PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 106, Number 4, August 1989

NORMAL FORMS FOR DEFINITE INTEGER UNIMODULAR QUADRATIC FORMS

SHMUEL FRIEDLAND

(Communicated by William W. Adams)

ABSTRACT. In this paper we show that any two positive definite integer unimodular quadratic forms have a common sublattice of codimension 2. Moreover, any such form is equivalent to a semi-normal form with at most three eigenvalues different from 1.

1. INTRODUCTION

Let $A(x,x)$ be a quadratic form over the integers. That is, $A(x,x)$ is represented by a symmetric matrix A with integer coefficients. Two symmetric forms $A(x,x)$ and $B(x,x)$ are called equivalent if $B = TAT^t$ for some unimodular T. A quadratic form $A(x,x)$ is called unimodular if A is unimodular, i.e. $\det(A) \in \{1, -1\}$. The equivalence class of indefinite integer unimodular forms is determined by the rank— $\rho(A)$ (the dimension of A), the signature— $\sigma(A)$ and the type (whether all diagonal entries of A are even or not). See for example [M-H]. In particular, any indefinite A is equivalent to a unique form $M \oplus N$. Here M is a direct sum of k copies of the indefinite unimodular form in two variables $2x_1x_2$ and $|\sigma(A)| = \rho(A) - 2k$. If A is of type (I) then either N or $-N$ is equal to the identity matrix I of dimension $|\sigma(A)|$. If A is of type (II) then either N or $-N$ is a direct sum of j copies of E_8—the unique positive definite unimodular form of type (II) and rank 8.

The (positive) definite quadratic unimodular forms have much richer structure. According to Eichler, e.g. [M-H, 2.6], definite unimodular quadratic forms decompose uniquely (up to a permutation of factors) to a direct sum of indecomposable definite unimodular quadratic forms. For $n = \rho(A) \leq 7$ there is only one trivial form (given by the identity matrix). For $n = 8$ one has two (nonequivalent) forms I_8 and E_8. Kneser showed that there are exactly seven indecomposable forms for $n \leq 16$. The number of equivalence classes of definite unimodular forms seems to grow exponentially with n. See [M-H, 2.6].

Received by the editors June 10, 1988 and, in revised forms, September 23, 1988 and December 8, 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11E12.

The author was partially supported by NSF grant DMS-8700610.

0002-9939/89 $1.00 + $.25 per page

In this paper we show that any positive definite unimodular form over integers can be brought to a normal form such that the corresponding symmetric matrix has at least $n-3$ eigenvalues equal to 1. More precisely we show:

Theorem. *Let $A(x,x)$ and $B(x,x)$ be two positive definite integer forms with rank n and the determinant equal to one. Then A and B are equivalent over the integers to $A_1 = (a_{ij})_1^n$ and $B_1 = (b_{ij})_1^n$ respectively, so that $a_{ij} = b_{ij}$ for $1 \le i, j \le n-2$. Furthermore, B is equivalent to the matrix:*

$$(1) \qquad \begin{aligned} &(I + \tau f g^t)(I + \tau g f^t) - hh^t, \qquad \tau \neq -1, f^t g = 1, \\ &(\tau+1)^2(1 - h^t h) + 2\tau(\tau+1)(h^t g)(h^t f) - \tau^2 (h^t g)^2 (f^t f) = 1. \end{aligned}$$

Here, τ is an integer, f, g, and h are column vectors with n integer coordinates. It follows that the above matrix has at least $n-3$ eigenvalues equal to 1.

We deduce our theorem by carefully analyzing the equivalent indefinite forms $A \oplus (-1)$ and $B \oplus (-1)$. In this analysis the use of the Smith normal form is crucial. In fact, our results are closely related to the recent results of [C-S, Ch. 26].

2. Proof

For a ring K let $M_n(K)$, $S_n(K)$ and $U_n(K)$ denote the set of $n \times n$ matrices, symmetric matrices and unimodular matrices with the coefficients in K respectively. By K^n we denote the set of column vectors of length n with coordinates in K. Let $\mathbf{Z}_p$ be the ring of p-adic integers and set $\mathbf{Z}_\infty = \mathbf{R}$. $A, B \in S_n(\mathbf{Z})$ are called p-equivalent if $B = TAT^t$ for some $T \in U_n(\mathbf{Z}_p)$. A and B are said to have the same genus if A and B are p equivalent for all $2 \le p \le \infty$. It is known, e.g. [Cas, p. 128] that there is only a finite number of equivalence classes with a prescribed nonzero determinant d. Clearly, if A and B have the same genus then $\det(A) = \det(B)$. It is well known that A and B can have the same genus and not be equivalent. The genera can be divided to smaller classes by using the spinor genera. The number of spinor genera in a genus is finite and is a power of 2. See [Cas, p. 202]. In fact if $\det(A)$ is not divisible by $p^{\delta(p,n)}$ for any prime p then each genus contains exactly one spinor genus. See [Cas, Thm. 1.5, p. 203]. Here

$$(2) \quad \delta(2,n) = n(n-3)/2 + [(n+1)/2], \qquad \delta(p,n) = n(n-1)/2 \quad \text{for } p > 2.$$

Let $A, B \in S_n(\mathbf{Z})$ be two positive definite unimodular forms. It is known that A and B are p-equivalent for all $p > 2$ [Cas, p. 116]. Obviously, if A and B are not of the same type then A and B are not 2-equivalent. It is known that A and B can belong to the same genus and may not be equivalent. For example, I_9 and $I_1 \oplus E_8$ belong to the same genus but obviously are not equivalent, e.g. [Ome, p. 106]. (Note that $n = 9$ is the smallest possible rank for which this phenomenon can happen).

Let $a > 0$ be an integer and set $E = A \oplus (-a)$, $F = B \oplus (-a) \in S_{n+1}(\mathbf{Z})$. Assume first that $a = 1$. Then E and F are indefinite, unimodular, with rank $n+1$, signature $n-1$ and type (I). Hence E and F are equivalent. Suppose next that

$$a \neq 0 \pmod{p^{\delta(p,n+1)}}, \qquad 2 \leq p < \infty. \tag{3}$$

Assume that A and B are equivalent over $\mathbf{Z}_2$. Then A and B belong to the same genus. Hence, E and F belong to the same genus. The assumption (3) yields that E and F are equivalent [Cas, Thm. 1.5, p. 203].

In what follows we assume that either $a = 1$ or A and B belong to the same genus and a satisfies (3). Hence, $F = PEP^t$, $P \in U_{n+1}(\mathbf{Z})$. Let

$$P = \begin{pmatrix} Q & u \\ v^t & \omega \end{pmatrix}, \qquad Q \in M_n(\mathbf{Z}),\ u, v \in \mathbf{Z}^n,\ \omega \in \mathbf{Z}.$$

Then, the equality $F = PEP^t$ is equivalent to

$$\begin{aligned} B &= QAQ^t - auu^t, \qquad a\omega u = QAv, \\ v^tAv &= a(\omega^2 - 1), \qquad \det(Q) = \omega \det(P). \end{aligned} \tag{4}$$

The first three equalities in (4) are straightforward. To deduce $\det(Q) = \omega \det(P)$ we argue as follows. First note that since A is positive definite and $a > 0$ the third equality of (4) yields $\omega \neq 0$. For $U \in M_{n+1}(\mathbf{Z})$ let $(U_{ij})_1^2$ be a partition of U to a 2×2 block matrix conformal with the above partition of P. Set

$$U = (U_{ij})_1^2, \qquad U_{11} = I_n, U_{12} = Av, \qquad U_{21} = 0, \qquad U_{22} = -a\omega.$$

In view of the second equality in (4) it follows that PU is block lower triangular matrix. Hence

$$\det(PU) = \det(Q)(v^tAv - a\omega^2) = \det(P)\det(U) = \det(P)(-a\omega).$$

Use the third equality of (4) to deduce $\det(Q) = \omega \det(P) = \pm\omega$.

For a vector $x \in \mathbf{Z}^n$ denote by $\overline{x} \in \mathbf{Z}^n$ the primitive vector corresponding to x. That is, the coordinates of $\overline{x}$ are coprime and $x = \xi\overline{x}$ for some $\xi \in \mathbf{Z}$. Set

$$u = \alpha\overline{u}, \qquad v = \beta\overline{v}.$$

Since P is unimodular it follows that the vectors (α, ω) and (β, ω) are primitive. Hence, the second equality in (4) implies $QA\overline{v} = \mu\omega\overline{u}$, $\mu \in \mathbf{Z}$. Let $D(Q)$ be the Smith normal form of Q. Thus $D(Q)$ is a diagonal matrix $\operatorname{diag}\{d_1, \ldots, d_n\}$, $d_i | d_{i+1}$ for $i = 1, \ldots, n-1$ and $\det(D(Q)) = \det(Q)\det(P) = d_1 \cdots d_n = \omega$. There exist two unimodular matrices S and T so that $Q = SD(Q)T^{-1}$. Let

$$A = TA_1T^t, \qquad B = SB_1S^t, \qquad u = Su_1, \qquad v = (T^{-1})^t v_1.$$

Substitute the above expressions into (4) to deduce that w.l.o.g. we may assume that $A = A_1$, $B = B_1$ and $Q = D(Q)$. As A is unimodular it follows that $A\overline{v}$

is primitive. We now claim that $d_i = 1$ for $i = 1, \dots, n-1$, i.e. $d_n = \omega$. Assume to the contrary that a prime p divides d_i for some $i < n$. For an integer m let $\operatorname{ord}_p(m)$ be the maximal integer e so that $p^e | m$. Our assumption yields that $\operatorname{ord}_p(d_i) < \operatorname{ord}_p(\omega)$ for all i. The equality $D(Q)A\overline{v} = \mu\omega\overline{u}$ implies that p divides each component of $A\overline{v}$. This is impossible since $\overline{v}$ is primitive and A is unimodular. As $\omega D(Q)^{-1}$ is an integer matrix the primitivity of $A\overline{v}$ implies that $\mu \in \{1, -1\}$. W.l.o.g. we may assume that $\mu = 1$. Let U be a unimodular matrix of the form $V \oplus (1)$. Note that U commutes with $D(Q)$. Thus, we can multiply the first equality in (4) from the left by U and from the right by U^t. Effectively, we replaced in the first equality of (4) A by UAU^t, B by UBU^t, u by Uu and v by $(U^t)^{-1}v$. Since V is an arbitrary $(n-1) \times (n-1)$ unimodular matrix it is possible to choose V so that the first $n-2$ components of Uu are equal to zero. That is, we may assume in (4) that

$$(5) \qquad Q = D(Q) = \operatorname{diag}\{1, \dots, 1, \omega\}, \qquad u^t = (0, \dots, 0, u_{n-1}, u_n).$$

The first part of the theorem follows from the first part of (4) with $a = 1$ and (5).

We now deduce the second part of the theorem. We have in the first equality of (4)

$$Q = D(Q) = \operatorname{diag}\{1, \dots, 1, \omega\} = I + (\omega - 1)ee^t, \qquad e^t = (0, \dots, 0, 1), \ \omega \neq 0.$$

Let $A(x, x) = (x, x)$ be the standard form. We then have the equality (4) with $a = 1$ and suppose furthermore that Q is of the form (5). Thus, A in (4) is given by RR^t for some R. Multiply the first equality in (4) by R^{-1} from the left and by $(R^t)^{-1}$ from the right. Substitute $A = RR^t$ to deduce the first part of (1) with $f = R^{-1}e$, $g = R^t e$, $h = R^{-1}u$ and $\tau = \omega - 1$. The second equality in (1) is equivalent to the condition $\det(B) = 1$. Indeed, note that

$$(I + \tau fg^t)(I + \tau gf^t) - hh^t = (I + \tau fg^t)(I - ww^t)(I + \tau gf^t),$$
$$w = (I - \tau(\tau + 1)^{-1} fg^t)h, \ \det(I + \tau fg^t) = \tau + 1, \ \det(I - ww^t) = 1 - w^t w.$$

Finally, note that if $x \in \mathbf{R}^n$ is orthogonal to f, g and h then $Bx = x$. That is, B has at least $n - 3$ eigenvalues equal to 1.

3. Remarks and comments

It is not clear to us that the results of our theorem are best possible. It would be nice to have an example of two unimodular definite quadratic forms which are not equivalent on any sublattice of codimension 1. Furthermore, we do not have any example of a positive definite unimodular quadratic form which can not be represented by a symmetric unimodular matrix with at least $n - 2$ eigenvalues equal to one. We now bring a few arguments to show that perhaps it is possible to improve the results of our theorem.

Suppose that the unimodular definite quadratic forms A and B are equivalent over the diadics. Then, the equality (4) holds for any $a > 0$ satisfying the condition (3). Thus, the arguments of the preceding section imply the existence of a sublattice of codimension 2 on which the two forms are equivalent. If $A(x,x)$ and $B(x,x)$ are not equivalent then these sublattices should depend on a. Hence we conjecture:

Conjecture. *Let $A(x,x)$ and $B(x,x)$ be two positive definite unimodular quadratic forms equivalent over diadics. Then there exist representations $A = (a_{ij})_1^n$ and $B = (b_{ij})_1^n$ so that $a_{ij} = b_{ij}$ for $1 \le i,\ j \le n-1$.*

Let A be the unimodular matrix given in (1). Since $\tau \neq -1$ it follows that the form $A(x,x)$ is positive definite on the subspace orthogonal to the vector h. The Cauchy interlacing theorem implies that A has at least $n-1$ positive eigenvalues. The second condition of (1) implies that $\det(A) = 1$. Hence, A is a positive definite unimodular matrix. Let $P = I + fy^t$ where $f^t y = 0$. Thus, $\det(P) = 1$. Consider the matrix $B = PAP^t$. Then B is given by

$$B = (I + fu^t)(I + uf^t) - vv^t, \qquad u = \tau g + y,\ v = h + (y^t h)f. \tag{6}$$

If we can choose y so that f, u and v are linearly dependent it would follows that B has at least $n-2$ eigenvalues equal to 1. The existence of such y seems to be possible in many cases.

Acknowledgment

I would like to thank to L. Gerstein for finding errors in earlier versions and his suggestions to correct them.

References

[Cas] J. W. S. Cassels, *Rational quadratic forms*, Academic Press, 1978.

[C-S] J. H. Conway and N. J. A. Sloane, *Sphere packing, lattices and groups*, Springer-Verlag, 1988.

[M-H] J. Milnor and D. Husemoller, *Symmetric bilinear forms*, Springer-Verlag, 1973.

[Ome] O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, 1963.

Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, Chicago, Illinois 60680