# UNIMODULAR EMBEDDINGS

MARK C. DUGGAN AND LARRY J. GERSTEIN

Abstract. In 1994 Morris Newman showed that a unimodular quadratic form on a lattice over a principal ideal domain can be represented by a triple-diagonal matrix of a rather special form, though the matrices associated with a given lattice in this way are generally not unique. The present paper considers positive definite unimodular lattices over the integers, and it begins the exploration of connections between those special matrix representations for a given lattice and the isometry class of that lattice.

The isometry problem for unimodular lattices over the integers is a major open problem that has this equivalent matrix-theoretic formulation: given symmetric unimodular matrices $A_1, A_2$ in $GL_n(\mathbb{Z})$, is there a unimodular matrix $T \in GL_n(\mathbb{Z})$ such that ${}^tTA_1T = A_2$? If this is the case, we write $A_1 \cong A_2$ and say that $A_1$ and $A_2$ are **congruent** over $\mathbb{Z}$. For the geometric formulation of the problem, let $V$ be an $n$-dimensional quadratic space over $\mathbb{Q}$. Thus $V$ is a vector space over $\mathbb{Q}$ carrying a symmetric bilinear form $B : V \times V \to \mathbb{Q}$ with associated quadratic form $q : V \to \mathbb{Q}$ given by $q(v) = B(v, v)$ for all $v \in V$. A **$\mathbb{Z}$-lattice** $L$ on $V$ is a $\mathbb{Z}$-module of the form $L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$, where $\mathbb{B} = \{v_1, \ldots, v_n\}$ is a basis for $V$. The associated matrix $A = \big(B(v_i, v_j)\big)$ is the **Gram matrix** of $L$ with respect to (or "in") $\mathbb{B}$, and we write $L \cong A$ with respect to $\mathbb{B}$. Changing the basis of $L$ results in a congruence transformation of the Gram matrix. We call $L$ *unimodular* if its Gram matrices are unimodular. In this setting, the unimodular classification problem is this: given unimodular lattices $L_1$ and $L_2$ on a space $V$, is there an isometry $\sigma \in O(V)$ such that $\sigma(L_1) = L_2$? An important special case of this problem is the question of whether a given unimodular lattice is actually isometric to the so-called "standard" unimodular lattice $\mathbb{Z}^n$.

The unimodular classification problem has been solved when $q$ is *indefinite*, that is, when the range of $q$ contains both positive and negative numbers. (See Gerstein [4], Theorem 9.22.) But it remains open in the definite case, and without loss of generality from now on we will assume all our spaces and lattices are *positive* definite: $q(v) > 0$ for all $v \neq 0$.

In the 19th century Jacobi showed that every symmetric integral matrix $A$ is congruent to a matrix in triple-diagonal form. More recently, Newman [7] showed that if $A$ is unimodular one can achieve a triple-diagonal form in which all elements on the sub- and super-diagonals are 1's, except for the bottom entry. Following

*Date*: January 17, 2013.

The first author was supported in part by College of Creative Studies Summer Undergraduate Research Fellowship.

Abbreviation: PDU stands for "positive definite unimodular."

Gerstein [3], we will use $[a_1, \ldots, a_n]$ for the triple-diagonal matrix

$$\begin{pmatrix} a_1 & 1 & & \\ 1 & a_2 & \ddots & \\ & \ddots & \ddots & 1 \\ & & 1 & a_n \end{pmatrix}$$

or for a lattice having this as a Gram matrix. If in the course of carrying out Newman's algorithm on $L$—when pursuing the question of whether a given unimodular lattice $L$ has an orthonormal basis—a vector $v$ is obtained with $q(v) = 1$, then by the Gram–Schmidt process the sublattice $\mathbb{Z}v$ can be split off from $L$, and we can focus on its orthogonal complement. Therefore our main interest in this paper will be on lattices of the form $[a_1, \ldots, a_n]$ with $a_i \geq 2$ for all $i$, and we assume this to be the case from now on. An induction argument shows that the discriminant of $\underbrace{[2, \ldots, 2]}_{n}$ is $n + 1$, and hence $[2, \ldots, 2]$ is positive definite for all $n \geq 1$; and since $[a_1, \ldots, a_n] = [2, \ldots, 2] + \mathrm{diag}(a_1 - 2, \ldots a_n - 2)$, it follows that $[a_1, \ldots, a_n]$ is positive definite.

In [3] a lattice $L \cong [a_1, \ldots, a_n]$ was called **nearly unimodular** for two reasons: elementary row and column operations show that all but one of the invariant factors of the matrix $[a_1, \ldots, a_n]$ are 1's, and Newman's theorem shows that a unimodular lattice $L$ of rank $n + 1$ has a nearly unimodular sublattice of rank $n$. So, upon localization over the rings of $p$-adic integers, it follows that if a nearly unimodular $\mathbb{Z}$-lattice $L$ of rank $n$ is a sublattice of a unimodular $\mathbb{Z}$-lattice $M$ of rank $n+1$, then over the $p$-adic integers the localized lattice $L_p$ contains a unimodular orthogonal component of $M_p$ of rank $\geq n-1$. It is therefore reasonable to hope that considering the nearly unimodular lattices inside a given unimodular lattice $M$ will lead to useful invariants for the isometry class of $M$.

In this paper we start by showing for which sequences of integers $a_1, \ldots, a_n$ a lattice $L \cong [a_1, \ldots, a_n]$ extends to a positive definite unimodular lattice of rank $n + 1$ with a Gram matrix of the form

$$\begin{pmatrix} a_1 & 1 & & & & \\ 1 & a_2 & \ddots & & & \\ & \ddots & \ddots & 1 & & \\ & & 1 & a_n & c & \\ & & & c & a_{n+1} \end{pmatrix}, \qquad (*)$$

and then we explore some consequences of this result. This will leave other problems for further research: applying the Jacobi/Newman algorithm to an assortment of Gram matrices for a given unimodular lattice will yield different nearly unimodular sublattices. Can one characterize the isometry classes of nearly unimodular lattices inside a given unimodular lattice? And if so, will that lead to a solution to the classification problem for positive definite unimodular lattices? In pursuit of a canonical form for the Gram matrices of lattices in a given class, can one extend Jacobi/Newman so that the resulting $a_i$ appearing on the diagonal satisfy a reasonable bound, or so that the discriminant $d[a_1, \ldots, a_n]$ is small?

Apart from the number-theoretic interest in classification of integral quadratic forms, lattices of the kind under discussion have applications in topology. Unimodular lattices are important invariants of 4-manifolds. For example, Freedman has shown that two smooth simply-connected 4-manifolds are homeomorphic if and only if their associated unimodular lattices are isometric. (See Freedman and Quinn [2]; or see Scorpan [9], page 240, for details.) And nearly unimodular lattices have arisen recently in the work of Greene [5] in connection with the study of lens spaces. (In [5] the lattices denoted here by $[a_1, \ldots, a_n]$ are called *linear lattices*.)

It is known that every positive definite unimodular $\mathbb{Z}$-lattice $L$ of rank $n \leq 7$ has an orthonormal basis $\{e_1, \ldots, e_n\}$. (See O'Meara [8], §106D.) Since every primitive vector (a vector extending to a basis of $L$) is a primitive linear combination of the $e_i$, it follows that every diagonal entry on a Gram matrix for such a lattice $L$ must be a primitive sum of $n$ integer squares.

From now on we will write PDU for the expression "positive definite unimodular."

**Example 1.** Both of the integers $3, 6$ are sums of three squares in essentially one way, and no dot product of the form $(\pm 1, \pm 1, \pm 1) \cdot (2, 1, 1)$ is equal to 1. Therefore no lattice with Gram matrix $\begin{pmatrix} 3 & 1 \\ 1 & 6 \end{pmatrix}$ is a sublattice of a PDU lattice of rank 3. On the other hand, because $(1, -1, 0, 1) \cdot (2, 1, 1, 0) = 1$, a PDU lattice of rank 4 does contain such a sublattice. In fact such a sublattice is *primitive*, meaning that a basis for it extends to a basis of the larger lattice. (See Cassels [1], Theorem 3.1, Chapter 7.)

When one begins to consider larger numbers as potential matrix entries, numbers that are primitive sums of squares may be expressible in many ways as primitive sums of squares. In fact every positive integer $k$ is a primitive sum of five squares: $k - 1$ is a sum of four squares (by Lagrange), and add 1 to that. Moreover, PDU lattices of rank $n \geq 8$ need not have orthonormal bases, and in fact the number of isometry classes of PDU lattices of rank $n$ grows rapidly with $n$. Therefore the consideration of sums of squares will generally not be sufficient to answer to our question of when a nearly unimodular lattice $[a_1, \ldots, a_n]$ extends to a PDU lattice with Gram matrix $(*)$. From now on we will denote the matrix $(*)$ by

$$[a_1, \ldots, a_n \mid a_{n+1}; c].$$

Given integers $a_1, \ldots, a_n$, define $d_0 = 1$, and for $n \geq 1$ define $d_n = \det[a_1, \ldots, a_n]$. Notice that $d_n = a_n d_{n-1} - d_{n-2}$.

**Lemma.** $(d_n, d_{n-1}) = 1$ *for all* $n \geq 1$*, and therefore every congruence of the form* $d_{n-1}x \equiv b \pmod{d_n}$ *has a unique solution.*

*Proof.* The first statement is clear if $n \leq 2$. If $n \geq 3$ the general result follows by induction from the equation $d_{k+1} = a_{k+1}d_k - d_{k-1}$. The second statement is then immediate. □

In what follows, we let $d_{n-1}^{-1}$ denote the inverse of $d_{n-1}$ in $\mathbb{Z} \pmod{d_n}$.

**Theorem 1.** *The nearly unimodular matrix* $[a_1, \ldots, a_n]$ *extends to a PDU matrix of the form* $A = [a_1, \ldots, a_n \mid a_{n+1}; c]$ *if and only if* $c$ *is a solution to the congruence*

$$x^2 \equiv -d_{n-1}^{-1} \pmod{d_n}.$$

*Proof.* If an extension of the stated type is possible, then

$$1 = \det A = a_{n+1}d_n - d_{n-1}c^2,$$

and so $d_{n-1}c^2 \equiv -1 \pmod{d_n}$.

Conversely, suppose the integer $c$ satisfies the congruence $d_{n-1}c^2 \equiv -1 \pmod{d_n}$. Then define $a_{n+1} = \dfrac{1 + d_{n-1}c^2}{d_n}$, and set $A = [a_1, \ldots, a_n | a_{n+1}; c]$. Then

$$\det A = a_{n+1}d_n - c^2 d_{n-1} = 1,$$

as desired. □

The following consequence of the preceding theorem is in the literature. For instance, see [1] (Lemma 6.3 in Chapter 9).

**Corollary.** Let $m$ be an integer $\geq 2$ with standard factorization $m = 2^{\alpha_0}p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Then $m$ is a primitive sum of two squares if and only if $\alpha_0 \leq 1$ and $p_i \equiv 1 \pmod 4$ for $i = 1, \ldots, r$.

*Proof.* We will apply the theorem to the $1 \times 1$ nearly unimodular matrix $[m]$; so $d_1 = m$ and $d_0 = 1$. By the theorem, $[m]$ extends to a $2 \times 2$ PDU matrix

$$A = \begin{pmatrix} m & c \\ c & a_2 \end{pmatrix}$$

if and only if $-1$ is a quadratic residue modulo $m$. But this happens if and only if $\alpha_0 \leq 1$ and $p_i \equiv 1 \pmod 4$ for all $i$. (For a proof, see Ireland and Rosen [6], Proposition 5.1.1.)

Now suppose $L$ is a $\mathbb{Z}$-lattice satisfying $L \cong A$ with respect to some basis $\{v_1, v_2\}$. Then $q(v_1) = m$, and therefore, by the remark preceding this corollary, $m$ is a primitive sum of two squares. □

**Example 2.** The purpose of this example is to show that if the nearly unimodular lattice $L \cong [a_1, \ldots, a_n]$ extends to the PDU lattices

$$M_1 \cong [a_1, \ldots, a_n \mid a_{n+1}; c] \quad \text{and} \quad M_2 \cong [a_1, \ldots, a_n \mid a'_{n+1}; c'],$$

then $M_1$ and $M_2$ need not be isometric. Recall that there are exactly two isometry classes of PDU lattices of rank 8: the class of the standard lattice $\mathbb{Z}^8 \cong \langle 1, \ldots, 1\rangle$ (this is *odd* or *type I*) and the class of the even (or *type II*) PDU lattice $E_8$. But we claim that both of these lattices are of the form $[2, \ldots, 2 \mid a_8; c]$. By an induction argument, the discriminant of a rank $n$ lattice $[2, \ldots, 2]$ is $n+1$. The theorem tells us that the rank 7 lattice $L \cong [2, \ldots, 2]$ extends to at least one PDU of rank 8: $d_6 = 7, d_7 = 8$, and $-7^{-1} \equiv 1 \pmod 8$. So an extension of the desired type exists if and only if $c^2 \equiv 1 \pmod 8$; equivalently, $c$ is odd. For example,

$$\mathbb{Z}^8 \cong [2, \ldots, 2 \mid 1; 1] \cong [2, \ldots, 2 \mid 43; 7]$$

and

$$E_8 \cong [2, \ldots, 2 \mid 8; 3] \cong [2, \ldots, 2 \mid 22; 5].$$

While the preceding example shows that a lattice $L \cong [a_1, \ldots, a_n]$ does not determine a unique class of PDU lattice $M \cong [a_1, \ldots, a_n \mid a_{n+1}; c]$ to which it extends (provided that there is at least one such extension), the following theorem tells us that *$L$ together with the congruence class of $c$ mod $d_n$* uniquely determines the class of $M$.

**Theorem 2.** *Given a nearly unimodular lattice $L \cong [a_1, \dots, a_n]$, with $a_i \geq 2$ for all $i$. Suppose $L$ extends to a PDU lattice $M \cong [a_1, \dots, a_n \mid a_{n+1}; c]$, and suppose $c' \equiv c \pmod{d_n}$. Then there is a unique integer $a'_{n+1}$ such that $M \cong [a_1, \dots, a_n \mid a'_{n+1}; c']$.*

*Proof.* Assume $c' = c + kd_n$.

First suppose $n = 1$. So $L \cong [a_1] \cong \langle a_1 \rangle$, and $M \cong [a_1 \mid a_2; c] = \begin{pmatrix} a_1 & c \\ c & a_2 \end{pmatrix}$ in $\{v_1, v_2\}$. Here $d_1 = a_1$. Set $v'_2 = v_2 + kv_1$ and $a'_2 = q(v'_2)$. Then $M \cong [a_1 \mid a'_2; c']$ in $\{v_1, v'_2\}$.

Now suppose $n \geq 2$.

Assume $M \cong [a_1, \dots, a_n \mid a_{n+1}; c]$ in the base $\{v_1, \dots, v_{n+1}\}$. Define

$$v'_{n+1} = \alpha_1 v_1 + \cdots + \alpha_n v_n + v_{n+1},$$

with

$$\alpha_i = \begin{cases} (-1)^i k d_{i-1} & \text{if } n \text{ is even} \\ (-1)^{i-1} k d_{i-1} & \text{if } n \text{ is odd.} \end{cases}$$

for $1 \leq i \leq n$, and set $a'_{n+1} = q(v'_{n+1})$.

Suppose $n$ is even. Then

$$\begin{aligned} B(v'_{n+1}, v_n) &= B\Big(\sum_{i=1}^{n} (-1)^i k d_{i-1} v_i + v_{n+1},\, v_n\Big) \\ &= B\Big((-1)^{n-1} k d_{n-2} v_{n-1} + (-1)^n k d_{n-1} v_n + v_{n+1},\, v_n\Big) \\ &= B(-k d_{n-2} v_{n-1} + k d_{n-1} v_n + v_{n+1},\, v_n) \\ &= c + k(a_n d_{n-1} - d_{n-2}) \\ &= c + k d_n = c'. \end{aligned}$$

And for $2 \leq j \leq n-1$ we have

$$\begin{aligned} B(v'_{n+1}, v_j) &= B\Big(k \sum_{i=1}^{n} (-1)^i d_{i-1} v_i,\, v_j\Big) \\ &= kB\Big((-1)^{j-1} d_{j-2} v_{j-1} + (-1)^j d_{j-1} v_j + (-1)^{j+1} d_j v_{j+1},\, v_j\Big) \\ &= (-1)^j k(\underbrace{-d_{j-2} + a_j d_{j-1}}_{d_j} - d_j) \\ &= 0. \end{aligned}$$

Finally,

$$B(v'_{n+1}, v_1) = kB(-v_1 + d_1 v_2, v_1) = kB(-v_1 + a_1 v_2, v_1) = 0.$$

Now suppose $n$ is odd. Then

$$\begin{aligned} B(v'_{n+1}, v_n) &= B\Big((-1)^{n-2} k d_{n-2} v_{n-1} + (-1)^{n-1} k d_{n-1} v_n + v_{n+1},\, v_n\Big) \\ &= k(-d_{n-2} + d_{n-1} a_n) + c \\ &= c + k d_n = c'. \end{aligned}$$

The proof that $B(v'_{n+1}, v_j) = 0$ if $j \leq n$ is essentially the same as when $n$ is even. In brief: the values of $B(v'_{n+1}, v_j)$ for $j \leq n-1$ when $n$ is even get multiplied by $-1$ if $n$ is odd.

Uniqueness of $a_{n+1}$ follows from the fact that $dM = 1$. □

**Remark.** The isometries

$$[2,\dots,2 \mid 1;1] \cong [2,\dots,2 \mid 43;7] \quad \text{and} \quad [2,\dots,2 \mid 8;3] \cong [2,\dots,2 \mid 22;5]$$

in the example preceding Theorem 2 follow from the uniqueness of the isometry classes of PDUs of type I and type II in rank 8. But the number of classes proliferates in higher ranks, so it is useful to see another argument. First note that if

$$M \cong [a_1,\dots,a_n \mid a_{n+1};c] \text{ in } \{v_1,\dots,v_n,v_{n+1}\}$$

then

$$M \cong [a_1,\dots,a_n \mid a_{n+1};-c] \text{ in } \{v_1,\dots,v_n,-v_{n+1}\}.$$

For instance $[2,\dots,2 \mid 8;3] \cong [2,\dots,2 \mid 8;-3]$. Here $d_7 = 8$, and $-3 \equiv 5 \pmod 8$. Therefore by Theorem 2 we have $[2,\dots,2 \mid 8;-3] \cong [2,\dots,2 \mid a'_8;5]$; and $a'_8 = 22$ because the lattice has discriminant 1. A similar argument holds for the other isometry.

Recall that if primitive roots exist mod $m$—that is, if $m$ is 2 or 4 or $p^\alpha$ or $2p^\alpha$ for some odd prime $p$—then a quadratic congruence mod $m$ has at most two solutions. (See Ireland and Rosen [6], Chapter 4, §2.)

**Corollary.** Suppose primitive roots exist mod $m$. Given $a_1,\dots,a_n$ with $a_i \geq 2$ for all $i$. If $d_n = d[a_1,\dots,a_n] = m$, then there is at most one isometry class of PDU lattices of the form

$$[a_1,\dots,a_n \mid a_{n+1},c].$$

*Proof.* From Theorem 1, such an extension exists if and only if the congruence $x^2 \equiv -d_{n-1}^{-1} \pmod m$ is solvable. But from the hypothesis on $m$, if $c$ satisfies this congruence then $c$ and $-c$ are the *only* solutions mod $m$. From the preceding remark we know

$$[a_1,\dots,a_n \mid a_{n+1},c] \cong [a_1,\dots,a_n \mid a_{n+1};-c],$$

and so the corollary follows from Theorem 2. □

**Example 3.** Suppose primitive roots exist mod $m$, and suppose

$$L \cong [\underbrace{2,\dots,2}_{m-1}].$$

Then $d_{m-1} = m$ and $d_{m-2} = m-1 \equiv -1 \pmod m$. Therefore $-d_{m-2}^{-1} \equiv 1 \pmod m$; so it follows from the preceding corollary that there is exactly one isometry class of PDU lattices of rank $m$ of the form $[2,\dots,2 \mid a_m;c]$. But $\mathbb{Z}^m$ is such a lattice, namely $\mathbb{Z}^m \cong [2,\dots,2 \mid 1;1]$. Therefore

$$[\underbrace{2,\dots,2}_{m-1} \mid a_m;c] \cong \mathbb{Z}^m.$$

## References


1. J. W. S. Cassels, *Rational Quadratic Forms*, Dover, 2008.
2. M. H. Freedman and F. Quinn, *Topology of 4-Manifolds*, Princeton University Press, 1990.
3. L. J. Gerstein, *Nearly unimodular quadratic forms*, Annals of Mathematics 142 (1995), 597-610.
4. L. J. Gerstein, *Basic Quadratic Forms*, American Mathematical Society, 2008.
5. J. Greene, *The lens space realization problem*, Annals of Mathematics, to appear.

6. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1982.
7. M. Newman, *Tridiagonal matrices*, Linear Algebra and Its Applications 201 (1994), 51-55.
8. O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, 1963 (reprinted in 2000).
9. A. Scorpan, *The Wild World of 4-Manifolds*, American Mathematical Society, 2005.

Department of Mathematics, University of California, Santa Barbara, CA 93106.
*E-mail address*: markduggan@umail.ucsb.edu

Department of Mathematics, University of California, Santa Barbara, CA 93106.
*E-mail address*: gerstein@math.ucsb.edu