Journal of Number Theory **76**, 330–336 (1999)
Article ID jnth.1998.2353, available online at http://www.idealibrary.com on IDEAL®

CORRIGENDUM/ADDENDUM

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

Jeffrey C. Lagarias

AT&T Labs, Florham Park, New Jersey 07932

and

Yang Wang

Georgia Institute of Technology, Atlanta, Georgia 30332

Communicated by Alan C. Woods

Received June 16, 1998

We correct an error in the proof of Theorem 1.5 in Lagarias and Wang (*J. Number Theory* **57**, 1996, 181–197). We also give a strengthened necessary condition for the existence of a Haar basis of the specified kind for every integer matrix $\mathbf{A}$ that has a given irreducible characteristic polynomial $f(x)$ with $|f(0)|=2$. A. Potiopa (Master's thesis, Siedlce University, 1997) found that the expanding polynomial $g(x)=x^4+x^2+2$ violates this necessary condition. Thus there exists a 4×4 expanding integral matrix $\mathbf{A}$ of determinant 2 and characteristic polynomial $g(x)$ which has no Haar-type wavelet basis using an integer digit set $\mathscr{D}\subseteq\mathbb{Z}^4$. © 1999 Academic Press

Key Words: Haar bases; ideal class semigroup; integer matrices.

1. INTRODUCTION

Our paper [4] studied the problem of whether every expanding $n\times n$ integer matrix $\mathbf{A}$ has a digit set $\mathscr{D}\subseteq\mathbb{Z}^n$ such that the pair $(\mathbf{A}, \mathscr{D})$ gives a Haar-type wavelet basis of $\mathbb{R}^n$. Theorem 1.5 of [4] asserted that this is always the case for $n\leqslant 3$. Recently J. Browkin [1] brought to our attention an error in the proof of one case in this theorem. Here we correct the proof.

We also obtain a strengthened necessary condition for the existence of a Haar basis of the above kind. Using this improved necessary condition A. Potiopa [7] has shown that there exists a 4×4 expanding integral matrix with characteristic polynomial x^4+x^2+2 that has no Haar basis using an integral digit set $\mathscr{D}\subseteq\mathbb{Z}^4$. This shows that the result of [4] does not extend to all higher dimensions.

0022-314X/99 $30.00

2. CLASS NUMBERS AND THE LATTIMER–MACDUFFEE THEOREM

We recall the definition of the class number of a commutative integral domain R with unit, as in Pohst and Zassenhaus [6, p. 264] and Dade, Taussky and Zassenhaus [2]. A *fractional ideal* $\mathbf{a}$ of R is an R-module of the form vI, where I is an ideal of R and v is a nonzero element of its quotient field K. Two fractional ideals $\mathbf{a}_1$ and $\mathbf{a}_2$ are in the same *ideal class* if there exist $\alpha_1, \alpha_2 \in K \backslash \{0\}$ such that $\alpha_1 \mathbf{a}_1 = \alpha_2 \mathbf{a}_2$. We denote the class of $\mathbf{a}$ by $[\mathbf{a}]$. There is a multiplication defined on fractional ideals by

$$(v_1 I_1)(v_2 I_2) = v_1 v_2 I_1 I_2,$$

which yields a well-defined multiplication on ideal classes which makes it a semigroup with identity element the class $[R]$ of R. We call this semigroup the *class semigroup* $\mathscr{S}(R)$. An ideal class $[\mathbf{a}]$ is *strictly invertible*[1] if it has an inverse in this semigroup, i.e., there exists a class $[\mathbf{b}]$ such that $[\mathbf{a}][\mathbf{b}] = [R]$. We call the group $\mathrm{Cl}(R)$ of strictly invertible elements of $\mathscr{S}(R)$ the *invertible class group* of R. We define the *class number* $h(R)$ of R to be $|\mathscr{S}(R)|$ and the *invertible class number* $h^*(R)$ of R to be $|\mathrm{Cl}(R)|$. It is well-known that a commutative integral domain R with unit is a Dedekind domain if and only if every ideal class is strictly invertible, i.e., if and only if $\mathscr{S}(R) = \mathrm{Cl}(R)$, so that $h(R) = h^*(R)$. See [6, p. 269]. It follows that: If the class number of a commutative integral domain R with unit is 1, then R must be a Dedekind domain.

The Lattimer–Macduffee theorem [5, Sect. III.6] gives a one-to-one correspondence between the set of $\mathbb{Z}$-similarity classes of integral matrices $\mathbf{A}$ having a fixed characteristic polynomial $f(x)$ of degree n that is irreducible over $\mathbb{Q}$ and the set of ideal classes of the commutative integral domain

$$R_\theta := \mathbb{Z}[1, \theta, \theta^2, ..., \theta^{n-1}], \tag{2.1}$$

where θ is a root of $f(x) = 0$. The ring R_θ is an *order* of the quotient field $K = \mathbb{Q}(\theta)$, i.e., it is a subring of finite index in the ring O_K of algebraic integers of K which contains 1. It is well known that an order R of an algebraic number field K is a Dedekind domain if and only if $R = O_K$, because a Dedekind domain is integrally closed in its quotient field [6, p. 269]. Therefore we have:

[1] This definition of invertibility is narrower than the definition used in Dade, Taussky, and Zassenhaus [2]. We require strictly invertible ideal classes $[\mathbf{a}]$ to consist of ideals $\mathbf{a}$ that are invertible in the sense of [2] and have the associated order $\mathrm{ord}(\mathbf{a}) := [\mathbf{a} : \mathbf{a}] = R$. Thus $\mathrm{Cl}(R)$ is the group $\mathrm{G}([R])$ in Prop. 1.2.10 of [2].

CLASS NUMBER ONE CRITERION. *If R_θ has class number $h(R_\theta)=1$, then R_θ is the full ring of integers in $K=\mathbb{Q}(\theta)$.*

We apply this criterion to obtain a necessary condition for the existence of Haar bases of the form $(\mathbf{A}, \mathscr{D})$, where $\mathscr{D}$ is an integral digit set. Recall from [4] that a necessary condition that $(\mathbf{A}, \mathscr{D})$ with $\mathscr{D} \subseteq \mathbb{Z}^n$ give a Haar basis is that $\mathscr{D}$ be a complete primitive digit set for $\mathbf{A}$, i.e., a digit set $\mathscr{D}$ that is a complete set of coset representatives of $\mathbb{Z}^n/\mathbf{A}(\mathbb{Z}^n)$ and which has $\mathbb{Z}^n = \mathbb{Z}[\mathscr{D}, \mathbf{A}(\mathscr{D}), \mathbf{A}^2(\mathscr{D}), ...]$.

COMPLETE PRIMITIVE DIGIT SET CRITERION. *Let $f(x) \in \mathbb{Z}(x)$ be an irreducible monic polynomial with $|f(0)|=2$, and let θ denote a root of $f(x)$. Suppose that for each integer matrix $\mathbf{A}$ with characteristic polynomial $f(x)$ there exists some complete primitive digit set. Then R_θ must be the full ring O_K of algebraic integers of $K=\mathbb{Q}(\theta)$, and the class number $h_K := h(O_K)=1$.*

Proof. This follows directly from Theorem 1.4 of [4, p. 184] together with the class number one criterion above. ∎

The complete primitive digit set criterion can be applied to show that Theorem 1.5 of [4] does not generalize to dimension 4 and various higher dimensions. A. Potiopa [7] found the expanding polynomial

$$f(x) = x^4 + x^2 + 2,$$

for which the ring R_θ has index 2 in the full ring of integers of $K=\mathbb{Q}(\theta)$. By the class number one criterion above, R_θ does not have class number 1, hence by the complete primitive digit set criterion there exists a 4×4 integral matrix $\mathbf{A}$ for which there is no digit set $\mathscr{D} \subseteq \mathbb{Z}^4$ such that the pair $(\mathbf{A}, \mathscr{D})$ gives a Haar-type wavelet basis of $\mathbb{R}^4$. To give an explicit example, we note that in terms of a root θ of the polynomial x^4+x^2+2 the ring of integers O_K of $K=\mathbb{Q}(\theta)$ is $\mathbb{Z}[1, \theta, \theta^2, \frac{1}{2}(\theta^2+\theta^3)]$, and the action of multiplication by θ on this basis (taken as column vectors) gives the integral matrix

$$\mathbf{A} := \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 2 \\ -1 & 0 & -1 & 1 \end{bmatrix}.$$

This matrix has the desired property by Theorem 1.4 of [4], since the ideal class $[O_K]$ is not the unit class in the ideal class semigroup $\mathscr{S}(R_\theta)$. A. Potiopa [7] also observed that there are no examples of expanding polynomials $f(x) \in \mathbb{Z}[x]$ of degree 5, with $f(0) = \pm 2$ and with R_θ not the full ring of integers of $\mathbb{Q}(\theta)$, and that there are exactly four such polynomials of degree 6, All of the quotient fields K from these expanding polynomials had a maximal order O_K with class number 1. Denoting the index $k = [O_K : R_\theta]$, the four polynomials of degree 6 are

$$x^6 - x^4 - x^2 + 2, \qquad k = 4,$$

$$x^6 + x^3 + x^2 - x + 2, \qquad k = 2,$$

$$x^6 + x^4 + 2, \qquad k = 2,$$

$$x^6 + x^5 + x^4 + 2x^3 + x^2 + x + 2, \qquad k = 3.$$

Another example where the complete primitive digit set criterion rules out the existence of Haar bases $(\mathbf{A}, \mathscr{D})$ as above is the polynomial $f(x) = x^n - 2$, with $n = 1093$ or 3511. In this case F. Hess [3] has observed that R_θ is not the full ring of integers of $\mathbb{Q}(2^{1/n})$, using the fact than $2^n \equiv 1 \pmod{n^2}$ in these two cases.

The observations made above lead to the following corrections to [4].

(1) To verify the assertions made for the case $\theta = 2^{1/n}$ described on [4, p. 185], one must check that R_θ is the full ring of algebraic integers of $\mathbb{Q}(2^{1/n})$ for $2 \leqslant n \leqslant 30$. This was done by F. Hess [3], who has verified by computations using KANT that R_θ is the full ring of integers for $2 \leqslant n \leqslant 1092$, but not for 1093 or 3511. We note that the open question raised in [4, p. 185] about the class number of the full ring of integers of $\mathbb{Q}(2^{1/n})$ remains unresolved.

(2) The proof of Corollary 1.4 requires the extra observation that the semigroup homomorphism $\mathscr{S}(R_\theta) \to \mathrm{Cl}(O_K)$ induced from the map $I \to I' := O_K I$ is surjective. This is immediate, since each O_K-ideal is an R_θ-ideal. Actually Corollary 2.1.11 of Dade, Taussky and Zassenhaus [2] states that this map restricted to the domain $\mathrm{Cl}(R_\theta)$ of strictly invertible ideal classes is surjective.

(3) The proof of Theorem 1.5 on [4, p. 196] for the case $f(x) = x^3 + x^2 - x + 3$ requires modification. In this case the order R_θ has index 2 in the maximal order O_K, hence the class number of R_θ is larger than 1. In Section 3 we supply a corrected proof that a complete primitive digit set always exists.

We also note the following misprints in the tables in [4]: In Table 5.2 the last entry $(a, b) = (-1, -1)$ has discriminant -59, not -83. In Table 5.3 the last entry should have $(a, b) = (-2, -1)$, not $(-2, 1)$.

3. PROOF OF THEOREM 1.5

The proof in [4] is correct when $|\det(\mathbf{A})|>3$ and in the remaining cases of determinant 2 or 3 where the associated order R_θ is the full ring of integers of $K=\mathbb{Q}(\theta)$, since it happens that $h(R_\theta)=h^*(O_K)=h_K=1$ in all those cases, and Theorem 1.4 of [4] applies. There remains one exceptional case, which consists of integral 3×3 matrices $\mathbf{A}$ which have characteristic polynomial $f(x)=x^3+x^2-x+3$. This polynomial has discriminant $-304=-4.76$ and R_θ is of index 2 in the maximal order O_K of the cubic field K of discriminant -76. The class number $h_K=1$, so all O_K-ideals are principal. The unit group of O_K is of rank 1 with fundamental unit $\varepsilon=\frac{1}{2}(\theta^2+1)$ and torsion group $\{-1, 1\}$. The maximal order $O_K=\mathbb{Z}[1, \theta, \varepsilon]$ as a $\mathbb{Z}$-module.

We claim that the class number $h(R_\theta)=2$, and that

$$\mathscr{S}(R_\theta)=\{[R_\theta], [O_K]\}. \tag{3.1}$$

It is easy to see that the multiplication table of this semigroup is as follows:

	$[R_\theta]$	$[O_K]$
$[R_\theta]$	$[R_\theta]$	$[O_K]$
$[O_K]$	$[O_K]$	$[O_K]$

We do not use the multiplication table in the sequel.

To prove the claim, let $\mathbf{a}$ be an integral R_θ-ideal, i.e., $\mathbf{a}\subseteq R_\theta$, and consider the O_K-ideal $\mathbf{a}'=\mathbf{a}O_K$. It is a principal ideal $\mathbf{a}'=\alpha O_K$, and since $\mathbf{a}\subseteq O_K$ each element of $\mathbf{a}$ is divisible by α. By dividing by α we obtain the R_θ-ideal $\mathbf{b}=(1/\alpha)\,\mathbf{a}$ with $[\mathbf{b}]=[\mathbf{a}]$ and $\mathbf{b}$ has the properties that $\mathbf{b}\subseteq O_K$ and $\mathbf{b}O_K=O_K$. We will show that $\mathbf{b}=R_\theta$ or O_K or S, where $S=\mathbb{Z}[\varepsilon, 1+\theta+\varepsilon, -1+\theta]$, and that $S=\varepsilon R_\theta$, so that $[R_\theta]=[S]$. If so, then the claim follows, because $[R_\theta]$ and $[O_K]$ are distinct classes. (Indeed any ideal in the same class as O_K is an O_K-ideal, while R_θ is not.)

To classify all such $\mathbf{b}$, we note first that $2O_K\subset R_\theta$, because R_θ is a $\mathbb{Z}$-submodule of O_K of index 2, and all such submodules contain $2O_K$, which is a $\mathbb{Z}$-submodule of O_K of index 8. Thus

$$2O_K=2(\mathbf{b}O_K)=\mathbf{b}(2O_K)\subseteq \mathbf{b}R_\theta=\mathbf{b}\subseteq O_K,$$

so that $\mathbf{b}$ is a union of some of the eight cosets of $2O_K$ in O_K. These cosets always include the zero coset, and the index $[O_K:\mathbf{b}]$ is a power of 2. An arbitrary element of O_K can be written

$$a+b\theta+c\varepsilon, \qquad \text{with} \quad a, b, c\in\mathbb{Z}.$$

The eight cosets of $O_K/2O_K$ are described by (a, b, c) (mod 2). In terms of cosets, we have

$$R_\theta = \{(0, 1, 0), (1, 0, 0), (1, 1, 0), (0, 0, 0)\}.$$

To compute multiplication on cosets, a calculation gives

$$(a + b\theta + c\varepsilon)(m + n\theta + p\varepsilon) = am - bn - bp - cn + (an + bm + bp + cn - cp)\,\theta$$
$$+ (ap + 2bn - bp + cm - cn + 2cp)\,\varepsilon.$$

Since $2O_K$ is closed under multiplication by O_K, it cannot be one of the ideals $\mathbf{b}$, hence any $\mathbf{b}$ contains at least one nonzero coset. The smallest R_θ-module generated by either of the cosets $(0, 1, 0)$ and $(1, 0, 0)$ is R_θ, which is an admissible $\mathbf{b}$. The smallest R_θ-module generated by the coset $(1, 1, 0)$ is $\{(1, 1, 0), (0, 0, 0)\}$. This is also an O_K-ideal, hence it cannot be any $\mathbf{b}$. Thus any candidate $\mathbf{b}$ that contains these two cosets must contain another coset, and hence be of index at most 2 in O_K. Next $(0, 0, 1)$ and $(1, 1, 1)$ each generate the R_θ-ideal

$$S := \{(0, 0, 1), (1, 1, 1), (1, 1, 0), (0, 0, 0)\},$$

and $SO_K = O_K$, so this is an admissible $\mathbf{b}$. The values $(1, 0, 1)$ and $(0, 1, 1)$ each generate the R_θ-ideal $\{(1, 0, 1), (0, 1, 1), (1, 1, 0), (0, 0, 0)\}$, but this ideal is also an O_K-ideal hence we do not obtain an admissible $\mathbf{b}$. All these R_θ-ideals are of index 2 in O_K. Thus any remaining candidates for $\mathbf{b}$ must have index smaller than 2, and this yields O_K, which completes the list of $\mathbf{b}$. The multiplication rule above allows one to check that $S = \varepsilon R_\theta$. Thus (3.1) holds.

We choose bases of the two $\mathbb{Z}$-modules $\mathbf{b}$ as follows:

$$R_\theta = \mathbb{Z}[1, \theta, \theta^2]$$

and

$$O_K = \mathbb{Z}[1, \theta, \tfrac{1}{2} + \tfrac{1}{2}\theta^2].$$

Matrix representatives of the two classes (representing multiplication by θ on these bases viewed as column vectors) are given by

$$\mathbf{A}_1 := \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -3 & 1 & -1 \end{bmatrix} \quad \text{and} \quad \mathbf{A}_2 := \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 2 \\ -1 & 1 & -1 \end{bmatrix}.$$

The principal class $\mathbf{A}_1$, because it is strictly invertible, necessarily has a primitive complete digit set. The class $\mathbf{A}_2$ is not strictly invertible, and has the primitive complete digit set

$$\mathscr{D} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}.$$

To see this, note that

$$\mathbf{A}_2(\mathbb{Z}^3) = \left\{ \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} : m_1 + m_2 - m_3 \equiv 0 \pmod 3 \right\}.$$

Hence $\mathscr{D}$ consists of all three residue classes (mod 3) so is complete. It is straightforward to verify that it is primitive. ∎

ACKNOWLEDGMENT

We are indebted to J. Browkin for a careful reading of this corrigendum, which uncovered yet another gap in an argument which we have now filled, and for other helpful comments.

REFERENCES

1. J. Browkin, private communication.
2. E. C. Dade, O. Taussky, and H. Zassenhaus, On the theory of orders, in particular on the semigroup of ideal classes and genera of an order of an algebraic number field, *Math. Ann.* **148** (1962), 31–64.
3. F. Hess, private communication.
4. J. C. Lagarias and Y. Wang, Haar bases for $L^2(\mathbb{R}^n)$ and algebraic number theory, *J. Number Theory* **57** (1996), 181–197.
5. M. Newman, "Integral Matrices," Academic Press, New York, 1972.
6. M. Pohst and H. Zassenhaus, "Algorithmic Algebraic Number Theory," Cambridge Univ. Press, Cambridge, UK, 1989.
7. A. Potiopa, "A Problem of Lagarias and Wang," Master's thesis, Siedlce University, Siedce, Poland, June 1997. [in Polish]