cyclotomic lattice*. We give a more detailed description of cyclotomic

lattices and their properties in Section 2, in particular explaining that they have bases of minimal vectors and

$$|S'(\Lambda_K)| = \begin{cases} n & \text{if } n \text{ is odd,} \\ \frac{1}{2}n & \text{if } n \text{ is even.} \end{cases}$$

Further, we demonstrate the well-known fact that in the cyclotomic case the orthogonality defect

$$\nu(\Lambda_K) = \left(\frac{\varphi(n)}{\prod_{p|n} p^{e_p - \frac{1}{p-1}}} \right)^{\frac{\varphi(n)}{2}}, \tag{4}$$

where $n = \prod_{p|n} p^{e_p}$ and the product in the denominator is over all primes dividing n. We also define the average coherence $\mathcal{A}(\alpha)$ for any $\alpha \in S'(\Lambda_K)$, as well as $\mathcal{A}(\Lambda_K)$, the average coherence of the lattice Λ_K, in (8) and (9), respectively. Finally, cyclotomic lattices are *strongly eutactic*, meaning that their sets of minimal vectors form uniform tight frames in their respective Euclidean spaces.

Cyclotomic lattices have been extensively studied in the context of lattice theory (see Section 8.7 of [6] and references therein), and their structure is generally understood. One goal of this note is to attract some attention to the notions of average and maximal coherence on lattices. We use cyclotomic lattices as a simple and attractive case study. As it turns out, there is a particularly simple and elegant arithmetic formula for the average coherence of this family of lattices.

Theorem 1. *Let $n > 2$ be an integer, and let Λ_K be the corresponding cyclotomic lattice for $K = \mathbb{Q}(\zeta_n)$. Then*

$$\mathcal{C}(\Lambda_K) = \begin{cases} 0 & \text{if } n \text{ is a power of } 2, \\ \frac{1}{p-1} & \text{if } p \text{ is the smallest odd prime dividing } n. \end{cases}$$

Additionally, for any $\alpha \in S'(\Lambda_K)$,

$$\mathcal{A}(\alpha) = \mathcal{A}(\Lambda_K) = \begin{cases} \frac{2^{\omega(n)}-1}{n-1} & \text{if } n \text{ is odd,} \\ \frac{2^{\omega(n)}-2}{n-2} & \text{if } n \text{ is even,} \end{cases} \tag{5}$$

where ω is the number of prime divisors function. Combining (5) *with* (4)*, we readily obtain an explicit formula for $\Pi(\Lambda_{\mathbb{Q}(\zeta_n)})$, which depends only on n:*

$$\Pi(\Lambda_{\mathbb{Q}(\zeta_n)}) = \begin{cases} \frac{n(n-2)\,\varphi(n)^{\frac{\varphi(n)}{2}-1}}{2(2^{\omega(n)}-2)\left(\prod_{p|n} p^{e_p - \frac{1}{p-1}}\right)^{\frac{\varphi(n)}{2}}} & \text{if } 2 \mid n, \\ \frac{n(n-1)\,\varphi(n)^{\frac{\varphi(n)}{2}-1}}{(2^{\omega(n)}-1)\left(\prod_{p|n} p^{e_p - \frac{1}{p-1}}\right)^{\frac{\varphi(n)}{2}}} & \text{if } 2 \nmid n. \end{cases}$$

We prove Theorem 1 in Section 3. In Section 4, we demonstrate several examples, aiming to determine values of n for which $\Pi(\Lambda_{\mathbb{Q}(\zeta_n)})$ is the largest in a fixed dimension $d = \varphi(n)$. For comparison purposes, we also compute the coherence and product measure values for the standard root lattices. Of course, it is easy to see that the product measure values for cyclotomic lattices are not nearly as large as for the root lattices in the same dimensions. On the other hand, root lattices are truly exceptional (in particular, they are local maxima of the packing density function in their dimensions; see, for instance, Chapter 4 of [13] for details), and there are

very few of them. Cyclotomic lattices present a larger family of lattices with interesting properties (in even dimensions given by the values of the Euler φ-function), including numerous examples of lattices with low maximal coherence. In fact, as we discuss at the end of Section 4, the maximal and average coherence of cyclotomic lattices, in contrast with the root lattices, are about the same on the average as $n \to \infty$, which can also make them potentially interesting from the standpoint of sparse signal processing: it guarantees that signal frequencies represented by the minimal vectors are well spread out, a useful feature for signal recovery (see [1] and [2]). For future research, it would be interesting to investigate average coherence of other families of lattices coming from algebraic constructions, including some more general ideal lattices, as well as to study properties and general behavior of average coherence as a function on lattices. We are now ready to proceed.

2. Cyclotomic lattices

In this section we give an alternative and for our purposes more convenient description of cyclotomic lattices. Let $K = \mathbb{Q}(\zeta_n)$ for $n > 2$, then K only has the complex embeddings

$$\tau_1, \bar{\tau}_1, \ldots, \tau_{d/2}, \bar{\tau}_{d/2} : K \hookrightarrow \mathbb{C},$$

so $r_1 = 0$ and $d = \varphi(n) = 2r_2$. For each $\alpha \in \mathcal{O}_K$, the trace of α is given by

$$\mathrm{Tr}_K(\alpha) := \sum_{k=1}^{d/2} (\tau_k(\alpha) + \bar{\tau}_k(\alpha)).$$

Using the notation of Section 8.7 of [6] (see also [3]), we can think of the cyclotomic lattice Λ_K as the free $\mathbb{Z}$-module $\mathcal{O}_K$ equipped with the bilinear form

$$\langle \alpha, \beta \rangle := \frac{1}{2} \mathrm{Tr}_K(\alpha\bar{\beta})$$

for any $\alpha, \beta \in \mathcal{O}_K$. It is easy to verify that $\langle \alpha, \beta \rangle$ is equal to the usual dot product of the vectors $\Sigma_K(\alpha)$ and $\Sigma_K(\beta)$ in $\mathbb{R}^d$. Then for any $\alpha = a + bi \in \mathcal{O}_K = \mathbb{Z}[\zeta_n]$ we have $\alpha\bar{\alpha} = a^2 + b^2$, and hence

$$\langle \alpha, \alpha \rangle = \sum_{k=1}^{d/2} \tau_k(a^2 + b^2) = \sum_{k=1}^{d/2} \left(\Re(\tau_k(\alpha))^2 + \Im(\tau_k(\alpha))^2 \right).$$

By the results of [9], Λ_K is WR with $|\Lambda_K| = \frac{\varphi(n)}{2}$ and $\alpha \in S(\Lambda_K)$ if and only if it is a root of unity, i.e.

$$S(\Lambda_K) = \{\pm\alpha : \alpha \in \mathcal{R}_n\} = \begin{cases} \mathcal{R}_n & \text{if } 2 \mid n \\ \mathcal{R}_{2n} & \text{if } 2 \nmid n, \end{cases}$$

since

$$-1 = e^{\pi i} = \begin{cases} e^{\frac{2(n/2)\pi i}{n}} & \text{if } 2 \mid n \\ e^{\frac{2n\pi i}{2n}} & \text{if } 2 \nmid n. \end{cases}$$

Let $\alpha, \beta \in S(\Lambda_K)$, then

$$\langle \alpha, \beta \rangle = \frac{1}{2} \mathrm{Tr}_K(\alpha\bar{\beta}),$$

where $\alpha\bar{\beta}$ is also a root of unity. Suppose that $\alpha\bar{\beta}$ is an m-th primitive root of unity of for some $m \mid n$; then it is a root of m-th cyclotomic polynomial $\Phi_m(x)$. Notice

that the trace of an algebraic number is the negative of the second coefficient of its minimal polynomial. It is a well-known fact that

$$\Phi_m(x) = x^{\varphi(m)} - \mu(m)x^{\varphi(m)-1} + \dots,$$

where μ is the Möbius function. Hence $\mathrm{Tr}_{\mathbb{Q}(\alpha\bar{\beta})}(\alpha\bar{\beta}) = \mu(m)$, and therefore

$$\langle \alpha, \beta \rangle = \frac{1}{2}\,\mathrm{Tr}_K(\alpha\bar{\beta}) = \frac{[K:\mathbb{Q}(\alpha\bar{\beta})]}{2}\,\mathrm{Tr}_{\mathbb{Q}(\alpha\bar{\beta})}(\alpha\bar{\beta}) = \frac{\varphi(n)}{2\,\varphi(m)}\mu(m). \tag{6}$$

Further, if $\alpha = \zeta_n^{k_1}$ and $\beta = \zeta_n^{k_2}$, then $m = \frac{n}{\gcd(k_1-k_2,n)}$, and so the cosine of the angle between these two vectors is

$$c(\alpha,\beta) := \frac{\langle \alpha, \beta \rangle}{\sqrt{\langle \alpha, \alpha \rangle \langle \beta, \beta \rangle}} = \frac{\varphi(n)}{\varphi(n)\,\varphi(m)}\mu(m) = \frac{\mu\left(\frac{n}{\gcd(k_1-k_2,n)}\right)}{\varphi\left(\frac{n}{\gcd(k_1-k_2,n)}\right)}. \tag{7}$$

Define $s := |S(\Lambda_K)|$, so $s = n$ if n is even and $s = 2n$ if n is odd. Then we can write

$$S(\Lambda_K) = \left\{\zeta_n^k, \zeta_n^{k+\frac{s}{2}} : 1 \le k \le s/2\right\},$$

where $\zeta_n^{k+\frac{s}{2}} = -\zeta_n^k$ and $c\left(\zeta_n^k, \zeta_n^{k+\frac{s}{2}}\right) = -1$, as expected. Hence let

$$S'(\Lambda_K) = \left\{\zeta_n^k : 1 \le k \le s/2\right\},$$

so the coherence of the lattice Λ_K is given by

$$\mathcal{C}(\Lambda_K) = \max\left\{|c(\alpha,\beta)| : \alpha, \beta \in S'(\Lambda_K), \alpha \ne \beta\right\}.$$

Then for any two $\alpha = \zeta^{k_1}, \beta = \zeta^{k_2} \in S'(\Lambda_K)$, $|k_1 - k_2| \le s/2 - 1$, so $c(\alpha,\beta) \ne \pm 1$. Additionally, for each $\alpha \in S'(\Lambda_K)$ define its average coherence to be

$$\mathcal{A}(\alpha) = \frac{1}{|S'(\Lambda_K)| - 1} \sum_{\beta \in S'(\Lambda_K)\setminus\{\alpha\}} |c(\alpha,\beta)|. \tag{8}$$

The average coherence of Λ_K is then given by

$$\mathcal{A}(\Lambda_K) = \max\{\mathcal{A}(\alpha) : \alpha \in S'(\Lambda_K)\}. \tag{9}$$

Now, the discriminant of the cyclotomic field $K = \mathbb{Q}(\zeta_n)$ is given by

$$\Delta_K = (-1)^{\frac{\varphi(n)}{2}} n^{\varphi(n)} \prod_{p|n} p^{-\frac{\varphi(n)}{p-1}},$$

where the product is over all primes p dividing n (see, for instance, Section 8.7.3 of [6]). Combining this observation with (1), (3), and the fact that $|\Lambda_K| = \varphi(n)/2$, we obtain (4).

We also briefly comment on the structure of cyclotomic lattices, which is well known (see, for instance, Section 8.7 of [6]). Two lattices $L_1, L_2 \subset \mathbb{R}^k$ are called *similar*, denoted $L_1 \sim L_2$, if there exists a nonzero real constant γ and a $k \times k$ real orthogonal matrix U such that $L_2 = \gamma U L_1$; if $\gamma = \pm 1$, L_1 and L_2 are *isometric*, denoted $L_1 \cong L_2$. For any lattice $L \subset \mathbb{R}^d$ of rank d, its *dual* is the lattice

$$L^* := \left\{\boldsymbol{x} \in \mathbb{R}^d : \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}\ \forall\ \boldsymbol{y} \in L\right\}.$$

The root lattice A_n is defined as

$$A_n = \left\{\boldsymbol{x} \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0\right\}, \tag{10}$$

which is a lattice of rank n, as is its dual A_n^*. With this notation, the following is true:

(1) If $n = p$ is an odd prime, then $\Lambda_K \sim A_{p-1}^*$,
(2) If $n = p^k$ is an odd prime power, then $\Lambda_K \sim \bigoplus_{j=1}^{p^{k-1}} A_{p-1}^*$,
(3) If $n = p^k q^l$ is a product of two distinct odd prime powers, then

$$\Lambda_K \sim \left(\bigoplus_{j=1}^{p^{k-1}} A_{p-1}^*\right) \otimes \left(\bigoplus_{j=1}^{q^{l-1}} A_{q-1}^*\right).$$

Lattices A_n^* are known to be strongly eutactic. Further, tensor products of strongly eutactic lattices as well as direct sums of isometric strongly eutactic lattices are strongly eutactic (see Chapter 3 of [13]). This observation, along with the above properties, implies that cyclotomic lattices are in general strongly eutactic.

3. Coherence of cyclotomic lattices

In this section we prove Theorem 1 in a series of several lemmas. Throughout this section, $K = \mathbb{Q}(\zeta_n)$ for the specified choices of n and Λ_K is the corresponding cyclotomic lattice.

Lemma 2. *Suppose $n = 2^m$ for some $m \geq 1$, then Λ_K is an orthogonal lattice, which is similar to $\mathbb{Z}^{2^{m-1}}$. In particular, $\mathcal{C}(\Lambda_K) = 0$.*

Proof. First notice that $\varphi(2^m) = 2^{m-1}$, thus Λ_K is a lattice of rank 2^{m-1} with 2^m minimal vectors. Let $\alpha, \beta \in S'(\Lambda_K)$ and suppose $\alpha\bar{\beta}$ is a k-th primitive root of unity for some $k \mid 2^m$. Then $k = 2^l$ for some $0 \leq l \leq m$, and by (6),

$$\langle \alpha, \beta \rangle = \frac{1}{2}\frac{\varphi(2^m)}{\varphi(2^l)}\mu(2^l) = 0,$$

unless $l = 0$ or 1. If $l = 0, 1$, then $\alpha\bar{\beta}$ is either a first or second root of unity, i.e. $\alpha\bar{\beta} = \pm 1$, which implies that $\alpha = \pm\beta$. Therefore $c(\alpha, \beta) = 0$ for any pair of distinct minimal vectors in $S'(\Lambda_K)$, and so $S(\Lambda_K)$ consists of $\varphi(n) = n/2 = 2^{m-1}$ plus-minus pairs of orthogonal basis vectors of equal norm. Hence $\Lambda_K \sim \mathbb{Z}^{2^{m-1}}$. □

Lemma 3. *Assume that n is not a power of 2, and let p be the smallest odd prime dividing n. Then*

$$\mathcal{C}(\Lambda_K) = \frac{1}{p-1}.$$

Proof. Let $\alpha = \zeta_n^{k_1} \in S'(\Lambda_K)$, then

$$\{\beta \in S'(\Lambda_K) : \beta \neq \alpha\} = \left\{\zeta_n^{k_2} : 1 \leq k_2 \leq s/2, k_2 \neq k_1\right\},$$

and so $k_1 - k_2$ takes on all nonzero integer values between $k_1 - 1$ and $k_1 - s/2$. In particular, $k_1 - k_2 < s/2$, which means that $c(\alpha, \beta) \neq \pm 1$. Since p is the smallest odd prime dividing n, $2 < p \leq s/2$. Then let $k_1 = p + 1$ and $k_2 = 1$, and for the corresponding $\alpha = \zeta_n^{k_1}$, $\beta = \zeta_n^{k_2}$, (7) gives

$$|c(\alpha, \beta)| = \frac{1}{p-1}.$$

On the other hand, $\frac{n}{\gcd(k_1-k_2,n)} \neq 1$ is a divisor of n, which cannot be equal to 2: $\frac{n}{\gcd(k_1-k_2,n)} = 2$ implies n is even and $|k_1 - k_2| = n/2 = s/2$, however we know that

$|k_1 - k_2| \leq s/2 - 1$. Hence it cannot be smaller than p, and so (7) guarantees that $\mathcal{C}(\Lambda_K) \leq \frac{1}{p-1}$. Thus we have the result. □

Lemma 4. *Assume n is odd and squarefree, then*

$$\mathcal{A}(\Lambda_K) = \frac{\tau(n) - 1}{n - 1},$$

where $\tau(n)$ is the number of divisors of n.

Proof. Since n is odd, we have $s/2 = n$. Let $\alpha = \zeta_n^k \in S'(\Lambda_K)$ for some $1 \leq k \leq s/2$, then by (7),

$$\begin{aligned} \mathcal{A}(\alpha) &= \frac{1}{s/2-1} \sum_{j=1,\ j\neq k}^{s/2} \frac{1}{\varphi\left(\frac{n}{\gcd(j-k,n)}\right)} = \frac{1}{n-1} \sum_{m=1-k,\ m\neq 0}^{n-k} \frac{1}{\varphi\left(\frac{n}{\gcd(m,n)}\right)} \\ &= \frac{1}{n-1} \sum_{d|n,\ d\neq n} \frac{a_d}{\varphi(n/d)}, \end{aligned}$$

where a_d = the number of times $\gcd(m,n) = d$ for nonzero $1 - k \leq m \leq n - k$. Notice that the set $\{1-k, \dots, n-k\}$ is a complete residue system modulo n, as is the set $\{0, \dots, n\}$ and hence the number of times $\gcd(m,n) = d$ for nonzero $1 - k \leq m \leq n - k$ equals the number of times $\gcd(m,n) = d$ for $1 \leq m \leq n$. Therefore we can write

$$\mathcal{A}(\alpha) = \frac{1}{n-1} \sum_{d|n, d\neq n} \frac{a_d}{\varphi(n/d)},$$

where

$$a_d = |\{1 \leq m \leq n : \gcd(m,n) = d\}| = \varphi(n/d),$$

which is independent of k and thus of the choice of α. Hence we have

$$\mathcal{A}(\Lambda_K) = \frac{1}{n-1} \sum_{d|n,\ d\neq n} \frac{\varphi(n/d)}{\varphi(n/d)} = \frac{1}{n-1} \sum_{d|n,\ d\neq n} 1 = \frac{\tau(n) - 1}{n-1}.$$

□

Lemma 5. *Assume n is even and squarefree, then*

$$\mathcal{A}(\Lambda_K) = \frac{\tau(n) - 2}{n - 2},$$

where $\tau(n)$ is the number of divisors of n.

Proof. Since n is even, we have $s/2 = n/2$. Let $\alpha = \zeta_n^k \in S'(\Lambda_K)$ for some $1 \leq k \leq s/2$, then by (7),

$$\begin{aligned} \mathcal{A}(\alpha) &= \frac{1}{s/2-1} \sum_{j=1,\ j\neq k}^{s/2} \frac{1}{\varphi\left(\frac{n}{\gcd(j-k,n)}\right)} = \frac{2}{n-2} \sum_{m=1-k,\ m\neq 0}^{\frac{n}{2}-k} \frac{1}{\varphi\left(\frac{n}{\gcd(m,n)}\right)} \\ &= \frac{2}{n-2} \sum_{d|n,\ d<\frac{n}{2}} \frac{b_d}{\varphi(n/d)}, \end{aligned}$$

where b_d = the number of times $\gcd(m,n) = d$ for nonzero $1 - k \leq m \leq \frac{n}{2} - k$. Notice that, if $d \neq 1, 2$, then for any such m there is a unique $m' = m + n/2$ so that

$\gcd(m',n) = \gcd(m,n) = d$ and $\frac{n}{2} - k \leq m' \leq n-k$. Therefore for each divisor $d \neq 1,2$ of n with $d < n/2$, $b_d = \frac{\varphi(n/d)}{2}$. On the other hand,

$$\gcd(m,n) = 1 \Leftrightarrow \gcd(m',n) = 2,\ \gcd(m,n) = 2 \Leftrightarrow \gcd(m',n) = 1,$$

so $b_1 + b_2 = \varphi(n) = \varphi(n/2)$. Further, observe that $d \mid n$ with $d < n/2$ if and only if $d \mid \frac{n}{2}$ and $d \neq n/2$. Hence

$$\begin{aligned}\mathcal{A}(\Lambda_K) &= \frac{2}{n-2}\left(\frac{\varphi(n/2)}{\varphi(n/2)} + \sum_{d|n,\ d<\frac{n}{2},\ d\neq 1,2} \frac{\varphi(n/d)}{2\,\varphi(n/d)}\right) \\ &= \frac{2}{n-2}\left(1 + \frac{1}{2}(\tau(n)-4)\right) = \frac{\tau(n)-2}{n-2},\end{aligned}$$

since the number of divisors d of n such that $d < n/2$ is $\tau(n) - 2$: we count all the divisors except for n and $n/2$. □

Corollary 6. *Let $n > 2$ be an integer and let $n' = \prod_{p|n} p$ be its squarefree part. Let Λ_K be the corresponding cyclotomic lattice for $K = \mathbb{Q}(\zeta_n)$. Then for any $\alpha \in S'(\Lambda_K)$,*

$$\mathcal{A}(\alpha) = \mathcal{A}(\Lambda_K) = \begin{cases} \frac{\tau(n')-1}{n-1} & \text{if } n \text{ is odd,} \\ \frac{\tau(n')-2}{n-2} & \text{if } n \text{ is even.} \end{cases}$$

Proof. For each $\alpha = \zeta_n^k \in S'(\Lambda_K)$, we have

$$\mathcal{A}(\alpha) = \frac{1}{|S'(\Lambda_K)|-1} \sum_{\beta \in S'(\Lambda_K)\setminus\{\alpha\}} |c(\alpha,\beta)| = \frac{2}{s-2} \sum_{j=1,\ j\neq k}^{s/2} \frac{\left|\mu\left(\frac{n}{\gcd(j-k,n)}\right)\right|}{\varphi\left(\frac{n}{\gcd(j-k,n)}\right)},$$

where for each $\beta = \zeta_n^j \in S'(\Lambda_K)$,

$$c(\alpha,\beta) = \frac{\mu\left(\frac{n}{\gcd(k-j,n)}\right)}{\varphi\left(\frac{n}{\gcd(k-j,n)}\right)} = 0,$$

unless $\frac{n}{\gcd(k-j,n)}$ is squarefree, i.e. a divisor of n'. Thus

$$\mathcal{A}(\alpha) = \frac{2}{s-2} \sum_{m=1-k,\ m\neq 0}^{\frac{s}{2}-k} \frac{\left|\mu\left(\frac{n}{\gcd(m,n)}\right)\right|}{\varphi\left(\frac{n}{\gcd(m,n)}\right)} = \frac{2}{s-2} \sum_{\frac{n}{d}|n',\ d<\frac{s}{2}} \frac{c_d}{\varphi(n/d)}, \tag{11}$$

where

$$c_d = \left|\left\{1-k \leq m \leq \frac{s}{2} - k : \gcd(m,n) = d\right\}\right|.$$

Notice that every divisor d of n such that n/d divides n' is of the form $d = d'(n/n')$, where $d' \mid n'$. Let $s' = n'$ if n' is even and $2n'$ if n' is odd, then

$$c_d = \left|\left\{1-k \leq m \leq \frac{s'}{2} - k : \gcd(m,n') = d'\right\}\right| = \begin{cases} a_{d'} & \text{if } 2 \nmid n' \\ b_{d'} & \text{if } 2 \mid n', \end{cases}$$

where $a_{d'}$ and $b_{d'}$ are as in Lemmas 4 and 5, respectively. The result then follows by combining (11) with these lemmas. □

Proof of Theorem 1. Notice that for any positive integer n with its squarefree part n', $\tau(n') = 2^{\omega(n)}$. The statement of the theorem now follows by combining Lemmas 2, 3 with Corollary 6. □

4. Coherence and orthogonality defect

Throughout this section, let us write $\mathcal{C}_n$, $\mathcal{A}_n$, ν_n and Π_n for $\mathcal{C}(\Lambda_{\mathbb{Q}(\zeta_n)})$, $\mathcal{A}(\Lambda_{\mathbb{Q}(\zeta_n)})$, $\nu(\Lambda_{\mathbb{Q}(\zeta_n)})$, and $\Pi(\Lambda_{\mathbb{Q}(\zeta_n)})$, respectively. We aim to understand the behavior of these functions as n ranges through natural numbers. The first observation is that for odd n, $\Lambda_{\mathbb{Q}(\zeta_{2n})} = \Lambda_{\mathbb{Q}(\zeta_n)}$, and the formulas from Section 1 yield

$$\mathcal{C}_{2n} = \mathcal{C}_n,\ \mathcal{A}_{2n} = \mathcal{A}_n,\ \nu_{2n} = \nu_n,\ \Pi_{2n} = \Pi_n,$$

as expected.

Let us start by briefly recalling the order of the arithmetic function $\varphi(n)$ (see Chapter 18 of [10] for further details). For all $n > 2$,

$$\frac{n}{e^{\gamma}\log\log n + \frac{3}{\log\log n}} < \varphi(n) < n, \tag{12}$$

where $\gamma = 0.57721\ldots$ is Euler's constant. In fact, $\varphi(n) < \frac{n}{e^{\gamma}\log\log n}$ for infinitely many n, although the average order of $\varphi(n)$ is

$$\frac{1}{n}\sum_{m=1}^{n}\varphi(m) = \frac{3n}{\pi^2} + O(\log n).$$

Recall now that $s/2$, the cardinality of $S'(\Lambda_{\mathbb{Q}(\zeta_n)})$ is n or $n/2$, depending on the parity of n, whereas the rank of $\Lambda_{\mathbb{Q}(\zeta_n)}$ is $\varphi(n)$. Since it is desirable to have the number of minimal vectors as large as possible, compared to the dimension, we may want to consider values of n for which $\varphi(n)$ is close to the lower bound of (12).

A particularly interesting situation from the stand-point of signal processing and of lattice theory arises when $2\,\varphi(n)/s$ and $\mathcal{A}_n$ are small, while ν_n is large: this would mean that $S(\Lambda_{\mathbb{Q}(\zeta_n)})$ is a configuration of many (in comparison to dimension) vectors, which are incoherent and non-orthogonal. Such configurations can be useful, for instance, in recovering signals transmitted with erasures (see [11]). To this end, we observe that the values of n that maximize Π_n for each fixed dimension $\varphi(n)$ are large n with small prime factors and small prime factor powers, and similarly for maximizing ν_n. On the other hand, values of n minimizing $\mathcal{A}_n$ are large n (for a fixed value of $\varphi(n)$) with few prime factors, whereas $\mathcal{C}_n$ is minimized by n with large prime factors. In particular, it appears that large Π_n is more correlated with large ν_n than with small $\mathcal{A}_n$. Indeed, consider the examples in Table 1: the values marked in bold are maximal among all n with that value of $\varphi(n)$ for ν_n and Π_n, and minimal for $\mathcal{C}_n$ and $\mathcal{A}_n$. We have also computed many additional examples, and the same observations seem to hold.

Further, although there is a general positive correlation between $\mathcal{A}_n$ and ν_n (see for instance dimension 24 in Table 1), there are nevertheless sequences of closely related values of n where the correlation is negative. Observe, for instance, dimension 72 in Table 1. Take $n \in \{111, 117, 135, 228, 252\}$. If we arrange these in order of number of minimal vectors of $\Lambda_{\mathbb{Q}(\zeta_n)}$, we have $s \in \{222, 228, 234, 252, 270\}$. These lattices respectively have $\mathcal{A}_n$ values of $0.0\overline{27}, 0.0265..., 0.0259..., 0.024$, and

0.0224.... However, as $\mathcal{A}_n$ decreases, we see an increase in ν_n, from $\nu_{111} = \nu_{222} = 2447.5...$ to $\nu_{135} = \nu_{270} = 1.124... \cdot 10^5$.

This is not a unique occurrence. It appears in many dimensions, most notably in those which are multiples of 24. It is perhaps worth noting that the prime factorization of the number of minimal vectors in such a sequence (e.g. 222, 228, 234, 252, 270) all have the same number of distinct prime factors, and at each step at least one large prime factor is converted into lower prime factors. For instance, $222 = 2 \cdot 3 \cdot 37$ while $228 = 2^2 \cdot 3 \cdot 19$, which converts the 37 to $2 \cdot 19$. This reduction of the largest term in the denominator of (4) drives up ν_n but holds $\omega(n)$ constant so drives down $\mathcal{A}_n$ as n increases.

For comparison purposes, we also record here the values of coherence, average coherence, orthogonality defect and product measure for the standard irreducible root lattices. We start by briefly recalling some standard notation. A lattice is called *irreducible* if it is not a direct sum of nonzero sublattices. A *root* in a lattice is a vector of squared-norm equal to 2, and an irreducible lattice is called a *root lattice* if it is generated by its roots. In this case, the roots are the minimal vectors of the lattice. There are precisely two infinite families of irreducible root lattices, denoted A_n and D_n, as well as the three exceptional examples E_6, E_7 and E_8. We already defined A_n in (10), and now recall that

$$D_n = \left\{ \boldsymbol{x} \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \in 2\mathbb{Z} \right\}, \; E_8 = D_8 \cup \left\{ \frac{1}{2} \left(\sum_{i=1}^{8} \boldsymbol{e}_i \right) + D_8 \right\}, \tag{13}$$

where $\boldsymbol{e}_i$ are the standard basis vectors in the corresponding $\mathbb{Z}^n$. Additionally,

$$E_7 = \{ \boldsymbol{x} \in E_8 : \langle \boldsymbol{x}, \boldsymbol{e}_7 + \boldsymbol{e}_8 \rangle = 0 \}, \; E_6 = \{ \boldsymbol{x} \in E_7 : \langle \boldsymbol{x}, \boldsymbol{e}_6 + \boldsymbol{e}_8 \rangle = 0 \}. \tag{14}$$

We refer the reader to [13] (Chapter 4) or [6] (Chapter 4) for the detailed information on the properties of root lattices. We will mention that, due to the remarkable symmetry properties of root lattices, their minimal vectors are indistinguishable in the following sense. Let L be a root lattice. Then for each vector $\boldsymbol{x} \in S(L)$ there is the same number of vectors $\boldsymbol{y} \in S(L)$ that have nonzero inner product $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ ([13], Proposition 4.10.12). Standard integrality conditions limit the only other possible inner product value to $|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| = 1$. With this in mind, the calculation of the average coherence of root lattices becomes straightforward, using Proposition 4.2.2 and Theorems 4.3.3, 4.4.4, 4.5.2 and 4.5.3 of [13]. The values held by the coherence, average coherence, orthogonality defect and product measure on the corresponding root lattices A_n for $n \geq 2$, D_n for $n \geq 4$, E_6, E_7, and E_8 are given in Table 2.

This data suggests that root lattices are generally better than cyclotomic lattices at simultaneously minimizing average coherence and maximizing orthogonality defect, however are worse at minimizing maximal coherence. Indeed, suppose some large p is the smallest prime dividing n and let $d = \varphi(n)$, then $\Lambda_{\mathbb{Q}(\zeta_n)})$ is a lattice in $\mathbb{R}^d$ with maximal coherence $1/(p-1)$, while A_d and D_d are root lattices in the same dimension with maximal coherence $1/2$.

In fact, an interesting feature of the cyclotomic lattices, in contrast with the root lattices, is that their maximal and average coherence are about the same on the

$\varphi(n)$	n	$\mathcal{C}_n$	$\mathcal{A}_n$	ν_n	Π_n
6	7	**0.166...**	0.166...	**1.666...**	11.662...
6	$9 = 3^2$	0.5	**0.125**	1.539...	**18.475...**
8	$15 = 3 \cdot 5$	0.5	0.214...	**3.640...**	**31.857...**
8	$16 = 2^4$	**0**	**0**	1	–
8	$20 = 2^2 \cdot 5$	0.25	0.157...	2.048	16.213...
8	$24 = 2^3 \cdot 3$	0.5	0.090...	1.777...	29.333...
24	$35 = 5 \cdot 7$	0.25	0.088...	**66.194...**	1094.055...
24	$39 = 3 \cdot 13$	0.5	0.078...	27.953...	575.369...
24	$45 = 3^2 \cdot 5$	0.5	0.068...	48.263...	**1327.257...**
24	$52 = 2^2 \cdot 13$	**0.083...**	0.04	4.975...	134.741...
24	$56 = 2^3 \cdot 7$	0.166...	0.037...	7.706...	242.742...
24	$72 = 2^3 \cdot 3^2$	0.5	**0.028...**	5.618...	294.979...
24	$84 = 2^2 \cdot 3 \cdot 7$	0.5	0.073...	43.297...	1035.542...
72	73	**0.013...**	0.013...	5.200...	379.606...
72	$91 = 7 \cdot 13$	0.166...	0.033...	56350.535...	$2.136... \cdot 10^6$
72	$95 = 5 \cdot 19$	0.25	0.031...	32670.615...	$1.350... \cdot 10^6$
72	$111 = 3 \cdot 37$	0.5	0.027...	2447.523...	$1.383... \cdot 10^5$
72	$117 = 3^2 \cdot 13$	0.5	0.025...	21841.954...	$1.372... \cdot 10^6$
72	$135 = 3^3 \cdot 5$	0.5	0.022...	$\mathbf{1.124... \cdot 10^5}$	$\mathbf{9.415... \cdot 10^6}$
72	$148 = 2^2 \cdot 37$	0.027...	0.013...	13.798...	1035.267...
72	$152 = 2^3 \cdot 19$	0.055...	0.013...	51.545...	4081.677...
72	$216 = 2^3 \cdot 3^3$	0.5	**0.009...**	177.376...	28469.292...
72	$228 = 2^2 \cdot 3 \cdot 19$	0.5	0.026...	9142.921...	$5.452... \cdot 10^5$
72	$252 = 2^2 \cdot 3^2 \cdot 7$	0.5	0.024.	81171.032...	$5.918... \cdot 10^6$
160	$187 = 11 \cdot 17$	0.1	0.016...	$1.163... \cdot 10^9$	$8.428... \cdot 10^{10}$
160	$205 = 5 \cdot 41$	0.25	0.014...	$3.928... \cdot 10^8$	$3.594... \cdot 10^{10}$
160	$328 = 2^3 \cdot 41$	**0.025**	0.006...	233.162...	77912.090...
160	$352 = 2^5 \cdot 11$	0.1	0.005...	104646.972...	$2.014... \cdot 10^7$
160	$400 = 2^4 \cdot 5^2$	0.25	**0.005...**	$1.684... \cdot 10^6$	$4.191... \cdot 10^8$
160	$440 = 2^3 \cdot 5 \cdot 11$	0.25	0.013...	$1.763... \cdot 10^{11}$	$1.769... \cdot 10^{13}$
160	$492 = 2^2 \cdot 3 \cdot 41$	0.5	0.012...	$2.318... \cdot 10^7$	$2.911... \cdot 10^9$
160	$528 = 2^4 \cdot 3 \cdot 11$	0.5	0.011...	$1.040... \cdot 10^{10}$	$1.505... \cdot 10^{12}$
160	$600 = 2^3 \cdot 3 \cdot 5^2$	0.5	0.010...	$1.675... \cdot 10^{11}$	$3.131... \cdot 10^{13}$
160	$660 = 2^2 \cdot 3 \cdot 5 \cdot 11$	0.5	0.021...	$\mathbf{1.753... \cdot 10^{16}}$	$\mathbf{1.699... \cdot 10^{18}}$

TABLE 1. Examples of coherence, average coherence, orthogonality defect and product measure values for cyclotomic lattices

average as $n \to \infty$. Indeed, $\mathcal{C}_n = 1/(\eta(n) - 1)$, where $\eta(n)$ is the smallest prime divisor of n. Now, the average order of $\eta(n)$ is known to be $(1 + o(1))n/2 \log n$ as $n \to \infty$ (see [12]). Hence the average order of $\mathcal{C}_n$ is $\frac{2 \log n}{n}$. On the other hand, the average order of $\omega(n)$ is $\log \log n$ (see Theorem 430 of [10]). Combining this observation with (5), we see that the average order of $\mathcal{A}_n$ is $\frac{\log 2 \log n}{n}$.

Lattice L	$\lvert S'(L)\rvert$	$\mathcal{C}(L)$	$\mathcal{A}(L)$	$\nu(L)$	$\Pi(L)$
A_n	$\frac{n(n+1)}{2}$	0.5	$\frac{2}{n+2}$	$\frac{2^{\frac{n}{2}}}{n+1}$	$(n+2)2^{\frac{n-4}{2}}$
D_n	$n(n-1)$	0.5	$\frac{2(n-2)}{n^2-n-1}$	$2^{\frac{n-4}{2}}$	$\frac{(n-1)(n^2-n-1)}{n-2}2^{\frac{n-6}{2}}$
E_6	36	0.5	$\frac{2}{7}$	$\frac{8}{3}$	56
E_7	63	0.5	$\frac{8}{31}$	$4\sqrt{2}$	13.138...
E_8	120	0.5	$\frac{28}{119}$	16	1020

TABLE 2. Coherence, average coherence, orthogonality defect and product measure values for root lattices

Acknowledgement: We thank the anonymous referee for many helpful remarks and suggestions that improved the quality of the paper.

REFERENCES

[1] W. Bajwa and R. Calderbank and S. Jafarpour. Why Gabor frames? Two fundamental measures of coherence and their role in model selection. *J. Commun. Netw.*, 12:289–307, 2010.

[2] W. Bajwa and R. Calderbank and D. G. Mixon. Two are better than one: fundamental parameters of frame coherence. *Appl. Comput. Harmon. Anal.*, 33(1):58–78, 2012.

[3] E. Bayer-Fluckiger. Cyclotomic modular lattices. *J. Théor. Nombres Bordeaux*, 12(2):273–280, 2000.

[4] E. Bayer-Fluckiger. Ideal lattices. *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, 168–184, Cambridge Univ. Press, Cambridge, 2002.

[5] A. I. Borevich and I. R. Shafarevich. Number theory. Translated from the Russian by Newcomb Greenleaf., Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966.

[6] J. H. Conway and N. J. A. Sloane. Sphere packings, lattices and groups, 3rd edition, Springer-Verlag, 1999.

[7] L. Fukshansky and D. Kogan. On the geometry of nearly orthogonal lattices. arXiv:2003.03840, 2020.

[8] L. Fukshansky and D. Needell and J. Park and Y. Xin. Lattices from tight frames and vertex transitive graphs. *Electron. J. Combin.*, 26 (2019), no. 3, Paper No. 3.49, 30 pp.

[9] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *Int. J. Number Theory*, 8(1):189–206, 2012.

[10] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers. 5th edition. The Clarendon Press, Oxford University Press, New York, 1979.

[11] R. B. Holmes and V. I. Paulsen. Optimal frames for erasures. *Linear Algebra Appl.*, 377:31–51, 2004.

[12] M. Kalecki. On certain sums extended over primes or prime factors. *Prace Mat.*, 8:121–129, 1963/1964.

[13] J. Martinet, Perfect lattices in Euclidean spaces, Springer-Verlag, 2003.

[14] J. Martinet and A. Schürmann, Bases of minimal vectors in lattices, III, Int. J. Number Theory, 8(2):551–567, 2012.

[15] D. Micciancio and S. Goldwasser, Complexity of lattice problems. A cryptographic perspective, The Kluwer International Series in Engineering and Computer Science, 671. Kluwer Academic Publishers, Boston, MA, 2002.

[16] M. Pohst, On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications, SIGSAM Bull., 15:37–44, 1981.

[17] M. A. Tsfasman and S. G. Vladut. *Algebraic-geometric codes*. Kluwer Academic Publishers Group, Dordrecht, 1991.

[18] S. F. D. Waldron. *An introduction to finite tight frames*. Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, New York, (2018).

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711
Email address: lenny@cmc.edu

Institute of Mathematical Sciences, Claremont Graduate University, Claremont, CA 91711
Email address: david.kogan@cgu.edu