IJMMS 2003:15, 935–946
PII. S0161171203203124
http://ijmms.hindawi.com
© Hindawi Publishing Corp.

ON THE STRUCTURE OF MULTIPLIERS OF $\mathbb{Z}^2$

EDGAR MARTÍNEZ-MORO and ROBERTO CANOGAR-MCKENZIE

Received 14 March 2002

We show the combinatorial structure of $\mathbb{Z}^2$ modulo sublattices similar to $\mathbb{Z}^2$. The tool we use for dealing with this purpose is the notion of association scheme. We classify when the scheme defined by the lattice is imprimitive and characterize its decomposition in terms of the decomposition of the Gaussian integer defining the lattice. This arises in the classification of different forms of tiling $\mathbb{Z}^2$ by lattices of this type. The main application of these structures is that they are closely related to two-dimensional signal constellations with a Mannheim metric in the coding theory.

2000 Mathematics Subject Classification: 05E20, 11Z05.

1. Introduction. A *similarity* σ of a *norm* c is a map from $\mathbb{R}^n$ to $\mathbb{R}^n$ such that $\sigma u \cdot \sigma v = cu \cdot v$, $u,v \in \mathbb{R}^n$. Let Λ be a two-dimensional lattice, then a sublattice $\Lambda' \subseteq \Lambda$ is *similar* to Λ if $\sigma(\Lambda) = \Lambda'$. The map σ is also called a *multiplier* of the norm c for Λ. We consider now the lattice $\Lambda = \mathbb{Z}[i] \cong \mathbb{Z}^2$ of the Gaussian integers; it is a known result [5] that the lattice $\mathbb{Z}^2$ has multipliers of norm c if and only if $c = r^2 + s^2$, $r,s \in \mathbb{Z}$.

In this paper, we study the combinatorial structure of sublattices similar to $\mathbb{Z}[i]$ given by $(r+si)\mathbb{Z}[i]$ by studying the quotient $\mathbb{Z}[i]/(r+si)\mathbb{Z}[i]$. From now on, this lattice is denoted by $\mathbb{Z}[i]_{(r+si)}$ for short. Sublattices similar to $\mathbb{Z}^2$ have been found useful for recursive constructions of lattices (see [5, 6]), and quotients of this lattices are used for coding two-dimensional signal constellations in the coding theory (see [10, 12]). We define an association scheme over the classes in the sublattice. This association scheme is defined by the orbitals of a transitive action (see [3] for a primer on these constructions). This approach is the same as defining the association scheme given by the Mannheim metric (see [12]) and it is well known in the coding theory (see [14, "An all-purpose construction"] or [4, 8]). This also arises to different ways of tiling $\mathbb{Z}^2$ according to the Gaussian integer we have chosen.

The organization of the paper is as follows. In Section 2, we state some of the algebraic preliminaries underlying the paper and also develop a general setting for dealing with schemes derived from quotient lattices. Section 3 shows the construction of the scheme and some of its properties such as the expression of relation matrices. Sections 4 and 5 are devoted to the concept of quotient schemes and its relation with tiling the lattice $\mathbb{Z}^2$.

2. Preliminaries on association schemes

Definition 2.1. Let X be a finite set. A d-class association scheme is a pair $(X,(R_i)_{i\in I})$, where $I:=\{0,1,\dots,d\}$, such that

(1) $(R_i)_{i\in I}$ is a partition of $X\times X$,

(2) for all $i\in I$, there exists $j\in I$ such that $R_i^t:=\{(y,x)\mid(x,y)\in R_i\}=R_j$,

(3) $R_0:=\{(x,x)\mid x\in X\}$,

(4) there are numbers p_{ij}^k such that for any pair $(x,y)\in R_k$, the number of $z\in X$ with $(x,z)\in R_i$ and $(z,y)\in R_j$ equals p_{ij}^k,

(5) $p_{ij}^k=p_{ji}^k$ for all $i,j,k\in I$.

Definition 2.2. (i) The association scheme is *symmetric* if $R_i=R_i^t$ for all $i\in I$.

(ii) Let $\Gamma_i=(X,R_i)$ be the graph whose vertex and edge sets are X and R_i, respectively. An association scheme $(X,(R_i)_{i\in I})$ is said to be *primitive* if all the Γ_i, $i\in I$, are connected. It is said to be imprimitive if it is not primitive.

A more convenient way to describe association schemes is in terms of adjacency matrices. From now on, we suppose that X has n-ordered elements: $X=\{x_1,\dots,x_n\}$. If we have an association scheme $(X,(R_i)_{i\in I})$, the family $(A_i)_{i\in I}$ of nonzero $n\times n$ $(0,1)$-matrices will denote the adjacency matrices of the corresponding relations (the rows and columns of A_i and all matrices of size $n\times n$ on what follows are indexed by X in the specified order). Now, we can rewrite the following conditions in terms of matrices:

(1) $\sum_{i\in I}A_i=J$,

(2) for all $i\in I$, there exists $j\in I$ such that $A_i^t=A_j$,

(3) $A_0=I_n$,

(4) $A_iA_j=\sum_{k\in I}p_{ij}^kA_k$ $(i,j\in I)$,

(5) $A_iA_j=A_jA_i$.

By conditions (1) to (4), the set $\{A_i\}_{i\in I}$ is a base (as a vector space over $\mathbb{C}$) of a subalgebra in $M_n(\mathbb{C})$ (the set of $n\times n$ matrices over $\mathbb{C}$), so the algebra has a dimension $d+1$. By (5), this subalgebra is commutative. The algebra $\mathcal{A}$ is called the *Bose-Mesner* algebra of the association scheme.

In the following discussion, we need some notation on permutation groups acting on finite sets. For a reference on this topic, see [3]. For a given permutation group $\mathcal{G}$ of elements of a finite set X, we denote the orbit of an element $x\in X$ as $(\mathcal{G})(x)=\{xg\mid g\in\mathcal{G}\}$. Two orbits are either identical or disjoint. We denote by $\mathbb{O}(\mathcal{G}\mid X)$ the set of all the orbits of the action. We denote the stabilizers by $\mathcal{G}_x=\{g\in\mathcal{G}\mid x=xg\}$. The relation between orbits and stabilizers is well known and given by

$$\begin{aligned}(\mathcal{G})(x)&\longrightarrow\mathcal{G}/\mathcal{G}_x,\\ xg&\longmapsto\mathcal{G}_xg.\end{aligned}\tag{2.1}$$

The action is *transitive* if there is just one orbit. If the action is transitive, a *congruence* is a $\mathcal{G}$-invariant equivalence relation on X. We say that the action is *imprimitive* if it has a nontrivial equivalence.

We recall the following construction of association schemes later in the paper. Let X be a finite abelian group and let G be a subgroup of the automorphism group $\operatorname{Aut}(X)$ of X. Denoting the G-orbits in X by $X_0,\dots,X_d$, define the relations $R_0,\dots,R_d$ on X as follows:

$$R_i := \{(x,y)\in X^2 \mid y^{-1}x\in X_i\}, \tag{2.2}$$

then $(X,\{R_0,\dots,R_d\})$ is an association scheme.

3. Definition of the scheme. Consider the lattice of Gaussian integers $\mathbb{Z}[i]$ and the sublattice $L=\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$, the set of Gaussian integers modulo $\alpha\mathbb{Z}[i]$ which is similar to $\mathbb{Z}[i]$. The *norm* of an element $\alpha\in\mathbb{Z}[i]$ is just $N(\alpha)=\alpha\cdot\bar{\alpha}$. The *units* are the elements of norm 1. Clearly, multiplication in L by an element on the group of units of the Gaussian integers $\mathcal{G}=\langle i\rangle$ (i is the imaginary unit) is an isometry fixing the origin (from now on, we refer to them as *rotations*), and also we denote the group of *translations* by $\mathcal{T}$.

Consider now the *semidirect* product of both groups $\mathcal{H}=\mathcal{G}\ltimes\mathcal{T}$. Roughly speaking, we also denote by $\mathcal{H}$ the permutation group on L generated by the permutation $(\alpha\mapsto i\alpha)$ and the translations in $\mathcal{T}$. It is clear that $\mathcal{H}$ acts transitively on L.

Consider the orbits of the action

$$\mathcal{H}\times(L\times L)\longrightarrow(L\times L) \tag{3.1}$$

induced by the action of $\mathcal{H}$ on L. They are called *orbitals* and they are the relations of a symmetric association scheme [3]. Since $\mathcal{H}$ is a transitive permutation group, if we take $\mathcal{G}_0$ (i.e., those permutations that fix 0), it is well known that we have the coset decomposition $\mathcal{H}=(\mathcal{G}_0)(p_0)\cup\cdots\cup(\mathcal{G}_0)(p_d)$, where p_i is the permutation transforming 0 in some complex number β belonging to the coset. Therefore, orbits can be rewritten as

$$(x,y)\in R_k \Longleftrightarrow x-y\in\big((\mathcal{G}_0)(p_k)\big)(0). \tag{3.2}$$

In our case, $C_4\cong\mathcal{G}_0=\mathcal{G}$, the cyclic group of four elements.

Remark 3.1. Let Λ be a lattice, the *automorphism group of* Λ, $\operatorname{Aut}(\Lambda)$, is the set of distance-preserving transformations (or isometries) of the space that fix the origin and take the lattice to itself. Let $\operatorname{Aut}_\Lambda(\Lambda')$ denote the *automorphism group of* Λ' *with respect to* Λ, that is, the subgroup of $\operatorname{Aut}(\Lambda)$ containing the operations that preserve Λ'. Note that it is clear that C_4 is contained in $\operatorname{Aut}_{\mathbb{Z}^2}(\Lambda')$;

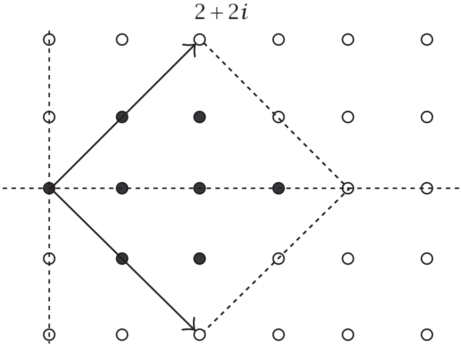

FIGURE 3.1. $\mathbb{Z}[i]_{(2+2i)}$.

moreover,

$$\operatorname{Aut}_{\mathbb{Z}[i]}\left((a+bi)\mathbb{Z}[i]\right) \cong \begin{cases} D_4 & \text{if } a=0, \text{ or } b=0, \text{ or } a=\pm b, \\ C_4 & \text{otherwise.} \end{cases} \tag{3.3}$$

EXAMPLE 3.2. Consider the sublattice $\mathbb{Z}[i]_{(2+2i)}$. We can give a system of representatives in the fundamental region given in Figure 3.1.

The orbitals of the previous action are given by the cosets (see (3.2))

$$\begin{aligned} X_0 &:= (\mathcal{G}_0)\cdot(0) = \{0\}, & X_1 &:= (\mathcal{G}_0)\cdot(1) = \{\pm 1, \pm i\}, \\ X_2 &:= (\mathcal{G}_0)\cdot(2) = \{2\}, & X_3 &:= (\mathcal{G}_0)\cdot(1+i) = \{1+i, 1-i\}, \end{aligned} \tag{3.4}$$

which allows us to construct the relations in the association scheme as $(x,y) \in R_i \Leftrightarrow x-y \in X_i$, $i = 0,1,2,3$.

THEOREM 3.3. *The association scheme $(X,(R_i)_{i\in I})$ with $X = L$ and $(R_i)_{i\in I}$ defined by the orbitals of the action above is primitive if and only if α is a prime in $\mathbb{Z}[i]$.*

PROOF. Suppose that α is not a prime in $\mathbb{Z}[i]$, that is, $\alpha = \alpha_1 \cdot \alpha_2$. Then, it is clear that the equivalence in L given by the quotient $L/[\mathbb{Z}[i]/\alpha_1\mathbb{Z}[i]] \subset L$ is $\mathcal{G}$-invariant, and therefore the action is imprimitive; hence by [2, Proposition 2.9.3], the association scheme is imprimitive.

Conversely, if α is prime, then it is a well-known fact in number theory (see [9]) that either it is $1+i$ multiplied by a unit or

(1) $N(\alpha) = p \equiv 1 \bmod 4$, p an odd prime, and in this case the lattice L has p points, and clearly $\mathcal{T} \cong \mathbb{Z}_p$,

(2) $\alpha = p \in \mathbb{Z}$ and $p \equiv 3 \bmod 4$; in this case L can be represented by $\mathbb{Z}_p[i]$ and therefore has p^2 points and $\mathcal{T} \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

In the case $1+i$, it is obvious that the scheme is primitive; in the other two cases, we have that the stabilizer of any point β in the lattice is given by the group of rotations around the point (i.e., $\mathcal{G}_\beta = t_\beta \mathcal{G}(t_\beta)^{-1}$, where t_β is the translation of vector β). It is clear that in both cases above, there is no group between $\mathcal{G}_\beta < \mathcal{H}$ since the group generated by a single element in $\mathcal{T}$ and the group $\mathcal{G}_\beta$ is $\mathcal{H}$ (see Remark 3.4 for a further explanation). Therefore, the stabilizer is maximal, and by [3, Theorem 1.9], the action is primitive and so is the association scheme. □

Remark 3.4. Indeed, it is easy to check that if $\mathcal{G}_\beta$ are the rotations around the point β and we add a new rotation, say i^j ($j = 1,2,3$), around, another point $\beta' \neq \beta$, then the composition of that one with the one given by i^{4-j} around β is a translation. So in the proof above, we can suppose that we always add one translation.

When there is a prime number of points, it is clear that a single translation generates the group $\mathcal{T}$ since it is cyclic of prime order. In the case $\mathcal{T} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, a translation t and the translation $i^{-1} \circ t \circ i$ are independent and generate the whole group $\mathcal{T}$. In Remark 3.5, we show the relation of this facts with the construction of constellations representing $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$, respectively.

The association scheme defined is a *translation asociation scheme*, and in the case of a prime number of points, $p \equiv 1 \bmod 4$ (i.e., $|X|$ is a prime) is a *cyclotomic* scheme (see [2] for the definitions).

Remark 3.5. The two constructions we present below are used to construct two-dimensional modulo metrics (in particular Mannheim distance) for the coding theory (for further details, see [10, 11, 12]).

(a) Let $\pi \in \mathbb{Z}[i]$ be an element whose norm is a prime integer p, and $p \equiv 1 \bmod 4$. It is well known (Fermat's two square theorem) that p can be written as

$$p = a^2 + b^2 = \pi\bar{\pi}, \quad \pi = a + ib \text{ (not unique)}. \tag{3.5}$$

If we denote by $\mathbb{Z}[i]_\pi$ the set of Gaussian integers modulo π, we define the modulo function $\nu : \mathbb{Z}[i] \to \mathbb{Z}[i]_\pi$ associating to each class in $\mathbb{Z}[i]_\pi$ its representant with a smallest norm:

$$\nu(\xi) = r, \quad \text{where } \xi = q\pi + r,\ \|r\| = \min\{\|\beta\| \mid \beta = \xi \bmod \pi\}. \tag{3.6}$$

This can be done because $\mathbb{Z}[i]$ is Euclidean domain. The quotient q can be calculated as $[\alpha\bar{\pi}/p]$, where $[x]$ denotes the Gaussian integer with real and imaginary part closest to x. The quotient q can be calculated as $[\alpha\bar{\pi}/p]$, where $[x]$ denotes the Gaussian integer with real and imaginary part closest to x.

Taking the carrier set of $\mathbb{F}_p$ as $\{0,1,\dots,p-1\} \subset \mathbb{Z}$, we can restrict to $\mathbb{F}_p$ the application ν so that it induces an isomorphism $\nu : \mathbb{F}_p \to \mathbb{Z}[i]_\pi$ given by

$$\text{for } g \in \mathbb{F}_p, \quad \nu(g) = g - \left[\frac{g\bar{\pi}}{p}\right]\pi. \tag{3.7}$$

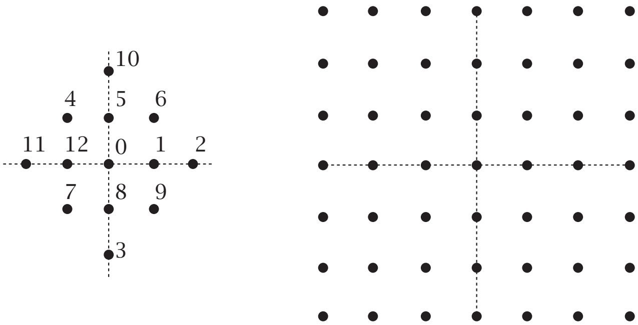

FIGURE 3.2. $\mathbb{F}_{13}$ as $\mathbb{Z}[i]_{3+2i}$ and $\mathbb{F}_{7^2}$ as $\mathbb{Z}_7[i]$.

So $\mathbb{F}_p$ and $\mathbb{Z}[i]_\pi$ are mathematically equivalent, and we use, from now on, that carrier set for a short notation.

(b) In the case $p \equiv 3 \bmod 4$, $\pi = p \in \mathbb{Z}$ and the isomorphism above does not give any relevant information over $\mathbb{F}_p$. For this type of primes, -1 is a quadratic nonresidue of p, hence we get the following isomorphism between $\mathbb{F}_{p^2}$ and $\mathbb{Z}_p[i]$ where

$$\mathbb{Z}_p[i] = \left\{k + il \mid k, l \in \left\{-\frac{(p-1)}{2}, \dots, -1, 0, 1, \dots, \frac{(p-1)}{2}\right\}\right\}. \tag{3.8}$$

EXAMPLE 3.6. Consider $\mathbb{Z}[i]_{3+2i}$ and $\mathbb{Z}_7[i]$, given by the carrier sets defined as in Remark 3.5. We have an alternative pictorial representation of them to a usual one derived as in Example 3.2 given by Figure 3.2. This representation is more suitable for showing the symmetries and rotations within the fundamental region. For the association scheme of this constellations of points, see Example 3.9.

REMARK 3.7. It is easy to check that the association schemes defined above are weakly metric (see [14] for a definition) for the Mannheim metric.

3.1. Matrix expression of the algebra. In this section, we develop an easy way for describing the matrices of the Bose-Mesner algebra associated with these sublattices in terms of circulant matrices.

DEFINITION 3.8. Let M be an $n \times n$ matrix and let $\{a_i\}_{i=0,\dots,n-1}$ be the first row of M. Then, M is *circulant* if

$$M_{ij} = a_{(i-j) \bmod n}, \quad i, j = 0, 1, \dots, n. \tag{3.9}$$

First, we insight in the case of a prime number of points p. In this case, we have that the translations $\mathcal{T}$ are a acyclic group of a prime order. Hence, if we choose an element generating $\langle t \rangle = \mathcal{T}$, any element $l \in L$ can be rewritten as

$l = t^j(0)$, $0 \le j \le p-1$, and choosing the order given by j for the points in the scheme, it is clear that the matrices R_i are circulant since t is an isometry.

Example 3.9. In the case $L = \mathbb{Z}[i]_{3+2i}$ of the previous example, the orbits can be described knowing the cosets

$$\begin{aligned} &(G_0)\cdot(p_0) = \{0\}, && (G_0)\cdot(p_1) = \{1,5,12,8\}, \\ &(G_0)\cdot(p_2) = \{6,4,7,9\}, && (G_0)\cdot(p_3) = \{2,10,11,3\}. \end{aligned} \tag{3.10}$$

And if we choose the translation given by adding 1 to each point for ordering the relations (the usual order for $\mathbb{F}_p$), then they are given by

$$\begin{aligned} &D_0 = [1,0,0,0,0,0,0,0,0,0,0,0,0], && D_1 = [0,1,0,0,0,1,0,0,1,0,0,0,1], \\ &D_2 = [0,0,0,0,1,0,1,1,0,1,0,0,0], && D_3 = [0,0,1,1,0,0,0,0,0,0,1,1,0]. \end{aligned} \tag{3.11}$$

Note that each matrix D is represented only by its first row since they are circulant. Moreover, as usual we collect all the information in a single matrix as

$$[0,1,3,3,2,1,2,2,1,2,3,3,1]. \tag{3.12}$$

Remark 3.10. For checking many properties of codes defined over association schemes, it is important to comput the eigenvalues associated with them (see [7, 14]). The eigenvalues of a circulant matrix are easily computed (see [1]) as sums of roots of the unit. Hence, so are the eigenvalues of the scheme (see [12]).

In the case of a nonprime number of points, we have a slightly modified construction based on the decomposition of $\mathcal{T}$ as the direct product of cyclic subgroups. The idea is the same as in Example 3.9, and now the matrices are circulant in blocks given by the acyclic subgroups. We illustrate this idea with an example.

Example 3.11. Consider $L = \mathbb{Z}[i]_{(2+2i)}$ as in Example 3.2. Consider the isomorphism given by

$$\begin{aligned} L = \mathbb{Z}[i]_{(2+2i)} &\xrightarrow{\sim} \mathbb{Z}_4 \times \mathbb{Z}_2 \\ 1 &\longmapsto (1,0) \\ 1+i &\longmapsto (0,1). \end{aligned} \tag{3.13}$$

Consider now the elements in the order given by

$$(0,0),(1,0),\dots,(3,0),(0,1),(1,1),\dots,(3,1). \tag{3.14}$$

The relation matrices can be expressed now as block-circulant matrices:

$$D_i = \begin{bmatrix} D_{i1} & D_{i2} \\ D_{i2} & D_{i1} \end{bmatrix}, \quad i = 0,\dots,3, \tag{3.15}$$

where each block is a circulant matrix. The relations in Example 3.2 can be represented in the same fashion as in the previous example

$$[0,1,2,1 \mid 3,1,3,1], \tag{3.16}$$

where | means the division of the blocks.

Remark 3.12. Suppose that we are given the sublattice $\mathbb{Z}[i]_{(r+si)}$. The problem above can be solved explicitly by reducing the generator matrix of the lattice

$$A = \begin{pmatrix} r & s \\ -s & r \end{pmatrix} \tag{3.17}$$

to its *Smith normal form*. Denote $d = \gcd(r,s)$; by Bezout's theorem, there are integers p, q such that $rp + sq = d$. If we consider

$$P := \begin{pmatrix} p & -q \\ \dfrac{s}{d} & \dfrac{r}{d} \end{pmatrix}, \qquad Q := \begin{pmatrix} 1 & \dfrac{(rq-sp)}{d} \\ 0 & 1 \end{pmatrix}. \tag{3.18}$$

Both P and Q are unimodular, and

$$S = PAQ = \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix}, \quad e = \frac{r^2+s^2}{d}. \tag{3.19}$$

Clearly, d divides e, and therefore S is the Smith normal form of A. Hence the abelian group $\mathbb{Z}[i]_{(r+si)}$ is isomorphic to $\mathbb{Z}_d \times \mathbb{Z}_e$.

Proposition 3.13. *The relation matrices can be expressed as block-circulant matrices, where each block is also a circulant matrix.*

Proof. It follows directly from the reasoning above, that is, the decomposition of the group of translations in a product of cyclic groups. □

4. Quotient schemes.

We introduce in this section the concept of a quotient scheme. For an account on this topic see [2]. Suppose a set of indices $\widetilde{0}$, and let us define the equivalence relation $\sim$ among the set of indices of the relations in the scheme $(X,\mathcal{R})$ as follows:

$$a \sim b \quad \text{if } p_{ab}^{i} \neq 0 \quad \text{for some } i \in \widetilde{0}. \tag{4.1}$$

As usual, $\widetilde{0}$ is the class of 0, and we write $\tilde{a}$ for the relation containing a.

Definition 4.1. We define a *quotient scheme* $(\tilde{X},\tilde{\mathcal{R}})$ of $(X,\mathcal{R})$ with respect to $\tilde{0}$ as the association scheme whose point set is the set $\tilde{X}$ of equivalence

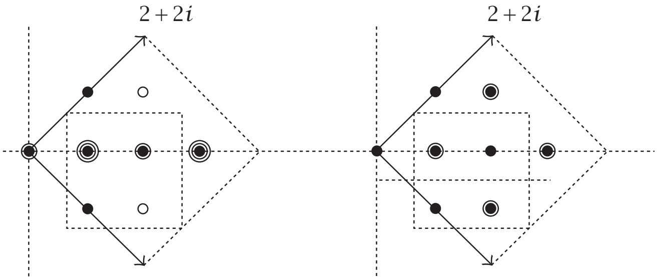

FIGURE 4.1. Quotients of $\mathbb{Z}[i]_{(2+2i)}$.

classes on X and whose relations are $\tilde{R}_{\tilde{i}}$, with

$$\tilde{R}_{\tilde{i}} = \{(\tilde{x},\tilde{y}) \mid \text{for } x \in \tilde{x},\ y \in \tilde{y}, (x,y) \in R_i \text{ with } i \in \tilde{i}\}. \tag{4.2}$$

PROPOSITION 4.2. *If the scheme defined on L is imprimitive, we can define a quotient scheme where $\tilde{0}$ is given by the classes of some of the elements divisors of* 0.

PROOF. It is obvious by the first part of the proof of Theorem 3.3. □

EXAMPLE 4.3. Consider $L = \mathbb{Z}[i]_{(2+2i)}$ as in Examples 3.2 and 3.11, and consider the relation given by $\tilde{0} = \{0,2\}$. With the notation in Example 3.11, we have

$$\begin{aligned} \widetilde{(0,0)} &= \{(0,0),(2,0)\}, & \widetilde{(1,0)} &= \{(1,0),(3,0)\}, \\ \widetilde{(0,1)} &= \{(0,1),(2,1)\}, & \widetilde{(1,1)} &= \{(1,1),(3,1)\}, \end{aligned} \tag{4.3}$$

and the relation matrix in the order given by $\widetilde{(0,0)}$, $\widetilde{(1,0)}$, $\widetilde{(0,1)}$, $\widetilde{(1,1)}$ is

$$[0,1,2,1]. \tag{4.4}$$

REMARK 4.4. Indeed, the previous example gives the translations by the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, this can be seen also because $2 = (1+i)(1-i)$ is not a Gaussian prime and admits a further quotient scheme given by

$$\widetilde{\widetilde{(0,0)}} = \{\widetilde{(0,0)},\widetilde{(0,1)}\}, \qquad \widetilde{\widetilde{(1,0)}} = \{\widetilde{(1,0)},\widetilde{(1,1)}\}. \tag{4.5}$$

This corresponds with the identifications in Figure 4.1.

REMARK 4.5. Note that following [2, page 52] if we let $A = \{a \mid p^0_{aa} = 1\}$, then for each $a \in A \setminus \{0\}$ we find an involution $\sigma_a : x \mapsto \bar{x}$, $(x,\bar{x}) \in R_a$, and if we set $\sigma_0 = 1$, then $\sigma_a\sigma_b = \sigma_b\sigma_a = \sigma_c$, where c is determined by $p^c_{ab} \neq 0$. Clearly, A has the structure of an elementary abelian 2-group.

Remark 4.6. There is a sort of Jordan-Hölder theory relating the facts above that for our example we can summarize the information in Figure 4.1 as follows:

$$\begin{array}{c} \mathbb{Z}[i]_{(2+2i)} \\ \cup \\ \mathbb{Z}[i]_{(2)} \\ \cup \\ \mathbb{Z}[i]_{(1+i)} \end{array} \tag{4.6}$$

$\mathbb{Z}[i]_{(\alpha)}$	$\mathcal{T}$	$\{a \mid p_{aa}^0 = 1\}$
$\mathbb{Z}[i]_{(2+2i)}$	$\mathbb{Z}_4 \times \mathbb{Z}_2$	$0,\ 2$
$\mathbb{Z}[i]_{(2)}$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\widetilde{(0,0)},\ \widetilde{(0,1)}$
$\mathbb{Z}[i]_{(1+i)}$	$\mathbb{Z}_2$	$\widetilde{\widetilde{(0,0)}}$

5. Relation with tilings. Up to now, we have shown that, we have three types of primitive sublattices, depending on the Gaussian prime defining it; this arises to three different forms of tiling the whole $\mathbb{Z}^2$:

(i) with tiles of type $\mathbb{Z}[i]_{(1+i)}$;

(ii) with tiles of type $\mathbb{Z}[i]_{(a+bi)}$ where $N(a+bi) = p$ an odd prime $\equiv 1 \bmod 4$;

(iii) with tiles of type $\mathbb{Z}_p[i]$; p an odd prime $\equiv 3 \bmod 4$.

Indeed, this has a close relationship with the well-known fact in the number theory given by the criterion for representing a number N by the sum of two squares, which says that any prime factor of N of the form $4k+3$ must divide N to an even power exactly. In our setting, this means (as we have seen) that the regions defined by an integer of norm p^n, p a prime of this type, must have p^{2n} points. This fact relates each prime in the factorization of the norm N with a type of the primitive tiles above.

In the last two cases above, the boundary of the Voronoi cell of the sublattice $\alpha\mathbb{Z}[i]$ does not contain any points of $\mathbb{Z}^2$, so following notation in [2], we called such sublattices *clean*. Also in the first two cases, we can find a complete set of representatives of the nonzero classes within the fundamental parallelotope defined by α and $i \cdot \alpha$.

Moreover, the boundary of the Voronoi cell is clean if there is an odd number of points [2], that is, there is no involution (see Remark 4.5), so the following corollary follows directly (as expected).

Corollary 5.1. *Any quotient of a clean sublattice L defined as in Section 3 is also clean.*

Remark 5.2. The primitive schemes above are the finest translation schemes from our setting. Recall that in the schemes defined for an odd prime, we have that in all cases all orbits are of size 4, but the schemes are not pseudocyclic (see [2] for a definition) since $\sum_i p_{ii}^k \neq 3$. We can go a bit farther with the following result of Rao et al. [2, page 52, (ii)] and [13]. They state that the finest translation association scheme for a set of odd order is pseudocyclic and the other translation schemes for the same set can be derived from this one by merging classes. In the case of the schemes in this paper, the scheme they recall is the one generated by the $1, i^2$ rotations and the translations, and clearly each relation of our scheme arises from the merging of two of its relations.

6. Conclusions. We have studied the combinatorial structure of the association schemes derived from the sublattices given by $\mathbb{Z}[i]/(r+si)\mathbb{Z}[i]$. As we have seen, there are close connections of this type of lattices with the coding theory, the recursive construction of lattices, and the self-similar lattices [2, 10, 11, 12]. In the study, the defined scheme plays a central role in the factorization of the Gaussian integer $(r+si)$ and also the factorization of the order of the group of translations $\mathcal{T}$ (i.e., the number of points in the sublattice). We have characterized the primitive cases and also identified the cases where the Voronoi cell is clean, both from a combinatorial point of view and from a number theoretical one. We can see the primitive case as the finest tiles of the lattice $\mathbb{Z}^2$, and they are useful in coding two-dimensional signal spaces with the Mannheim metric [10]. We have also shown how to derive an easy expression of the matrices defining the relations in the scheme based in their circulant structure. A similar study can be done with hexagonal schemes and hexagonal metrics based on Einsestein-Jacobi integers [12] and will be shown elsewhere. Future trends of investigation point toward classifying the partition designs derived from this type of association schemes.

References

[1] N. Biggs, *Algebraic Graph Theory*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1993.

[2] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 18, Springer-Verlag, Berlin, 1989.

[3] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.

[4] P. Camion, *Codes and association schemes: basic properties of association schemes relevant to coding*, Handbook of Coding Theory, Vol. I, II, North-Holland Publishing, Amsterdam, 1998, pp. 1441–1566.

[5] J. H. Conway, E. M. Rains, and N. J. A. Sloane, *On the existence of similar sublattices*, Canad. J. Math. **51** (1999), no. 6, 1300–1306.

[6] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren der Mathematischen Wissenschaften, vol. 290, Springer-Verlag, New York, 1999.

[7] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. (1973), no. 10, vi+97.

[8] P. Delsarte and V. I. Levenshtein, *Association schemes and coding theory*, IEEE Trans. Inform. Theory **44** (1998), no. 6, 2477–2504.

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

[10] K. Huber, *Codes over Gaussian integers*, IEEE Trans. Inform. Theory **40** (1994), no. 1, 207–216.

[11] ______, *The MacWilliams theorem for two-dimensional modulo metrics*, Appl. Algebra Engrg. Comm. Comput. **8** (1997), no. 1, 41–48.

[12] E. Martínez-Moro, F. J. Galán-Simón, M. A. Borges-Trenard, and M. Borges-Quintana, *Combinatorial structure of finite fields with two dimensional modulo metrics*, Cryptography and Coding (Cirencester, 1999), Lecture Notes in Computer Science, vol. 1746, Springer, Berlin, 1999, pp. 45–55.

[13] S. B. Rao, D. K. Ray-Chaudhuri, and N. M. Singhi, *On imprimitive association-schemes*, Combinatorics and Applications (Calcutta, 1982), Indian Statist. Inst., Calcutta, 1984, pp. 273–291.

[14] P. Solé, *On the parameters of codes for the Lee and modular distance*, Discrete Math. **89** (1991), no. 2, 185–194.

Edgar Martínez-Moro: Departamento de Matemática Aplicada Fundamental, Universidad de Valladolid, Valladolid, Spain
E-mail address: edgar.martinez@ieee.org

Roberto Canogar-Mckenzie: Departamento de Matemáticas, Universidad Nacional de Educación a Distancia (UNED), Madrid, Spain
E-mail address: rcanogar@mat.uned.es