On the Existence of Similar Sublattices

J. H. Conway
Mathematics Department
Princeton University
Princeton, NJ 08540

E. M. Rains and *N. J. A. Sloane*
Information Sciences Research
AT&T Shannon Lab
Florham Park, NJ 07932-0971

November 17, 1998; revised October 8, 1999. A slightly different version of this paper appeared in the *Canadian Jnl. Math.*, **51** (1999), pp. 1300–1306. Pdf version prepared May 7, 2000.

DEDICATED TO H. S. M. COXETER

ABSTRACT

Partial answers are given to two questions. When does a lattice Λ contain a sublattice Λ' of index N that is geometrically similar to Λ? When is the sublattice "clean", in the sense that the boundary of the Voronoi cells for Λ' do not intersect Λ?

1. Introduction

A *similarity* σ of norm c is a linear map from $\mathbb{R}^n$ to $\mathbb{R}^n$ such that $\sigma u \cdot \sigma v = c\ u \cdot v$ for $u, v \in \mathbb{R}^n$. Let Λ be an n-dimensional rational lattice, i.e. $u \cdot v \in \mathbb{Q}$ for $u, v \in \Lambda$. A sublattice $\Lambda' \subseteq \Lambda$ is *similar* to Λ if $\sigma(\Lambda) = \Lambda'$ for some similarity σ of norm c. We also call σ a *multiplier of norm* c for Λ. The index $N = [\Lambda : \Lambda']$ is $c^{n/2}$, so if n is odd c must be a square, say $c = a^2$, and we could take σ to be scalar multiplication by a. In other words the norms of similarities of odd-dimensional lattices are precisely the integral squares. Henceforth we will assume that $n = 2k$ is even.

Multipliers of small norm, especially 2 (also called "norm-doubling maps") are useful for recursive constructions of lattices ([10], Chap. 8). If the root lattice E_6 had a norm-doubling map σ, then the "u, $u+v$" construction[1] would produce a denser 12-dimensional lattice than the Coxeter-Todd lattice K_{12}. However, some years ago W. M. Kantor and N.J.A.S. showed by direct search that no such map exists. This result now follows from Theorem 2.

The question of the existence of multipliers of given norm arose recently in constructing "multiple description" vector quantizers [15, 17]. In an ordinary vector quantizer an n-dimensional lattice Λ is specified, and successive n-tuples $(x_1, \ldots, x_n) \in \mathbb{R}^n$ are replaced by the closest lattice points (cf. [10, Chapter 2]). In a multiple description scheme we also choose a number N and a labeling

$$u \in \Lambda \mapsto (l(u), r(u)) \in \mathbb{Z} \times \mathbb{Z}$$

such that $|l^{-1}(i) \cap r^{-1}(j)| \le 1$, $|l^{-1}(i)| \le N$, $|r^{-1}(j)| \le N$ for all $i, j \in \mathbb{Z}$. The numbers $l(u)$ and $r(u)$ are transmitted over different channels. If both numbers are received then u is uniquely determined, but if only one number is received (and the other lost) then u is determined to within a small region of $\mathbb{R}^n$ (and the goal is to choose l and r so that this region is as small as possible). The method proposed in [15, 17] for constructing such labelings makes use of a sublattice Λ' that has index N in Λ and is similar to Λ. For this application it is also of interest to know when the boundary of the Voronoi cell of the sublattice Λ' does not contain any points of Λ: we call such sublattices "clean".

In Section 2 we give several results about the existence of similar sublattices, and in Section 3 we give a partial answer to the existence of clean sublattices in the two-dimensional case.

The only references we have found which treat the first problem are Baake and Moody [2],

[1] Take the lattice consisting of the vectors $(u, u+v)$ for $u \in E_6$, $v \in \sigma(E_6)$.

[3], which are concerned with lattices (and more general $\mathbb{Z}$-modules related to quasicrystals) in dimensions 1 to 4. These authors use techniques from ideal theory and quaternion algebras to enumerate similar substructures of given index.

A related problem has been studied in the crystallographic literature [1], [4], [5], [13]: given a lattice Λ (or more generally a $\mathbb{Z}$-module) in $\mathbb{R}^n$, when does there exist an isometry σ such that the "coincidence site sublattice" $\Lambda' = \Lambda \cap \sigma(\Lambda)$ has finite index in Λ? This is a somewhat different problem, since Λ' need not be similar to Λ, nor can every similar sublattice of Λ be obtained in this way.

We discovered the above references by accident. Using a computer we found that the lattice A_4 has multipliers of norm c precisely when c is one of the numbers

$$1, 4, 5, 9, 11, 16, 19, 20, 25, 29, 31, 36, \ldots$$

The same sequence appears in [1][2], as the indices of coincidence site sublattices in a certain three-dimensional quasicrystal. [1] identifies these numbers as those positive integers in which all primes congruent to 2 or 3 (mod 5) appear to an even power. As Theorem 2 shows, this is the same as our sequence. Although this can hardly be a coincidence, we do not at present see a direct connection between the A_4 and quasicrystal problems.

Two papers by Chapman [6], [7] consider a different, though again related, problem concerning sublattices of $\mathbb{Z}^n$.

2. The existence of similar sublattices

Let Λ be a rational $2k$-dimensional lattice with Gram matrix A, and let $c \in \mathbb{N}$. We wish to know if Λ has a sublattice Λ' such that $\sigma(\Lambda) = \Lambda'$ for some similarity σ of norm c. The existence of Λ' can be determined (in principal) by searching through Λ to see if it contains a set of vectors with Gram matrix cA. For small k and c this is quite feasible. We know of no other method that will always succeed.

By using the rational invariants of Λ we can obtain a necessary condition for Λ' to exist, which in some cases is also sufficient. The Hilbert symbol ([11], [18]) provides a convenient way to specify this condition.

For a rational number $r > 0$ we write (r) for the fractional ideal $r\mathbb{Q}$. A lattice Λ is (r)-*maximal* if Λ is maximal with respect to the property that $u \cdot u \in (r)$ for all $u \in \Lambda$ ([11], [12]).

[2]Found with the help of [16], where it is Sequence A31363.

The importance of this concept stems from the result ([12], Section 102:3) that the (r)-maximal lattices in a rational class form a single genus. We also say that Λ is *unigeneric* if it is unique in its genus.

Theorem 1. *A necessary condition for a $2k$-dimensional lattice Λ to have a multiplier of norm c is that the Hilbert symbol*

$$(c, (-1)^k \det \Lambda)_p = 1 \tag{1}$$

for all primes p dividing $2c \det \Lambda$. If Λ is unigeneric and (r)-maximal for some $r \in \mathbb{Q}$ then this condition is also sufficient.

Proof. If σ is a multiplier of norm c for Λ, then $\Lambda' = \sigma(\Lambda)$ and Λ are rationally equivalent, hence equivalent over the p-adic rationals for all p, and so have the same Hasse-Minkowski invariant ϵ_p for all p. The p-adic Hasse-Minkowski invariants for Λ and Λ' differ by a factor of $(c, (-1)^k \det \Lambda)_p$ ([18], p. 46; [11], Theorem 3.4.2). Since this invariant is 1 if p does not divide $2c \det \Lambda$, the first assertion follows. Conversely, if (1) holds for all p then Λ and the rescaled lattice $\sqrt{c}\Lambda$ are rationally equivalent. For $u \in \sqrt{c}\Lambda$, $u \cdot u \in (cr) \subseteq (r)$, so $\sqrt{c}\Lambda$ is contained in some maximal (r)-lattice M, say. By [12], Section 102:3, M and Λ are in the same genus, and since Λ is unigeneric, M is in the same class as Λ. Hence Λ has a sublattice in the same class as $\sqrt{c}\Lambda$. ∎

Note that it is not enough for Λ to be unigeneric for the condition of the theorem to be sufficient. The lattice with Gram matrix $\left[\begin{smallmatrix}1 & 0\\ 0 & 4\end{smallmatrix}\right]$ is unigeneric and rationally equivalent to $\left[\begin{smallmatrix}2 & 0\\ 0 & 8\end{smallmatrix}\right]$, but does not have a similarity of norm 2.

Many familiar lattices of small determinant and dimension are unigeneric (see [8]), and are often (1)-maximal (if they contain vectors of odd norm) or (2)-maximal (if they contain only vectors of even norm). In these cases Theorem 1 provides the answer to our first question, as the following theorem illustrates. The straightforward proof is omitted.

Theorem 2. *The lattices $\mathbb{Z}^2$, A_2, A_4, $\mathbb{Z}^6$, E_6 have multipliers of norm c just for the following* *values:*

$\mathbb{Z}^2$ *or* $\mathbb{Z}^6$*:* $c = r^2 + s^2$, $r, s \in \mathbb{Z}$ *(Sequence A001481); i.e.*

primes $\equiv 3 \pmod 4$ *appear to even powers in c,*

A_2 *or* E_6*:* $c = r^2 - rs + s^2$, $r, s \in \mathbb{Z}$ *(Sequence A003136); i.e.*

primes $\equiv 2 \pmod 3$ *appear to even powers in c,*

A_4*:* $c = r^2 + rs - s^2$, $r, s \in \mathbb{Z}$ *(Sequence A031363); i.e.*

primes $\equiv \pm 2 \pmod 5$ *appear to even powers in c.*

In some cases explicit similarities are easily found. For $\mathbb{Z}^2$ and A_2 we use complex coordinates and take σ to be multiplication by $r + si$ and $r + \omega s$ respectively, where $\omega = e^{2\pi i/3}$. For E_6 we use three complex coordinates ([10], p. 126, Eq. (120)) and again multiply by $r + s\omega$.

For A_4 some similarities can be found using the element

$$\alpha = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

of $Aut(A_4)$. It can be shown that $\sigma = a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4$ is a similarity for A_4 of norm

$$\tfrac{1}{2}\,[a_1 \quad a_2 \quad a_3 \quad a_4] \begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

provided

$$[a_1 \quad a_2 \quad a_3 \quad a_4] \begin{bmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 \\ -1 & -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = 0 \,.$$

This gives similarities of norms $1, 5, 11, \ldots$ but not $19, 29, \ldots$. We do not know a simple way to find the other similarities. Of course analogous similarities can be found for any cyclotomic lattice.

Theorem 3. *The lattices* $\mathbb{Z}^{4m}$*,* D_{4m} *and* D_{4m}^+ $(m \geq 1)$*,* E_8*,* K_{12}*, the Barnes-Wall lattice* BW_{16} *and the Leech lattice* Λ_{24} *have multipliers of every norm.*

Remark. Baake and Moody [3] establish this for $\mathbb{Z}^4$ and D_4 and also give a Dirichlet generating function for the number of similar sublattices of given index.

Proof. For $\mathbb{Z}^{4m}$, D_{4m}, D_{4m}^{+} we represent the vectors by m Hurwitz integral quaternions; then right multiplication by $q = r + si + tj + uk$ is a similarity of norm $|q|^2 = r^2 + s^2 + t^2 + u^2$.

We write the vectors of Λ_{24} in 4×6 MOG coordinates [10] and convert each of the six columns to a quaternion according to the scheme

$$\begin{array}{|cc|cc|cc|} \hline 1 & 1 & 1 & 1 & 1 & 1 \\ k & j & k & j & k & j \\ \hline i & k & i & k & i & k \\ j & i & j & i & j & i \\ \hline \end{array} \; .$$

In this form left or right multiplication by i, j or $\omega = \frac{1}{2}(-1 + i + j + k)$ are all automorphisms of Λ_{24}, as is the column permutation $(1,2)(3,4)(5,6)$. Then right multiplication by q is a similarity of Λ_{24} of norm $|q|^2$.

We define BW_{16} to be the sublattice of Λ_{24} in which the last two columns of the MOG are zero, and again use q. Finally, we define K_{12} to be the sublattice of Λ_{24} consisting of vectors

$$\begin{array}{|cc|cc|cc|} \hline a & b & c & d & e & f \\ A & B & C & D & E & F \\ \hline A & B & C & D & E & F \\ A & B & C & D & E & F \\ \hline \end{array} \; ,$$

which we associate with the three-dimensional quaternionic vector

$$(a + bi + \sqrt{3}Aj + \sqrt{3}Bk, \ldots, e + fi + \sqrt{3}Ej + \sqrt{3}Fk) \; . \tag{2}$$

Then right multiplication of (2) by $r + si + \sqrt{3}tj + \sqrt{3}uk$ defines a similarity of norm $r^2 + s^2 + 3t^2 + 3u^2$. Since the latter form represents $1, \ldots, 15$, by the "15-Theorem" of J.H.C. and W. A. Schneeberger (cf. [10]) it represents all numbers, and the proof is complete. (Of course the universality of this form was already known: it appears in [14].) ∎

Another easy consequence of Theorem 1 is:

Theorem 4. *A necessary condition for Λ to have a norm-doubling map is that $\dim \Lambda$ be even and that all primes $\equiv \pm 3 \pmod 8$ appear to even powers in $\det \Lambda$. If Λ is unigeneric and (r)-maximal for some $r \in \mathbb{Q}$ then this condition is also sufficient.*

3. The existence of clean sublattices in the two-dimensional case

The Voronoi cell of a two-dimensional lattice is either a hexagon or a rectangle ([9], Fig. 1). We assume that the lattice is generated by 1 and an imaginary quadratic integer. Similar arguments could be applied to more general two-dimensional lattices but the answers would be much more complicated.

We first consider a lattice Λ with a hexagonal Voronoi cell, generated say by 1 and $\omega = (-1+\sqrt{-N})/2$, $N \equiv 3 \pmod 4$. A similarity σ of norm c is represented by multiplication by $\alpha = a + b\omega$, $a, b \in \mathbb{Z}$, with $c = |\alpha|^2 = a^2 - ab + (N+1)b^2/4$. We begin with the case $N = 3$, the hexagonal lattice (a rescaled version of A_2).

Theorem 5. *For the hexagonal lattice generated by* 1 *and* $\omega = e^{2\pi i/3}$*, multiplication by* $\alpha = a + b\omega$ *yields a clean sublattice if and only if* $\alpha\theta$ *is a primitive element*[3] *of* $\mathbb{Z}[\omega]$*, where* $\theta = \omega - \bar{\omega} = \sqrt{-3}$*. There is a clean sublattice of index* c *if and only if* c *is a product of primes* $\equiv 1 \pmod 3$.

Proof. The Voronoi cell of Λ is a regular hexagon, and all edges are equivalent, so it is enough to consider say the left-hand edge L. This edge is the middle third of the line M from ω to $\bar{\omega}$. The lattice $\Lambda' = \alpha\Lambda$ is clean if and only if there is no point of Λ on the line αL. Since Λ is a lattice, if there is a point in the interior of M then there is a point on L. So Λ' is clean if and only if there is no point of Λ in the interior of αM, i.e. if and only if $\alpha\theta$ is primitive. The second assertion follows easily from the fact that the numbers primitively represented by $a^2 - ab + b^2$ are of the form 3^ϵ times a product of distinct primes $\equiv 1 \pmod 3$, where $\epsilon = 0$ or 1. ∎

We state the result for the general case without proof. The argument is similar to the above, but one must consider all sides of the Voronoi cell.

Theorem 6. *For the hexagonal-type lattice generated by* 1 *and* $\omega = (1+\sqrt{-N})/2$*, the similarity defined by multiplication by* $\alpha = a + b\omega$ *yields a clean sublattice if and only if*

(i) $\alpha\theta$ *is primitive, where* $\theta = \omega - \bar{\omega} = \sqrt{-N}$*,*

(ii) there is an odd number k *dividing* $N+1$ *such that* $\alpha(N-\theta)/(2k)$ *is integral and primitive, and*

(iii) there is an odd number k *dividing* $N+1$ *such that* $\alpha(N+\theta)/(2k)$ *is integral and primitive.*

[3] An element $r + s\omega \in \mathbb{Z}[\omega]$ is primitive if and only if $gcd(r, s) = 1$.

For the Kleinian lattice generated by 1 and $\omega = (1+\sqrt{-7})/2$, for example, $k = 1$ is the only possibility, and the theorem states that $\alpha\Lambda$ is clean if and only if $\alpha\theta$, $\alpha\omega\theta$ and $\alpha\bar{\omega}\theta$ are all primitive. Equivalently, $(a+b\omega)\Lambda$ is primitive if and only if a is odd, b is even and $gcd(a,b) = 1$.

Similar arguments also give the result for lattices with rectangular Voronoi cells. Again we omit the proof.

Theorem 7. *For the rectangular-type lattice generated by* 1 *and* $\theta = \sqrt{-N}$*,* $N \geq 1$*, the similarity defined by multiplication by* $\alpha = a + b\sqrt{-N}$ *yields a clean sublattice if and only if* $\alpha\bar{\alpha} = a^2 + Nb^2$ *(or equivalently* $a + Nb$*) is odd.*

Remarks. M. Baake has pointed out to us that by combining Theorems 5 and 7 with the results of [1] we can say that a sublattice of A_2 (or $\mathbb{Z}^2$) is clean if and only if it is a coincidence site sublattice.

It would be nice to know what happens in higher dimensions. What is the analogue of Theorem 5 for D_4 or E_8, for instance?

Acknowledgments. We thank H.-G. Quebbemann for suggesting that the similar sublattice problem is best handled via the Hilbert symbol, and for pointing out an error in the first version of this paper. We also thank V. A. Vaishampayan and S. D. Servetto for many conversations concerning vector quantization, and M. Baake and J. Martinet for comments on the manuscript. R. Schulze-Pillot drew our attention to the Chapman references.

References

[1] M. Baake, Solution of the coincidence problem in dimensions $d \leq 4$, in R. V. Moody, ed., *The Mathematics of Long-Range Aperiodic Order*, Kluwer, Dordrecht, 1997, pp. 199–237.

[2] M. Baake and R. V. Moody, Similarity submodules and semigroups, in J. Patera, ed., *Quasicrystals and Discrete Geometry*, Fields Institute Monographs, Vol. **10**, Amer. Math. Soc., Providence, RI, 1998, pp. 1–13.

[3] M. Baake and R. V. Moody, Similarity submodules and root systems in four dimensions, *Canad. J. Math.*, **51** (1999).

[4] M. Baake and P. A. B. Pleasants, Algebraic solution of the coincidence problem in two and three dimensions, *Z. Naturforschung* **50A** (1995), 711–717.

[5] M. Baake and P. A. B. Pleasants, The coincidence problem for crystals and quasicrystals, in G. Chapuis and W. Paciorek, eds., *Aperiodic '94*, World Scientific, Singapore, 1995, pp. 25–29.

[6] R. J. Chapman, Shrinking integer lattices, *Discrete Math.* **142** (1995), 39–48.

[7] R. J. Chapman, Shrinking integer lattices II, *J. Pure Appl. Alg.* **78** (1992), 123–129.

[8] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices I: Quadratic forms of small determinant, *Proc. Royal Soc. London* **418A** (1988), 17–41.

[9] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices VI: Voronoi reduction of three-dimensional lattices, *Proc. Royal Soc. London* **436A** (1992), 55–68.

[10] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 3rd ed., 1998.

[11] Y. Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge Univ. Press, Cambridge, 1993.

[12] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, NY, 1971.

[13] P. A. B. Pleasants, M. Baake and J. Roth, Planar coincidences for N-fold symmetry, *J. Math. Phys.* **37** (1996), 1029–1058.

[14] S. Ramanujan, On the expression of a number in the form $ax^2 + by^2 + cz^2 + du^2$, *Proc. Camb. Phil. Soc.* **19** (1917), 11–21; *Collected Papers*, Cambridge Univ. Press, Cambridge, 1927, pp. 169–178.

[15] S. D. Servetto, V. A. Vaishampayan and N. J. A. Sloane, Multiple description lattice vector quantization, in *Proceedings DCC '99: Data Compression Conference* (*Snowbird, 1999*), J. A. Storer and M. Cohn, Eds., IEEE Computer Society, Los Alamitos, CA, 1999, pp. 13–22.

[16] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/∼njas/sequences/.

[17] V. A. Vaishampayan, N. J. A. Sloane and S. D. Servetto, Multiple description vector quantization with lattice codebooks: design and analysis, preprint.

[18] G. L. Watson, *Integral Quadratic Forms*, Cambridge Univ. Press, Cambridge, 1960.