JOURNAL OF NUMBER THEORY **57**, 181–197 (1996)
ARTICLE NO. 0042

Haar Bases for $L^2(\mathbb{R}^n)$ and Algebraic Number Theory

JEFFREY C. LAGARIAS

AT&T Bell Laboratories, Murray Hill, New Jersey 07974

AND

YANG WANG

Georgia Institute of Technology, Atlanta, Georgia 30332

Communicated by Alan C. Woods

Received July 26, 1994

Gröchenig and Madych showed that a Haar-type orthonormal wavelet basis of $L^2(\mathbb{R}^n)$ can be constructed from the characteristic function χ_Q of a set Q if and only if Q is an affine image of an integral self-affine tile T which tiles $\mathbb{R}^n$ using the integer lattice $\mathbb{Z}^n$. An integral self-affine tile $T = T(\mathsf{A}, \mathscr{D})$ is the attractor of an iterated function system $T = \bigcup_{i=1}^{m} \mathsf{A}^{-1}(T + \mathbf{d}_i)$ where $\mathsf{A} \in M_n(\mathbb{Z})$ is an expanding $n \times n$ integer matrix and the digit set $\mathscr{D} = \{\mathbf{d}_1, \mathbf{d}_2, ..., \mathbf{d}_m\} \subseteq \mathbb{Z}^n$ has $m = |\det(\mathsf{A})|$, provided that the Lebesgue measure $\mu(T) > 0$. Two necessary conditions for $T(\mathsf{A}, \mathscr{D})$ to tile $\mathbb{R}^n$ with the integer lattice $\mathbb{Z}^n$ are that $\mathscr{D}$ be a complete set of coset representatives of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$ and that $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$, where $\mathbb{Z}[\mathsf{A}, \mathscr{D}]$ is the smallest A-invariant lattice containing all $\{\mathbf{d}_i - \mathbf{d}_j : i \neq j\}$. These two conditions are necessary and sufficient in the special case that $|\det(\mathsf{A})| = 2$. We study these two conditions for an arbitrary matrix $\mathsf{A} \in M_n(\mathbb{Z})$. We prove that a digit set $\mathscr{D}$ satisfying the two conditions exists whenever $|\det(\mathsf{A})| \geqslant n + 1$. When $|\det(\mathsf{A})| = 2$ there are number-theoretic obstructions to the existence of such $\mathscr{D}$. Using these we exhibit a (non-expanding) $\mathsf{A} \in M_2(\mathbb{Z})$ for which no digit set has $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^2$. However we show that for all expanding integer matrices A in dimensions 2 and 3, there exists some digit set $\mathscr{D}$ that satisfies the two conditions. Could this be true for all expanding integer matrices in dimensions $n \geqslant 4$? A necessary condition is that the (non-Galois) field $\mathbb{Q}(\sqrt[n]{2})$ have class number one for all $n \geqslant 4$.

1. INTRODUCTION

In 1910 Haar [8] constructed an orthonormal basis of $L^2([0, 1])$ which consists of certain dilations and translations of a single function $\psi(x)$. The function $\psi(x)$ is the step function

$$\psi(x) = \begin{cases} 1 & 0 \leqslant x < 1/2, \\ -1 & 1/2 < x \leqslant 1, \\ 0 & \text{otherwise}, \end{cases}$$

0022-314X/96 $18.00

and the Haar basis of $L^2([0,1])$ is $\{2^{m/2}\psi(2^m x+n): m\in\mathbb{Z}_{\geqslant 0}, n\in\mathbb{Z}\}$. There is also a Haar basis of $L^2(\mathbb{R})$, which consists of the enlarged set of functions $\{2^{m/2}\psi(2^m x+n): m\in\mathbb{Z}, n\in\mathbb{Z}\}$.

Haar bases of $L^2(\mathbb{R}^n)$ are orthonormal wavelet bases that are higher dimensional analogues of the Haar basis of $L^2(\mathbb{R})$. As explained in §2, they are defined to be those wavelet bases of $L^2(\mathbb{R}^n)$ constructed by a multiresolution analysis whose scaling function is the characteristic function χ_Q of a set Q. Gröchenig and Madych [7] studied the problem of finding all such bases, and showed that Q must necessarily be an affine image of an integral self-affine tile T. Integral self-affine tiles T are constructed using certain data $(\mathsf{A}, \mathscr{D})$, in which A is an $n\times n$ integer matrix which is expanding, i.e. its characteristic polynomial has all its roots $|\lambda_i|>1$, and $\mathscr{D}=\{\mathbf{d}_1, ..., \mathbf{d}_m\}\subseteq\mathbb{Z}^n$ is a set of $m=|\det(\mathsf{A})|$ digits. The set $T=T(\mathsf{A},\mathscr{D})$ is the unique compact set satisfying the (set-valued) functional equation:

$$\mathsf{A}(T)=\bigcup_{i=1}^{m}(T+\mathbf{d}_i). \tag{1.1}$$

In fact T is also given by

$$T=\left\{\sum_{j=0}^{\infty}\mathsf{A}^{-j}\mathbf{d}_{i_j}: \text{all } \mathbf{d}_{i_j}\in\mathscr{D}\right\}. \tag{1.2}$$

Such a T is an *integral self-affine tile* if its Lebesgue measure $\mu(T)>0$. This name is justified by the property that, if $\mu(T)>0$, then T always tiles $\mathbb{R}^n$ by translation by some subset $\mathscr{S}$ of $\mathbb{Z}^n$, and we call any such $\mathscr{S}$ a *tiling set* for T. The condition $\mu(T)>0$ always holds when $\mathscr{D}=\{\mathbf{d}_1, ..., \mathbf{d}_m\}\subseteq\mathbb{Z}^n$ is a complete set of coset representation of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$, see Bandt [2]. Gröchenig and Madych [7] show that a further necessary condition for an integral self-affine tile T to give rise to a Haar basis is that T tile $\mathbb{R}^n$ with the full integer lattice $\mathbb{Z}^n$.

This paper addresses the question: Does every expanding integer matrix A possess some integer digit set $\mathscr{D}\subseteq\mathbb{Z}^n$ whose tile $T(\mathsf{A},\mathscr{D})$ gives rise to a Haar-type wavelet basis of $L^2(\mathbb{R}^n)$? This question was raised by Gröchenig and Haas [6]. It has an affirmative answer for dimension $n=1$, as shown by Kenyon [9] and Gröchenig and Haas [6], and for dimension $n=2$, as shown by Lagarias and Wang [13]. It is unresolved for dimensions $n\geqslant 3$, and this paper presents results bearing on this case.

As remarked above, not all pairs $(\mathsf{A},\mathscr{D})$ give Haar-type wavelet bases of $L^2(\mathbb{R}^n)$. More precisely, Gröchenig and Madych [7] show that the characteristic function $\chi_T(\mathbf{x})$ of the tile T is the scaling function for a multiresolution analysis and an associated wavelet basis of $L^2(\mathbb{R}^n)$ if and only if the digit set $\mathscr{D}$ is a complete set of coset representatives of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$ and the whole lattice $\mathbb{Z}^n$ is a tiling set for T, see Theorem 2.1 in Section 2.

There are two simple necessary conditions for an integral self-affine tile $T(\mathsf{A}, \mathscr{D})$ to have a $\mathbb{Z}^n$-tiling, stated as Theorem 1.1 below. A digit set $\mathscr{D}$ is *complete* if it is a complete set of residues of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$. A lattice Γ is A-invariant if $\mathsf{A}(\Gamma) \subseteq \Gamma$. The *containment lattice* $\mathbb{Z}[\mathsf{A}, \mathscr{D}]$ of a pair $(\mathsf{A}, \mathscr{D})$ is the smallest A-invariant lattice containing all differences of digits $\{\mathbf{d}_i - \mathbf{d}_j\colon\ 1 \leqslant i, j \leqslant n\}$, i.e.

$$\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}[\mathsf{A}^k(\mathbf{d}_j - \mathbf{d}_1)\colon 2 \leqslant j \leqslant m, k \geqslant 0]. \tag{1.3}$$

An integer digit set $\mathscr{D}$ is *primitive* (for A) if $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$. Lagarias and Wang [11] showed:

THEOREM 1.1. *Let $\mathsf{A} \in M_n(\mathbb{Z})$ be an expanding integer matrix in $\mathbb{R}^n$. If a digit set $\mathscr{D} \subseteq \mathbb{Z}^n$ with $|\mathscr{D}| = \det(\mathsf{A})$ gives a tile $T(\mathsf{A}, \mathscr{D})$ that $\mathbb{Z}^n$-tiles $\mathbb{R}^n$, then*:

(i) *$\mathscr{D}$ is a complete set of residues (mod $\mathsf{A}(\mathbb{Z}^n)$).*

(ii) $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$.

These two necessary conditions assert that $(\mathsf{A}, \mathscr{D})$ is a primitive complete digit set, or, in the terminology of [11], a primitive standard digit set.[1]

These necessary conditions are sufficient for $n = 1$ as was proved by Kenyon [9], and Gröchenig and Haas [6]. In dimensions $n \geqslant 2$ they are not sufficient, as shown by the example $\mathsf{A} = \left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right]$, $\mathscr{D} = \left\{\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 3 \\ 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 3 \\ 1 \end{smallmatrix}\right]\right\}$ which has $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^2$ but does not tile with the lattice $\mathbb{Z}^2$, see Lagarias and Wang [10], Example 2.3. The structure of exceptional pairs $(\mathsf{A}, \mathscr{D})$ having $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$ but no $\mathbb{Z}^n$-tiling is classified in Lagarias and Wang [12], §6. In particular Corollary 6.2 of [12] implies that if $|\det(\mathsf{A})| = p$ is prime then the conditions (i) and (ii) of Theorem 1.1 are necessary and sufficient for $\mathrm{T}(\mathsf{A}, \mathscr{D})$ to $\mathbb{Z}^n$-tile $\mathbb{R}^n$.

There remains the possibility that there are expanding integer matrices which have no Haar-type wavelet bases because the necessary conditions of Theorem 1.1 fail to hold for every digit set. Motivated by this possibility, this paper studies the problem: Which integer matrices A have a primitive complete digit set? This question makes sense for any $\mathsf{A} \in M_n(\mathbb{Z})$, so we do not require that A be an expanding matrix.

In Section 2 we prove the following simple fact.

[1] The notion of *standard digit set* in [11] is more general than the notion of complete digit set, but primitive complete digit set $\equiv$ primitive standard digit set.

THEOREM 1.2. (i) *If there exists a primitive complete digit set $\mathscr{D}$ for the integer matrix A and if $\tilde{\mathsf{A}}$ is similar to A over $\mathbb{Z}$, then there is a primitive complete digit set for $\tilde{\mathsf{A}}$.*

(ii). *For every integer matrix A there is some integer matrix $\tilde{\mathsf{A}}$ similar to A over $\mathbb{Q}$ such that $\tilde{\mathsf{A}}$ has a primitive complete digit set.*

Thus the property of having a complete primitive digit set is a $\mathbb{Z}$-similarity invariant of A.

In Section 3 we show that primitive complete digit sets exist for most integer matrices.

THEOREM 1.3. *Let A be any integer matrix with $|\det(\mathsf{A})| \geqslant n+1$. Then A has a digit set $\mathscr{D} \subset \mathbb{Z}^n$ consisting of a complete set of residues of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$ such that $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$.*

The hypothesis $|\det(\mathsf{A})| \geqslant n+1$ cannot be removed, for there are examples of 2×2 matrices A with $|\det(\mathsf{A})| = 2$ having no primitive complete digit set.

In Section 4 we treat matrices A with $|\det(\mathsf{A})| = 2$, which have a characteristic polynomial $f_{\mathsf{A}}(x)$ that is irreducible over $\mathbb{Q}$. This case covers all expanding integer matrices with $|\det(\mathsf{A})| = 2$, because the characteristic polynomial of any such matrix is irreducible.[2] We show that there are number theoretic conditions which must be satisfied for a primitive complete digit set to exist.

THEOREM 1.4. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n irreducible over $\mathbb{Q}$ with $|f(0)| = 2$, and let θ be a root of $f(x)$. Then every matrix $\mathsf{A} \in M_n(\mathbb{Z})$ with characteristic polynomial $f(x)$ has a primitive complete digit set if and only if the ring $R_\theta := \mathbb{Z}[1, \theta, \theta^2, ..., \theta^{n-1}]$ has class number one.*

For the (nonexpanding) polynomial $f(x) = x^2 - 11x - 2$ the ring $R_\theta = [1, (1+\sqrt{129})/2]$ has class number 2, so there exists a (nonexpanding) matrix A with characteristic polynomial $f(x)$ that has no primitive complete digit set, e.g. $\mathsf{A} = \left[\begin{smallmatrix} 17 & -10 \\ 10 & -6 \end{smallmatrix}\right]$.

An expanding integer matrix A for which the class number of the corresponding ring R_θ is greater than one would give an example of an A having no associated Haar-type wavelet bases. We do not know of any expanding integer matrix A having this property. The results of section 5 below show that any such expanding matrix must have dimension $n \geqslant 4$.

[2] If $f_{\mathsf{A}}(x)$ were reducible, it would contain at least one monic factor $f(x)$ over $\mathbb{Z}[x]$ having $|f(0)| = 1$. Then $f(x)$ has some root $|\theta| \leqslant 1$, so $f_{\mathsf{A}}(x)$ cannot be expanding.

An infinite family of expanding matrices with $|\det(\mathsf{A})| = 2$ is provided by the family of matrices A having characteristic polynomials $f(x) = x^n - 2$, for $n \geqslant 2$. Concerning these, Theorem 1.4 yields the following result.

COROLLARY 1.4. *For $n \geqslant 3$, let $\sqrt[n]{2}$ denote the positive real n-th root of 2. If the (non-Galois) field $\mathbb{Q}(\sqrt[n]{2})$ has class number h_n greater than 1, then there is an $n \times n$ expanding integer matrix $|\mathsf{A}|$ with $|\det(\mathsf{A})| = 2$ such that no digit set $\mathscr{D} \subseteq \mathbb{Z}^n$ which is a complete set of residues of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$ has $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$. If so, then there are no integer digit sets $\mathscr{D}$ for A giving a Haar-type wavelet basis of $L^2(\mathbb{R}^n)$.*

By analogy with cyclotomic fields, one might guess that the class number h_n of $\mathbb{Q}(\sqrt[n]{2})$ will become large as $n \to \infty$. However Michael Pfeifer (private communication) has computed that $h_n = 1$ for for $2 \leqslant n \leqslant 29$, using the algebraic number theory package KANT.[3] Thus we still have the:

OPEN QUESTION. *Is the class number h_n of the (non-Galois) field $\mathbb{Q}(\sqrt[n]{2})$ equal to 1 for all $n \geqslant 3$?*

How strongly does the evidence of Pfeifer's computations support the belief that all $h_n = 1$? The discriminant bounds of Odlyzko, assuming the Generalized Riemann Hypothesis, would force the class number to be 1 up to perhaps $n \approx 20$, see Odlyzko [18]. If further numerical work shows that $h_n = 1$ for all $n \leqslant 50$, then the possibility that all $h_n = 1$ might well be taken seriously. We note that it is a well-known open problem to show that there are infinitely many different algebraic number fields whose ring of integers has class number one.

In §5 we treat expanding integer matrices in dimensions 2 and 3. We first prove that, in any dimension, there are only finitely many $\mathbb{Z}$-similarity classes of expanding integer matrices A having $|\det(\mathsf{A})| = p$, when p is prime (Lemma 5.1). By computation we determine the complete list of such similarity classes in dimension $n = 2$ for $p = 2$, and in dimension 3 for $p = 2$ and 3. Combining this with Theorem 1.3 and 1.4 we obtain the following result.

THEOREM 1.5. *For $n = 1, 2$ and 3 every expanding $n \times n$ integer matrix A has a digit set $\mathscr{D} \subseteq \mathbb{Z}^n$ consisting of a complete set of residues of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$ such that $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$.*

The result for $n = 3$ is new, while the result for $n = 1$ is deducible from the results of Kenyon [9] and Gröchenig and Haas [6] and for $n = 2$ from the results of Lagarias and Wang [13].

[3] Pfeifer actually computed that the ring $\mathbb{Z}[1, \theta, \theta^2, ..., \theta_{n-1}]$ with $\theta = \sqrt[n]{2}$ has class number 1, for $2 \leqslant n \leqslant 29$. For a description of KANT see Graf von Schmettow [5].

Finally, we note that Haar-type wavelet bases make up the families of wavelets of compact support in $\mathbb{R}^n$ with the least amount of smoothness, i.e., they are discontinuous. An important unresolved issue concerns the existence and construction of smoother wavelets of compact support, which are in $C^k(\mathbb{R}^n)$ for some $k \geqslant 0$, for general matrices A, cf. Strichartz [19].

We are indebted to I. Daubechies, K. H. Gröchenig, A. Haas and A. M. Odlyzko for helpful comments and references.

2. Haar-Type Wavelet Bases and Primitive Complete Digit Sets

We describe in more detail the notion of Haar-type wavelet basis, and then prove Theorem 1.2.

Multiresolution analysis is a general procedure for constructing orthonormal wavelet bases of $L^2(\mathbb{R}^n)$, due to Meyer [16] and Mallat [15]. *A multiresolution analysis in* $\mathbb{R}^n$ is done with respect to a pair (Γ, A), where Γ is a (full rank) lattice Γ in $\mathbb{R}^n$ and $\mathsf{A} \in M_n(\mathbb{R})$ is a matrix which has the two properties:

(i) A is an expanding matrix, i.e. all its eigenvalues $|\lambda_i| > 1$.

(ii) Γ is an invariant lattice of A, i.e. $\mathsf{A}(\Gamma) \subseteq \Gamma$.

Such an A is called an *acceptable dilation* for Γ and condition (ii) implies that $m = |\det(\mathsf{A})|$ is an integer. The main ingredient in a multiresolution analysis is a *scaling function* $\phi(\mathbf{x}) \in L^2(\mathbb{R}^n)$. Necessary and sufficient conditions for $\phi(\mathbf{x})$ to give a multiresolution analysis are:

(i) The scaling function ϕ satisfies a dilation equation

$$\phi(\mathbf{x}) = \sum_{\gamma \in \Gamma} a_\gamma \, |\det(\mathsf{A})|^{1/2} \, \phi(\mathsf{A}\mathbf{x} - \gamma),$$

and $\{\phi(\mathbf{x} - \gamma): \gamma \in \Gamma\}$ is an orthonormal basis of the linear space V_0 that it spans.

(ii) Let V_j be the linear space spanned by $\{\phi(\mathsf{A}^j\mathbf{x} - \gamma): \gamma \in \Gamma\}$. Then

$$\bigcap_{j \in \mathbb{Z}} V_j = \{0\} \qquad \text{and} \qquad \overline{\bigcup_{j \in \mathbb{Z}} V_j} = L^2(\mathbb{R}^n).$$

When these two conditions are satisfied, there are $m-1$ associated wavelets constructed from ϕ, which have the form

$$\psi_i(\mathbf{x}) = \sum_{\gamma \in \Gamma} b_\gamma^{(i)} \, |\det(\mathsf{A})|^{1/2} \, \phi(\mathsf{A}\mathbf{x} - \gamma), \qquad 1 \leqslant i \leqslant m-1,$$

for certain coefficient sets $\{b_\gamma^{(i)}\}$. (They form a basis of the orthogonal complement of V_0 in V_1.) The associated orthonormal wavelet basis of $L^2(\mathbb{R}^n)$ is then

$$\{|\det(\mathsf{A})|^{j/2}\,\psi_i(\mathsf{A}^j\mathbf{x}-\boldsymbol{\gamma}):\ 1\leqslant i\leqslant m-1,\ j\in\mathbb{Z},\ \boldsymbol{\gamma}\in\Gamma\}.$$

Not all orthonormal wavelet bases come from a multiresolution analysis. However it may be that all compactly supported orthonormal wavelet bases do come from a multiresolution analysis. This has been proved in dimension 1 by Lemarié [14]. For more details on multiresolution analysis, see Daubechies [3, Chap. 5] or Mallat [15].

The Haar basis $\{2^{m/2}\psi(2^m x+n):\ m,n\in\mathbb{Z}\}$ of $L^2(\mathbb{R})$ provides the simplest example of a multiresolution analysis, with $\mathsf{A}=[2]$ and $\Gamma=\mathbb{Z}$. The scaling function is

$$\phi(x):=\chi_{[0,\,1]}(x)=\begin{cases}1 & x\in[0,1]\\ 0 & \text{otherwise,}\end{cases}\tag{2.1}$$

and the associated wavelet is

$$\psi(x)=\phi(2x)-\phi(2x+1).\tag{2.2}$$

The scaling function $\phi(x)$ satisfies the dilation equation

$$\phi(x)=\phi(2x)+\phi(2x-1),\tag{2.3}$$

and the orthonormality conditions

$$\int_{\mathbb{R}}\phi(x)\,\phi(x-n)\,dx=\begin{cases}1 & \text{if}\quad n=0,\\ 0 & \text{if}\quad n\in\mathbb{Z}\setminus\{0\}.\end{cases}\tag{2.4}$$

These orthonormality conditions express the fact that the interval $[0,1]$ tiles $\mathbb{R}$ using the lattice $\mathbb{Z}$, and the orthonormality of the Haar basis of $L^2(\mathbb{R})$ follows from (2.2)–(2.4).

A *Haar-type wavelet basis* of $L^2(\mathbb{R}^n)$ is one arising from a multiresolution analysis in which the scaling function $\phi(\mathbf{x})$ is the characteristic function $\chi_Q(\mathbf{x})$ of a compact set $Q\subseteq\mathbb{R}^n$. Haar-type wavelet bases consist of compactly-supported functions.

One can always convert any multiresolution analysis to a case where the lattice $\Gamma=\mathbb{Z}^n$ and the matrix $\mathsf{A}\in M_n(\mathbb{Z})$ is an expanding integer matrix, by making a suitable linear change of variable. This reduction preserves the Haar-type wavelet basis property, so without loss of generality we suppose that $\Gamma=\mathbb{Z}^n$ and $\mathsf{A}\in M_n(\mathbb{Z})$.

Let $T_1=T_2$ mean that T_1 and T_2 agree up to a set of measure zero. Gröchenig and Madych [7] proved:

THEOREM 2.1 (Gröchenig and Madych). *Suppose that a multiresolution analysis associated with* $(\mathbb{Z}^n, \mathsf{A})$ *has a scaling function* $\phi(\mathbf{x}) = c_Q \chi_Q(\mathbf{x})$ *where* Q *is a measurable set of finite measure and* c_Q *is chosen so that* $\|\phi(\mathbf{x})\|_2 = 1$. *Then there is a compact set* T *with* $Q \simeq T$ *such that*:

(i) $T = T(\mathsf{A}, \mathscr{D})$ *is an integral self affine tile with digit set* $\mathscr{D} \subseteq \mathbb{Z}^n$.

(ii) *The digit set* $\mathscr{D} = \{\mathbf{d}_1, ..., \mathbf{d}_m\} \subseteq \mathbb{Z}^n$ *is a primitive complete set of residue classes of* $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$.

(iii) T *tiles* $\mathbb{R}^n$ *with a* $\mathbb{Z}^n$*-tiling.*

Conversely if a set $Q = T$ *for a set* T *having properties* (i), (ii), (iii) *then* $\chi_Q(\mathbf{x})$ *is the scaling function for a multiresolution analysis associated with* $(\mathbb{Z}^n, \mathsf{A})$.

Proof. This is Theorem 1 of Gröchenig and Madych [7], combined with some remarks they make just after the theorem statement. Note that condition (ii) implies that necessarily $c_Q = \mu(T)^{-1/2} = 1$. ∎

Theorem 1.1 shows that condition (ii) can be omitted in this theorem—it is implied by condition (iii). Also using Theorem 1.1 we see that a Haar-type wavelet basis can only arise from a pair $(\mathsf{A}, \mathscr{D})$ where $\mathscr{D}$ is a primitive complete digit for A. We now prove some properties of primitive complete digit sets.

Proof of Theorem 1.2. (i) For any matrix $\mathsf{B} \in M_n(\mathbb{R})$, the formula (1.2) yields

$$T(\mathsf{BAB}^{-1}, \mathsf{B}(\mathscr{D})) = \mathsf{B}(T(\mathsf{A}, \mathscr{D})) \tag{2.5}$$

and (1.3) yields

$$\mathbb{Z}[\mathsf{BAB}^{-1}, \mathsf{B}(\mathscr{D})] = \mathsf{B}(\mathbb{Z}[\mathsf{A}, \mathscr{D}]). \tag{2.6}$$

Here $\tilde{\mathsf{A}} = \mathsf{BAB}^{-1} \in M_n(\mathbb{R})$ is not necessarily an integral matrix. However if $\tilde{\mathsf{A}}$ is integrally similar to A, then $\tilde{\mathsf{A}} = \mathsf{UAU}^{-1}$ for some $\mathsf{U} \in GL(n, \mathbb{Z})$, and if $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$, then (2.2) yields

$$\mathbb{Z}[\tilde{\mathsf{A}}, \mathsf{U}(\mathscr{D})] = \mathsf{U}(\mathbb{Z}[\mathsf{A}, \mathscr{D}]) = \mathbb{Z}^n.$$

Finally if $\mathscr{D}$ is a primitive complete set of digits for $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$, then $\mathsf{U}(\mathscr{D})$ is a complete set of digits for $\mathbb{Z}^n/\tilde{\mathsf{A}}(\mathbb{Z}^n)$, so (i) follows.

(ii) Take any complete set of digits $\mathscr{D}$ for A having $\mathbf{0} \in \mathscr{D}$. If $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$ we are done, so suppose $\mathbb{Z}[\mathsf{A}, \mathscr{D}] \neq \mathbb{Z}^n$. Let $\mathsf{B} \in M_n(\mathbb{Z})$ be a matrix whose columns form a basis of the lattice $\mathbb{Z}[\mathsf{A}, \mathscr{D}]$, so that

$$\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathsf{B}(\mathbb{Z}^n), \tag{2.7}$$

and $|\det(\mathsf{B})| = [\mathbb{Z}^n: \mathbb{Z}[\mathsf{A}, \mathscr{D}]] > 1$. Let $[\mathbf{e}_1 \mathbf{e}_2 \cdots \mathbf{e}_n]$ denote the standard basis of unit column vectors giving the identity matrix. The vectors $\mathsf{AB}\mathbf{e}_i$ are all in $\mathbb{Z}[\mathsf{A}, \mathscr{D}]$ because it is A-invariant, hence $\mathsf{AB}\mathbf{e}_j = \mathsf{B}\tilde{\mathbf{a}}_j$ for some $\tilde{\mathbf{a}}_j \in \mathbb{Z}^n$. Thus

$$\mathsf{AB} = \mathsf{B}\tilde{\mathsf{A}}$$

where $\tilde{\mathsf{A}} = [\tilde{\mathbf{a}}_1 \cdots \tilde{\mathbf{a}}_n] \in M_n(\mathbb{Z})$, and $\tilde{\mathsf{A}}$ is similar to A over $\mathbb{Q}$.

Now define $\tilde{\mathscr{D}} = \{\tilde{\mathbf{d}}_i: 1 \leqslant i \leqslant m\}$ by $\mathbf{d}_i = \mathsf{B}\tilde{\mathbf{d}}_i$, so $\mathscr{D} = \mathsf{B}(\tilde{\mathscr{D}})$. We will show that $\tilde{\mathscr{D}}$ is a primitive complete digit set for $\tilde{\mathsf{A}}$.

We first observe that $\tilde{\mathscr{D}} \subseteq \mathbb{Z}^n$ because $\mathbf{d}_i = \mathbf{d}_i - \mathbf{0} \in \mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathsf{B}(\mathbb{Z}^n)$. Now (2.2) gives

$$\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathsf{B}(\mathbb{Z}[\tilde{\mathsf{A}}, \tilde{\mathscr{D}}]),$$

whence (2.7) gives $\mathbb{Z}[\tilde{\mathsf{A}}, \tilde{\mathscr{D}}] = \mathbb{Z}^n$. Finally we show that $\tilde{\mathscr{D}}$ is a complete digit set for $\mathbb{Z}^n/\tilde{\mathsf{A}}(\mathbb{Z}^n)$. Suppose not, and that $\tilde{\mathbf{d}}_i - \tilde{\mathbf{d}}_j = \tilde{\mathsf{A}}\mathbf{v}$ for some $\mathbf{v} \in \mathbb{Z}^n$. Then (2.4) gives

$$\mathbf{d}_i - \mathbf{d}_j = \mathsf{B}\tilde{\mathsf{A}}\mathbf{v} = \mathsf{AB}\mathbf{v} \in \mathsf{A}(\mathbb{Z}^n),$$

which contradicts $\mathscr{D}$ being a complete digit set for $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$. ∎

3. Primitive Complete Digit Sets: $\det(\mathsf{A}) > n$

We construct a primitive complete digit set for all matrices $\mathsf{A} \in M_n(\mathbb{Z})$ with $|\det(\mathsf{A})| > n$.

Proof of Theorem 1.3. Without loss of generality, suppose $\mathscr{D} = \{\mathbf{0}, \mathbf{d}_1, ..., \mathbf{d}_{m-1}\}$, so $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}[\mathsf{A}^k\mathbf{d}_i: 1 \leqslant i \leqslant m-1, k \geqslant 0]$. Since $|\det(\mathsf{A})| \geqslant n+1$, there are at least n nonzero digits. We assert that one can already choose the first n of them so that

$$\mathbb{Z}^n = \mathbb{Z}[\mathbf{d}_1, ..., \mathbf{d}_n] \subseteq \mathbb{Z}[\mathsf{A}, \mathscr{D}].$$

If so, then completing the set $\mathbf{d}_1, ..., \mathbf{d}_n$ in any way whatsoever to a complete set of coset representatives of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$ yields a primitive complete digit set.

This assertion is equivalent to the following:

Claim. *If* $\mathsf{A} \in M_n(\mathbb{Z})$ *has* $|\det(\mathsf{A})| \geqslant n+1$, *then there is a basis* $[\mathbf{d}_1, ..., \mathbf{d}_n]$ *of* $\mathbb{Z}^n$ *whose elements lie in distinct nonzero residue classes of* $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$.

Since $\{\mathbf{0}, \mathbf{d}_1, ..., \mathbf{d}_n\}$ are then distinct residue classes of $\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n)$, one certainly needs the hypothesis $|\det(\mathsf{A})| \geqslant n+1$ in this claim.

It remains to prove the claim. We make use of the Smith normal form for A: there exist $\mathsf{UV} \in GL(n, \mathbb{Z})$ such that

$$\mathsf{UAV} = \operatorname{diag}(s_1, s_2, ..., s_n) = \begin{bmatrix} s_1 & & & \\ & s_2 & & \\ & & \ddots & \\ & & & s_n \end{bmatrix}, \tag{3.1}$$

in which the s_i are positive integers such that s_{i+1} divides s_i. (See Newman [17], Theorem II.9; it is easy to reverse the order of diagonal elements by using permutation matrices, and all $s_i \geqslant 1$ because $\det(\mathsf{A}) \neq 0$.) Set $\mathsf{M} = \mathsf{UAV}$, and

$$\mathbb{Z}^n/\mathsf{A}(\mathbb{Z}^n) \cong \mathbb{Z}^n/\mathsf{M}(\mathbb{Z}^n) \cong (\mathbb{Z}/s_1\mathbb{Z}) \oplus (\mathbb{Z}/s_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/s_n\mathbb{Z}).$$

We first show that M has a basis $[\tilde{\mathbf{b}}_1, ..., \tilde{\mathbf{b}}_n]$ with the required property. Suppose that $s_i > 1$ for $1 \leqslant i \leqslant k$ and $s_i = 1$ for $k+1 \leqslant i \leqslant n$. A complete set of coset representatives of $\mathbb{Z}/\mathsf{M}(\mathbb{Z}^n)$ is:

$$a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \cdots + a_k\mathbf{e}_k, \tag{3.2}$$

where $[\mathbf{e}_1\mathbf{e}_2...\mathbf{e}_n]$ is the standard basis of unit column vectors and each integer a_i has $0 \leqslant a_i \leqslant s_i - 1$. Totally order this set of $|\det(\mathsf{M})|$ elements in order of increasing value of $t = \sum_{i=1}^{k} a_i$, using the lexicographic ordering of $(a_1, ..., a_k)$ to break ties for representatives having the same value of t. Denote the reordered set of vectors $\mathbf{x}_0, \mathbf{x}_1, ..., \mathbf{x}_{m-1}$, where $m = |\det(\mathsf{M})|$, in which case $\mathbf{x}_0 = \mathbf{0}$ and $\mathbf{x}_i = \mathbf{e}_i$ for $1 \leqslant i \leqslant k$. We then set

$$\begin{aligned} \tilde{\mathbf{b}}_i &:= \mathbf{e}_i, \qquad 1 \leqslant i \leqslant k, \\ \tilde{\mathbf{b}}_i &:= \mathbf{e}_i + \mathbf{x}_i, \qquad k+1 \leqslant i \leqslant n. \end{aligned} \tag{3.3}$$

Since $m \geqslant n$ the vectors $\tilde{\mathbf{b}}_0 := \mathbf{0}$, $\tilde{\mathbf{b}}_1, \tilde{\mathbf{b}}_2, ..., \tilde{\mathbf{b}}_n$ lie in distinct cosets of $\mathbb{Z}^n/\mathsf{M}(\mathbb{Z}^n)$, because $\tilde{\mathbf{b}}_i - \mathbf{x}_i \in \mathsf{M}(\mathbb{Z}^n)$ for $1 \leqslant i \leqslant n$. Also $[\tilde{\mathbf{b}}_1, ..., \tilde{\mathbf{b}}_n]$ form a basis for $\mathbb{Z}^n$ because the change of basis from $\mathbf{e}_i$ to $\tilde{\mathbf{b}}_i$ is lower triangular with 1's on the diagonal.

Now set $\tilde{\mathsf{A}} := \mathsf{V}^{-1}\mathsf{AV}$, so that

$$\mathsf{M} = \mathsf{UAV} = \mathsf{UV}\tilde{\mathsf{A}}, \tag{3.4}$$

and also set

$$\tilde{\mathbf{d}}_i := \mathsf{V}^{-1}\mathsf{U}^{-1}\tilde{\mathbf{b}}_i, \qquad 1 \leqslant i \leqslant n. \tag{3.5}$$

Clearly $[\tilde{\mathbf{d}}_1, ..., \tilde{\mathbf{d}}_n]$ is a basis of $\mathbb{Z}^n$ because $\mathsf{V}^{-1}\mathsf{U}^{-1} \in GL(n, \mathbb{Z})$. Also $\tilde{\mathbf{d}}_0 = \mathbf{0}$ and all residues of $\tilde{\mathbf{d}}_0, \tilde{\mathbf{d}}_1, ..., \tilde{\mathbf{d}}_n$ are distinct in $\mathbb{Z}^n/\tilde{\mathsf{A}}(\mathbb{Z}^n)$, since

$$\tilde{\mathbf{d}}_i - \tilde{\mathbf{d}}_j \in \tilde{\mathsf{A}}(\mathbb{Z}^n) \Leftrightarrow \mathsf{V}^{-1}\mathsf{U}^{-1}(\tilde{\mathbf{b}}_i - \tilde{\mathbf{b}}_j) \in \tilde{\mathsf{A}}(\mathbb{Z}^n)$$
$$\Leftrightarrow \tilde{\mathbf{b}}_i - \tilde{\mathbf{b}}_j \in \mathsf{UV}\tilde{\mathsf{A}}(\mathbb{Z}^n) = \mathsf{M}(\mathbb{Z}^n).$$

Thus $\tilde{\mathsf{A}}$ has a basis $\tilde{\mathscr{D}} = [\tilde{\mathbf{d}}_1, ..., \tilde{\mathbf{d}}_n]$ of the required kind. Finally $\mathsf{A} = \mathsf{V}\tilde{\mathsf{A}}\mathsf{V}^{-1}$ has the basis $\mathscr{D} = \mathsf{V}(\tilde{\mathsf{D}})$ of the required kind, as in Theorem 1.2. This proves the claim, which completes the proof. ∎

4. Primitive Complete Digit Sets: $\det(\mathsf{A}) = 2$

Suppose that $\mathsf{A} \in M_n(\mathbb{Z})$ is a (not necessarily expanding) matrix with $|\det(\mathsf{A})| = 2$. In this case any primitive digit set for A is automatically a complete digit set. To see this, without loss of generality reduce to the case that $\mathscr{D} = \{\mathbf{0}, \mathbf{d}\}$, and note that if $\mathbf{d} \in \mathsf{A}(\mathbb{Z}^n)$ then

$$\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}[\mathsf{A}^k\mathbf{d}: k \geqslant 0] \subseteq \mathsf{A}(\mathbb{Z}^n). \tag{4.1}$$

Theorem 1.2 says that the existence of a primitive complete digit set for A is determined by the $\mathbb{Z}$-similarity class of A. The $\mathbb{Z}$-similarity classes of matrices A having a fixed characteristic polynomial $f(x)$ irreducible over $\mathbb{Q}$ are classified by the Lattimer–MacDuffee theorem, cf. Newman [17], Sect. III.16. This theorem says that there is a one-to-one correspondence between $\mathbb{Z}$-similarity classes and ideal classes of the ring $R_\theta := \mathbb{Z}[1, \theta, ..., \theta^{n-1}]$, where θ is a root of $f(x) = 0$. More precisely, choose a right eigenvector $\mathbf{v} = (v_1, ..., v_n)^T$ for the eigenvalue θ, which has all $v_i \in \mathbb{Q}(\theta)$. This can always be done. Then set

$$\mathfrak{a} = \mathfrak{a}(\mathbf{v}) := \mathbb{Z}[v_1, ..., v_n]. \tag{4.2}$$

It is an R_θ-ideal, because $\mathsf{A}\mathbf{v} = \theta\mathbf{v}$, and it depends on the choice of $\mathbf{v}$. The set $\mathscr{I}_\mathsf{A} = \{\alpha\mathfrak{a}: \alpha \in \mathbb{Q}(\theta)\}$ specifies an ideal class of (fractional) ideals in R_θ, which is independent of the choice of eigenvector $\mathbf{v}$, so depends only on A. The Lattimer–MacDuffee theorem then says that if A and $\tilde{\mathsf{A}}$ both have the same irreducible characteristic polynomial, then A is $\mathbb{Z}$-similar to $\tilde{\mathsf{A}}$ if and only if $\mathscr{I}_\mathsf{A} = \mathscr{I}_{\tilde{\mathsf{A}}}$.

Theorem 1.4 is an easy consequence of the following result.

Theorem 4.1. *Suppose that $\mathsf{A} \in M_n(\mathbb{Z})$ has $|\det(\mathsf{A})| = 2$, and that its characteristic polynomial $f_\mathsf{A}(x)$ is irreducible over $\mathbb{Q}$. Let θ be a root of $f_\mathsf{A}(x)$. Then A has a digit set $\mathscr{D} = \{\mathbf{d}_1, \mathbf{d}_2\} \subset \mathbb{Z}^n$ with $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$ if and only if A^T corresponds to a principal ideal of the ring $\mathbb{Z}[1, \theta, ..., \theta^n]$ under the Lattimer–MacDuffee correspondence.*

Proof. Without loss of generality, we may suppose $\mathbf{0} \in \mathscr{D}$, so that $\mathscr{D} = \{\mathbf{0}, \mathbf{d}\}$. We claim that

$$\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}[\mathbf{d}, \mathsf{A}\mathbf{d}, \mathsf{A}^2\mathbf{d}, ..., \mathsf{A}^{n-1}\mathbf{d}]. \tag{4.3}$$

By the Cayley-Hamilton theorem A^n is a $\mathbb{Z}$-linear combination of $\{\mathsf{A}^k: 0 \leqslant k \leqslant n-1\}$, hence all $\{\mathsf{A}^k\mathbf{d}; k \geqslant n\}$ are in the lattice given by the right side of (4.3). The vectors $\{\mathsf{A}^i\mathbf{d}: a \leqslant i \leqslant n-1\}$ span $\mathbb{R}^n$, because they generate an A-invariant rational subspace, and no nonzero rational subspace except $\mathbb{R}^n$ is A-invariant, because $f_{\mathsf{A}}(x)$ is irreducible. Thus $\mathbb{Z}[\mathsf{A}, \mathscr{D}]$ has full rank and has the basis matrix

$$\mathsf{B} = [\mathbf{d}\ \mathsf{A}\mathbf{d} \ldots \mathsf{A}^{n-1}\mathbf{d}], \tag{4.4}$$

so $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$ if and only if $\det(\mathsf{B}) = \pm 1$.

Now A^T has the same characteristic polynomial as A, so it has a right-eigenvector $\tilde{\mathbf{v}} = (\tilde{v}_1, ..., \tilde{v}_n)^T$ with eigenvalue θ and with all $\tilde{v}_i \in \mathbb{Q}(\theta)$. Furthermore we can scale it to have all $\tilde{v}_i \in \mathbb{Z}[1, \theta, ..., \theta^{n-1}]$. By the Lattimer–MacDuffee theorem the R_θ-ideal $\mathfrak{a}(\mathbf{v}) = \mathbb{Z}[\tilde{v}_1, ..., \tilde{v}_n]$ is in the ideal class associated to A^T. A simple calculation gives

$$\mathsf{B}^T\tilde{\mathbf{v}} = \begin{bmatrix} \mathbf{d}^T\tilde{\mathbf{v}} \\ \mathbf{d}^T\mathsf{A}^T\tilde{\mathbf{v}} \\ \cdots \\ \mathbf{d}^T(\mathsf{A}^T)^{n-1}\tilde{\mathbf{v}} \end{bmatrix} = \langle \mathbf{d}, \tilde{\mathbf{v}} \rangle \begin{bmatrix} 1 \\ \theta \\ \vdots \\ \theta^{n-1} \end{bmatrix}, \tag{4.5}$$

with $\langle \mathbf{d}, \tilde{\mathbf{v}} \rangle \in R_\theta$ and $\langle \mathbf{d}, \tilde{\mathbf{v}} \rangle \neq 0$ because B^T has full rank and $\tilde{\mathbf{v}} \neq \mathbf{0}$. If, however, $\det(\mathsf{B}) = \pm 1$ then (4.5) says that $\mathfrak{a}(\tilde{\mathbf{v}})$ spans the same R_θ-module as the principal ideal $(\langle \mathbf{d}, \tilde{\mathbf{v}} \rangle)$. Thus A^T must be in the principal class.

For the other direction, suppose that A^T corresponds to the principal class. By Theorem 1.2 the matrix A is $\mathbb{Q}$-similar to some integer matrix $\tilde{\mathsf{A}}$ having a complete primitive digit set. However we have shown that $\tilde{\mathsf{A}}$ can't have a primitive digit set unless $\tilde{\mathsf{A}}^T$ corresponds to the principal class. Thus A^T must be $\mathbb{Z}$-similar to $\tilde{\mathsf{A}}^T$ since both correspond to the principal class. Thus A is $\mathbb{Z}$-similar to $\tilde{\mathsf{A}}$ so by Theorem 1.2 it has a complete primitive digit set since $\tilde{\mathsf{A}}$ does. ∎

Remark. A monic polynomial $f(x)$ has the associated *companion matrix* C_f whose last row entries are the coefficients of $f(x)$. The matrix C_f has right eigenvector $(1, \theta, ..., \theta^{n-1})^T$ with eigenvalue θ, and corresponds to the principal class of R_θ. The matrix C_f clearly has the primitive digit set $\{\mathbf{0}, \mathbf{e}_n\}$ where $\mathbf{e}_n = (0, ..., 0, 1)^T$, since $\mathsf{C}_f^i\mathbf{e}_n = \mathbf{e}_{n-i}$ for $1 \leqslant i \leqslant n-1$. Consequently Theorem 4.1 shows that C_f^T corresponds to the principal class. It then follows from the Lattimer–MacDuffee theorem that C_f^T is $\mathbb{Z}$-similar to C_f. This gives a rather indirect proof of this well-known fact, cf. Taussky [20].

Proof of Theorem 1.4. This follows immediately from Theorem 4.1. In particular, if the ring R_θ has class number greater than 1, then a representative of a nonprincipal class under the Lattimer-MacDuffee correspondence gives a matrix A with characteristic polynomial $f(\mathbf{x})$ which has no digit set $\mathscr{D} = \{\mathbf{d}_1, \mathbf{d}_2\} \subseteq \mathbb{Z}^n$ with $\mathbb{Z}[\mathsf{A}, \mathscr{D}] = \mathbb{Z}^n$.

There are two-dimensional examples with non-expanding $f_{\mathsf{A}}(x)$ having class number greater than one. For $f(x) = x^2 - ax - 2$ with $a \geqslant 0$, the smallest value of a where this happens is $a = 11$. Then $\theta = (11 + \sqrt{129})/2$, and $\mathbb{Z}[1, (11 + \sqrt{129})/2]$ is the full ring of integers of $\mathbb{Q}(\sqrt{129})$, which has class number 2. The matrix $\left[\begin{smallmatrix} 17 & -10 \\ 10 & -6 \end{smallmatrix}\right]$ represents the nonprincipal class. We can check directly that no basis $\{\mathbf{0}, \mathbf{d}\}$ works, for if $\mathbf{d} = (x, y)^T$ then the matrix B in (4.4) is

$$\mathsf{B} = \begin{bmatrix} x & 17x - 10y \\ y & 10x - 6y \end{bmatrix}$$

so $\det(\mathsf{B}) = 10x^2 - 23xy + 10y^2$, and this quadratic form does not integrally represent 1 or -1.

Proof of Corollary 1.4. The class number h_n of the field $K = \mathbb{Q}(\sqrt[n]{2})$ is by definition the number of elements in the class group of the ring of integers O_K of K. Now O_K contains the subring $R = \mathbb{Z}[1, \theta, \theta^2, ..., \theta^{n-1}]$, where $\theta = \sqrt[n]{2}$, and it is well known that the class number h_n of O_K divides the class number h_R of the subring R. Thus if $h_n > 1$, then $h_R > 1$ and the result follows from Theorem 1.4. ∎

5. Primitive Complete Digit Sets: Dimensions 2 and 3

We will show that in dimensions 2 and 3 all expanding integer matrices have a primitive complete digit set.

Recall that the expanding property of a matrix A is a property of its characteristic polynomial, and we call a monic polynomial $f(x) \in \mathbb{Z}[x]$ *expanding* if all its roots $|\lambda_i| > 1$.

Lemma 5.1. (i) *For any positive integers m and n, there are finitely many expanding polynomials $f(x) \in \mathbb{Z}[x]$ of degree n having $|f(0)| = m$.*

(ii) *If in addition m is a prime p, then there are finitely many $\mathbb{Z}$-similarity classes of expanding matrices $\mathsf{A} \in M_n(\mathbb{Z})$ having $|\det(\mathsf{A})| = p$.*

Proof. (i) Let

$$f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i,$$

TABLE 5.1

Expanding Polynomials: Degree 2, $|f(0)| = 2$

$f(x)$	Roots	Polynomial discriminant
$x^2 - 2$	$\pm\sqrt{2}$	8
$x^2 + 2$	$\pm i\sqrt{2}$	-8
$x^2 - x + 2$	$\frac{1}{2}(1 \pm i\sqrt{7})$	-7
$x^2 - 2x + 2$	$1 \pm i$	-4

then $a_0 = \pm m$, and the expanding property implies that all roots $|\theta_i| \leqslant m$, whence

$$|a_i| \leqslant \binom{n}{i} m^i, \qquad 1 \leqslant i \leqslant n-1.$$

(ii) Any expanding polynomial with $|f(0)| = p$ must be irreducible over $\mathbb{Q}$. Otherwise $f(x) = f_1(x) f_2(x)$ implies $|f(0)| = |f_1(0)|\,|f_2(0)|$, and each $|f_i(0)| > 1$ since they are also expanding, which contradicts $|f(0)|$ being prime. Combining (i) with the Lattimer–MacDuffee theorem gives the finiteness result. ∎

Proof of Theorem 1.5. Theorem 1.3 proves the result in dimension 1, and also covers all cases where $|\det(\mathsf{A})| \geqslant 3$ in dimension 2, and where $|\det(\mathsf{A})| \geqslant 4$ in dimension 3. By Lemma 5.1 there are only a finite set of $\mathbb{Z}$-similarity classes of expanding matrices with $|\det(\mathsf{A})| = 2$ in dimension 2 and $|\det(\mathsf{A})| = 2$ or 3 in dimension 3. To complete the proof it suffices to enumerate them and to exhibit a primitive complete digit set for each one.

TABLE 5.2

Expanding Polynomials: Degree 3, $f(0) = 2$

$f(x) = x^3 + ax^2 + bx + 2$ (a, b)	Real root	Polynomial discriminant
$(2, 2)$	-1.544	-44
$(1, 1)$	-1.353	-83
$(1, 0)$	-1.696	-116
$(0, 0)$	-1.260	-108
$(0, -1)$	-1.521	-104
$(0, -2)$	-1.769	-76
$(-1, -1)$	-1.206	-83

TABLE 5.3

Expanding Polynomials: Degree 3, $f(0) = 3$

$f(x) = x^3 + ax^2 + bx + 3$ (a, b)	Real root	Polynomial discriminant
(4, 5)	−2.466	−31
(3, 4)	−1.682	−31
(3, 3)	−2.259	−108
(3, 2)	−2.672	−239
(2, 3)	−1.392	−87
(2, 2)	−1.810	−139
(2, 1)	−2.174	−231
(2, 0)	−2.485	−339
(2, −1)	−2.757	−439
(1, 2)	−1.275	−175
(1, 1)	−1.574	−204
(1, 0)	−1.863	−255
(1, −1)	−2.130	$-304 = -4.76$
(1, −2)	−2.374	−327
(1, −3)	−2.598	−300
(1, −4)	−2.806	−199
(0, 1)	−1.213	−247
(0, 0)	−1.442	−243
(0, −1)	−1.671	−239
(0, −2)	−0.893	−211
(0, −3)	−2.103	−135
(−1, 0)	−1.174	−231
(−1, −1)	−1.359	−172
(−1, −2)	−1.546	−87
(−2, 1)	−1.147	−31

To accomplish the enumeration, we first determine all allowable expanding polynomials $f(x)$. For dimension 2 these consist of all expanding polynomials with $|f(0)| = 2$, given in Table 5.1. For dimension 3 these consist of all expanding polynomials with $|f(0)| = 2$ or 3. We can reduce to the cases $f(0) = 2$ or 3 because those with $f(0) = -2$ or -3 are exactly $\tilde{f}(x) := -f(-x)$. The complete lists are given in Tables 5.2 and 5.3, respectively.

As an illustration of the computation, consider the case

$$f(x) = x^3 + ax^2 + bx + 3.$$

Since all roots $|\theta_i| < 3$, and $|\theta_1\theta_2\theta_3| = 3$, we have

$$|a| \leqslant |\theta_1| + |\theta_2| + |\theta_3| < 5$$
$$|b| \leqslant |\theta_1\theta_2| + |\theta_1\theta_3| + |\theta_2\theta_3| < 7.$$

A direct test of all cases yields Table 5.3. In fact, since $f(0) = 3$, if $f(-1) \leqslant 0$ then $f(x)$ has a real root in $[-1, 0]$, and if $f(1) \leqslant 0$ then it has a root in $[0, 1]$, and if $f(3) \leqslant 0$ then it has a real root in $[3, \infty)$, while if $f(-3) \geqslant 0$ then it has a real root in $(-\infty, -3]$. All these cases are excluded, and every remaining (a, b) pair is actually expanding. A similar result holds for the other two tables.

To enumerate $\mathbb{Z}$-similarity classes we use the Lattimer–MacDuffee theorem. For each ring $R_\theta = [1, \theta, ..., \theta^{n-1}]$ its discriminant is the discriminant of the polynomial $f(x)$, and Tables 5.1–5.3 give these values (computed using MACSYMA). In the $|\det(\mathsf{A})| = 2$ case for $n = 2$, 3 these match the discriminants of the full ring of integers of the corresponding fields $\mathbb{Q}(\theta)$; in the cubic field case this follows using the table in Delone and Faddeev [4], p. 160. Thus R_θ is the full ring of integers, and the needed class number is the class number of $\mathbb{Q}(\theta)$. In all cases this class number is 1, as is well known for the quadratic fields in Table 5.1, while for the cubic fields it follows from the tables in Delone and Faddeev [4], p. 141–146. Theorem 4.1 guarantees that complete primitive digit sets exist in these cases.

In the case $n = 3$ and $|\det(\mathsf{A})| = 3$, the polynomial discriminants reveal that R_θ is the full ring of integers for the corresponding cubic field, with the single exception $f(x) = x^3 + x^2 - x + 3$, which has discriminant $-304 = -4.76$; and R_θ is then of index 2 in the full ring of integers O_K of the cubic field K of discriminant -76. In all cases where the full ring of integers occurs, the class number is 1 using either the tables of Delone and Faddeev [4] or the (unpublished) table of Angell [1] for $d = -199$, -339, -439. In the remaining case $f(x) = x^3 + x^2 - x + 3$, the ring of integers O_K has class number 1. Furthermore its subring R_θ also has class number 1, since there is a unit $\varepsilon_K = \frac{1}{2}(1 + \theta^2)$ of O_K that lies in the nontrivial coset of $O_K/R_\theta \cong \mathbb{Z}/2\mathbb{Z}$, so that every principal ideal in O_K can be generated by an element in R_θ. Consequently every such $\mathbb{Z}$-similarity class contains a representative matrix A that is a companion matrix. It then suffices to take $\mathscr{D} = \{\mathbf{0}, \mathbf{d}_1, \mathbf{d}_2\}$ where $\mathbf{d}_1 = (0, 0, 1)^T$ and $\mathbf{d}_2$ is any digit in the remaining equivalence class of $\mathbb{Z}^3/\mathsf{A}(\mathbb{Z}^3)$. ∎

References

1. I. O. Angell, A table of complex Cubic Fields, *Bull. Lond. Math. Soc.* **5** (1973), 37–38.
2. C. Bandt, Self-similar sets 5. Integer matrices and fractal tilings of $\mathbb{R}^n$, *Proc. Amer. Math Soc.* **112** (1991), 549–562.

3. I. Daubechies, "Ten Lectures on Wavelets," CBMS Volume 61, SIAM, Philadelphia, 1992.
4. B. N. Delone and D. K. Faddeev, "The Theory of Irrationalities of the Third Degree," Amer. Math. Soc. Providence, RI, 1964.
5. J. Graf von Schmettow, KANT—a tool for computations in algebraic number fields, *in* "Computational Number Theory" (A. Pethö, M. E. Pohst, H. C. Williams, and H. G. Zimmer, Eds.), pp. 291–330, de Gruyter, Berlin, 1991.
6. K. Gröchenig and A. Haas, Self-Similar Lattice Tilings, *J. Fourier Analysis Appl.* **1** (1994), 131–170.
7. K. Gröchenig and W. Madych, Multiresolution analysis, Haar bases, and self-similar tilings, *IEEE Trans. Inform. Theory* **38** (1992), 556–568.
8. A. Haar, Zur Theorie der orthogonalen Funktionen-Systeme, *Math. Ann.* **69** (1910), 331–371.
9. R. Kenyon, Self-replicating tilings, *in* "Symbolic Dynamics and Its Applications" (P. Walters, Ed.), Contemporary Math., Vol. 135, pp. 239–264, 1992.
10. J. C. Lagarias and Y. Wang, Self-affine tiles in $\mathbb{R}^n$, *Adv. Math.*, to appear.
11. J. C. Lagarias and Y. Wang, Integral self-affine tiles in $\mathbb{R}^n$ I. Standard and nonstandard digit sets, *J. London Math. Soc.*, to appear.
12. J. C. Lagarias and Y. Wang, Integral self-affine tiles in $\mathbb{R}^n$ II. Lattice tilings, preprint, 1994.
13. J. C. Lagarias and Y. Wang, Haar-type wavelet bases in $\mathbb{R}^2$, *J. Fourier Analysis Appl.* **2** (1995), 1–14.
14. P. G. Lemarié, La propriété de support minimal dans les analyses multirésolution, *C.R. Acad. Sci Paris* **312** (1991), 773–776.
15. S. Mallat, Multiresolution approximation and wavelet orthogonal bases of $L^2(\mathbb{R})$, *Trans. Amer. Math. Soc.* **315** (1989), 69–87.
16. Y. Meyer, Ondelettes, fonctions splines et analyses graduées, Cahiers Math. de la Decision 8703, Ceremade, 1986.
17. M. Newman, "Integral Matrices," Academic Press, New York, 1972.
18. A. M. Odlyzko, Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results, *Sem. Theorie Nombres, Bordeaux* **2** (1991), 119–141.
19. R. S. Strichartz, Wavelets and self-affine tilings, *Construct. Approx.* **9** (1983), 327–346.
20. O. Taussky, On matrix classes corresponding to an ideal and its inverse, *Illinois J. Math.* **1** (1957), 108–113.