Math. Proc. Camb. Phil. Soc. (2007), **143**, 521 © 2007 *Cambridge Philosophical Society*
doi:10.1017/S0305004107000710 *Printed in the United Kingdom*

Polynomial bounds for equivalence of quadratic forms with cube-free determinant

BY RAINER DIETMANN

Institut für Algebra und Zahlentheorie,
Pfaffenwaldring 57,
D-70569 *Stuttgart, Germany.*
e-mail: dietmarr@mathematik.uni-stuttgart.de

(*Received* 24 *October* 2005*; revised* 12 *October* 2006)

Abstract

Given two integrally equivalent integral quadratic forms in at least three variables and with cube-free determinant, we establish an upper bound on the smallest unimodular matrix transforming one of the forms into the other. This bound is polynomial in the height of the two forms involved, confirming a conjecture of Masser for the class of forms considered.

1. *Introduction*

Let $Q_1, Q_2 \in \mathbf{Z}[X_1, \ldots, X_s]$ be classically integral non-singular quadratic forms. By this we mean that Q_1 and Q_2 are of the form

$$Q_1(X_1, \ldots, X_s) = \sum_{1 \leqslant i,j \leqslant s} a_{ij} X_i X_j, \; Q_2(X_1, \ldots, X_s) = \sum_{1 \leqslant i,j \leqslant s} b_{ij} X_i X_j \qquad (1)$$

for suitable integral symmetric $s \times s$-matrices $A = (a_{ij})$ and $B = (b_{ij})$ with $\det A \neq 0$, $\det B \neq 0$. We call Q_1 and Q_2 integrally equivalent, if there is a unimodular linear transformation $R : \mathbf{Z}^s \to \mathbf{Z}^s$ with $Q_2(X_1, \ldots, X_s) = Q_1(R(X_1, \ldots, X_s))$. Here unimodular means having determinant 1 or -1. Clearly this defines an equivalence relation on the set of classically integral quadratic forms. Using the matrix notation from (1·1) and writing $A[B]$ for $B^T AB$ with B^T denoting the transpose of B, this can also be expressed in the following form: Q_1 and Q_2 are integrally equivalent if and only if there is a unimodular integral $s \times s$-matrix R with $B = A[R]$. So we can also speak of integrally equivalent symmetric matrices $A, B \in \mathbf{Z}^{s \times s}$, where $\mathbf{Z}^{s \times s}$ denotes the ring of integral $s \times s$-matrices (and we use the same notation when $\mathbf{Z}$ is replaced by another ring). Unfortunately, this definition of equivalence at first sight is not effective: how can we decide if there is a unimodular $R \in \mathbf{Z}^{s \times s}$ with $B = A[R]$? The theory of spinor genera ([1, chapter 11]) for indefinite forms in principle gives an effective method for deciding if or not such R exists, whereas for definite forms it is easy to give a bound on such R which reduces deciding equivalence to a finite number of tests. Here we are concerned with such an explicit version of this problem: write $||A||$ for the maximum norm of a $s \times s$-matrix A, so $\|A\| = \max_{1 \leqslant i,j \leqslant s} |a_{ij}|$ (and analogously for vectors), and let $H = \max\{\|A\|, \|B\|\}$. Then Siegel [**8**] established a *search bound* for equivalence of two symmetric $A, B \in \mathbf{Z}^{s \times s}$ of the following kind: if there is a unimodular $R \in \mathbf{Z}^{s \times s}$ with $B = A[R]$, then there is one with $\|R\| \leqslant \Lambda_s(H)$ for a function $\Lambda_s(H)$ (the search bound) depending only on s and H. Clearly this allows one to decide whether A and B are integrally equivalent or not by testing a finite number of possible R's. Furthermore, if such R exists this algorithm also allows one to get hold of it (for another approach to decide solvability of quadratic Diophantine equations see [**3**]). However, Siegel's bound when made explicit turns out to be very large: in [**9**, Hauptsatz 5·4] it was shown that Siegel's method gives

$$\Lambda_s(H) = \exp\left(C_1(s)|\det A|^{\frac{s^3+s^2}{2}}\right) H^{\frac{s^3-s^2}{2}}$$

for a constant $C_1(s)$ depending only on s. So for fixed s this bound grows exponentially in H since generally $|\det A|$ is of order of magnitude H^s. For binary forms this is not too far from the truth as shown by the following result.

THEOREM 1. *There are positive constants C_2 and C_3 such that there are infinitely many non-singular symmetric $A, B \in \mathbf{Z}^{2\times 2}$ with the following property: there is a unimodular $R \in \mathbf{Z}^{2\times 2}$ with $B = A[R]$, but there is no such R with*

$$\|R\| < C_2\, 2^{C_3(\|A\|+\|B\|)^{1/2}}.$$

This result is closely connected to the exponential growth of fundamental solutions of Pell's equation and for this reason might not be too surprising. In the ternary case the situation changes completely. In the author's recent work on small solutions of quadratic Diophantine equations ([**2**, theorem 4]) the following bound for ternary quadratic forms was established.

THEOREM 2. *Let $A, B \in \mathbf{Z}^{3\times 3}$ be symmetric and non-singular, and suppose that there is a unimodular $R \in \mathbf{Z}^{3\times 3}$ with $B = A[R]$. Then there is such R with*

$$\|R\| \ll_\epsilon |\det A|^{162+\epsilon}(\|A\| + \|B\|)^{231+\epsilon}.$$

So in the ternary case a bound holds that is polynomial in $H = \max\{\|A\|, \|B\|\}$. Masser ([**6**, conjecture on page 252]) conjectured that for all $s \geqslant 3$ a polynomial bound in H is possible. Polynomial search bounds for quadratic Diophantine equations which have been established by different means for $s \geqslant 4$ ([**2**, **5**]) would then easily follow via reduction theory, so in some sense the equivalence problem for quadratic forms seems to be the most fundamental one in this context. Unfortunately, the method applied to prove Theorem 2 made use of some specific properties of ternary quadratic forms and cannot readily be generalized to higher dimensions. By appealing to a different method we can inductively extend Theorem 2 to forms in more variables satisfying an extra condition on their determinant. So for a large class of quadratic forms we are able to confirm Masser's conjecture.

THEOREM 3. *Let $A, B \in \mathbf{Z}^{s\times s}$ be symmetric and non-singular, where $s \geqslant 4$, and suppose that* det *A is cube-free, not divisible by four and that not all coefficients on the diagonal of A are even. Furthermore, suppose that there is a unimodular $R \in \mathbf{Z}^{s\times s}$ with $B = A[R]$. Then there is such R with*

$$\|R\| \leqslant \begin{cases} C_4 H^{9900}|\det A|^{27200} & \text{when } s = 4 \\ C_5 H^{500000}|\det A|^{1540000} & \text{when } s = 5 \\ C_6(s) H^{(4(s+5))^s}|\det A|^{(5(s+9))^s} & \text{when } s \geqslant 6. \end{cases}$$

The constants C_4, C_5, and C_6 are effectively computable.

2. *A lower bound for binary forms*

In this section we will give a short proof of Theorem 1. Let H be sufficiently large. Then it follows from the proof of theorem 2 in [**4**] that there are non-zero integers a, b with $|a|, |b| \leqslant H$ such that every integer solution (x, y) of the binary quadratic equation

$$ax^2 + by^2 = -1 \tag{2·1}$$

has $|x| + |y| \geqslant 2^{H/5}$, and there is at least one solution. Now let (x_0, y_0) be any integer solution of (2·1). Clearly x_0 and y_0 are coprime. Write

$$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

By the arguments leading to [**2**, lemma 24] it is easily proved that there is a unimodular $R \in \mathbf{Z}^{2\times 2}$ with first column $(x_0, y_0)^T$ and $\|A[R]\| \ll |\det A| \ll H^2$. Note that $B : = A[R]$ has $b_{11} = -1$ by construction of R. Now let R' be any unimodular integral 2×2-matrix with $B = A[R']$. Then the first column $(x, y)^T$ of R' gives a solution of (2·1). However, (2·1) has no integer solution (x, y) with $|x| + |y| < 2^{H/5}$. Therefore,

$$||R'|| \geqslant C_2(|x| + |y|) \geqslant C_2\, 2^{H/5} \geqslant C_2\, 2^{C_3(||A||+||B||)^{1/2}} \tag{2·2}$$

for suitable positive constants C_2 and C_3. Hence there are infinitely many $A, B \in \mathbf{Z}^{2\times 2}$ which are integrally equivalent, but every unimodular $R' \in \mathbf{Z}^{2\times 2}$ with $B = A[R']$ satisfies (2·2). This completes the proof of Theorem 1.

3. *Preliminary lemmata*

Before proving Theorem 3 we first have to collect some auxiliary results on quadratic forms. Our first lemma yields a bound on the smallest integer solution of a quadratic Diophantine equation, provided there is an integer solution at all.

LEMMA 1. *Let $A \in \mathbf{Z}^{s\times s}$ be symmetric and non-singular, where $s \geqslant 4$. Furthermore, let $\boldsymbol{\xi} \in \mathbf{Z}^s$, and let $\kappa \in \mathbf{Z}\backslash\{0\}$ and $\eta \in \mathbf{N}$. Then if there is any solution $\mathbf{x} \in \mathbf{Z}^s$ to the equation*

$$A[\mathbf{x}] = \kappa; \ \ \mathbf{x} \equiv \boldsymbol{\xi} \pmod{\eta},$$

then there is one with

$$\|\mathbf{x}\| \ll \begin{cases} |\kappa|^{1+\epsilon}\eta^{11+\epsilon}\|A\|^{10+\epsilon}|\det A|^{12+\epsilon} & \text{for } s = 4 \\ \eta^{(3s-2)/(s-4)+\epsilon}\|A\|^{(s^2-3s+2)/(s-4)+\epsilon}|\det A|^{(3s+1)/(s-4)+\epsilon} & \\ \quad \times \max\{|\kappa|^{1/2}, \eta\} & \text{for } s \geqslant 5. \end{cases}$$

Proof. This follows from [**2**, proposition 1] on using the estimate $\Theta \ll \eta^{s-1}$.

Our next result gives an effective description of the method of ‘completing the square’ for writing a quadratic form as the sum of a square and a quadratic form in one variable less.

LEMMA 2. *Let $A \in \mathbf{Z}^{s\times s}$ be of the form*

$$A = \begin{pmatrix} n & \mathbf{c}^T \\ \mathbf{c} & C \end{pmatrix}$$

with $n \in \{-1, 1\}$, $\mathbf{c} \in \mathbf{Z}^{s-1}$ and symmetric $C \in \mathbf{Z}^{(s-1)\times(s-1)}$, and let $I \in \mathbf{Z}^{(s-1)\times(s-1)}$ be the identity matrix. Then

$$R = \begin{pmatrix} 1 & -n^{-1}\mathbf{c} \\ \mathbf{0} & I \end{pmatrix} \tag{3·1}$$

is unimodular such that $A[R]$ *is of the form*

$$A[R] = \begin{pmatrix} n & \mathbf{0}^T \\ \mathbf{0} & D \end{pmatrix}$$

for some symmetric $D \in \mathbf{Z}^{(s-1)\times(s-1)}$ *with* $\|D\| \ll \|C\| + \|\mathbf{c}\|^2$.

Proof. We have

$$A[\mathbf{X}] = n(X_1 + n^{-1}(c_1X_2 + \cdots + c_{s-1}X_s))^2 + D[X_2, \ldots, X_s]$$

for a suitable symmetric $D \in \mathbf{Z}^{(s-1)\times(s-1)}$ with $\|D\| \ll \|C\| + \|\mathbf{c}\|^2$. Hence by using the unimodular transformation $\mathbf{Y} = T\mathbf{X}$ where

$$T = \begin{pmatrix} 1 & n^{-1}\mathbf{c} \\ \mathbf{0} & I \end{pmatrix}$$

we conclude that $A[T^{-1}\mathbf{Y}] = nY_1^2 + D[Y_2, \ldots, Y_s]$. Since $T^{-1} = R$ with R given by (3·1), we immediately obtain the conclusion of the lemma.

4. *Local conditions*

In this section we collect conditions on a quadratic form $Q \in \mathbf{Z}[X_1, \ldots, X_s]$ making sure that Q represents 1 and -1 over $\mathbf{Z}$. When p is a rational prime we write $\mathbf{Z}_p$ for the ring of p-adic integers. As is well known (see [**1**, theorem 1·5 in chapter 9]), a sufficient condition for Q to represent an integer n over $\mathbf{Z}$ is that $s \geqslant 4$, that Q is non-singular and indefinite and that Q represents n over $\mathbf{Z}_p$ for all primes p. So our aim is to find conditions on Q forcing Q to represent 1 and -1 over $\mathbf{Z}_p$. As usual in the quadratic forms business, the case $p \neq 2$ is much easier.

LEMMA 3. *Let p be an odd prime, let* $s \geqslant 4$, *and let* $Q \in \mathbf{Z}[X_1, \ldots, X_s]$ *be a quadratic form with* $p^3 \nmid \det Q$. *Then Q represents both* 1 *and* -1 *over* $\mathbf{Z}_p$.

Proof. Quadratic forms over $\mathbf{Z}_p$ can be diagonalized (see [**1**, theorem 3·1, chapter 8]), so we may assume that Q is of the form $Q(X_1, \ldots, X_s) = a_1X_1^2 + \cdots + a_sX_s^2$ for suitable $a_1, \ldots, a_s \in \mathbf{Z}_p$. Since the diagonalization of Q did not change the property $p^3 \nmid \det Q$ we may by $s \geqslant 4$ without loss of generality suppose that $p \nmid a_1a_2$. Now it is well known (see for example [**7**, §92]) that in this case $a_1X_1^2 + a_2X_2^2$ represents over $\mathbf{Z}_p$ all p-adic units, in particular 1 and -1, and the conclusion of the lemma immediately follows by setting the other variables $x_3, \ldots, x_s$ to zero.

In the case of $p = 2$ a more complicated condition on the quadratic form is needed. We write $2 \mid Q$ when all the coefficients on the diagonal of a matrix representing Q are even. This property clearly does not change under unimodular transformations and is equivalent to Q only representing even numbers. Analogously, we write $2 \nmid Q$ if not all coefficients on the diagonal of Q are even.

LEMMA 4. *Let* $Q \in \mathbf{Z}[X_1, \ldots, X_s]$ *be a classically integral quadratic form where* $s \geqslant 4$. *Furthermore, suppose that* $2 \nmid Q$ *and that* $4 \nmid \det Q$. *Then Q represents both* 1 *and* -1 *over* $\mathbf{Z}_2$.

Proof. If Q satisfies the hypotheses of the lemma then $-Q$ also does. Hence it suffices to prove that Q represents 1 over $\mathbf{Z}_2$. Though it may be impossible to diagonalize Q over $\mathbf{Z}_2$, there is an ‘almost diagonal’ form $\mathbf{Z}_2$-equivalent to Q. To be more precise, by [**1**, lemma 4·1, chapter 8] there is an $T \in \mathbf{Z}_2^{s\times s}$ with odd determinant such that $Q' := Q[T]$ is a sum of forms of the types $2^a(X^2 + XY + Y^2)$, $2^b XY$, and cX^2. Here a and b are positive integers, and c is of the form $c = 2^r t$ with $r \in \mathbf{Z}$, $r \geqslant 0$ and $t \in \{1, 3, 5, 7\}$. Now $\det Q' \equiv \det Q \cdot (\det T)^2 \equiv \det Q \pmod 8$, so $4 \not| \det Q'$. Moreover, $2 \not| Q'$ since $2 \not| Q$. Hence Q' must belong to one of the following types of forms:

$$\begin{aligned}
Q_1(X_1, \ldots, X_s) &= aX_1^2 + bX_2^2 + cX_3^2 + dX_4^2 + Q_1'(X_5, \ldots, X_s),\\
Q_2(X_1, \ldots, X_s) &= aX_1^2 + dX_2^2 + 2\big(X_3^2 + X_3X_4 + X_4^2\big) + Q_2'(X_5, \ldots, X_s),\\
Q_3(X_1, \ldots, X_s) &= aX_1^2 + 2X_2X_3 + Q_3'(X_4, \ldots, X_s),\\
Q_4(X_1, \ldots, X_s) &= aX_1^2 + 2\big(X_2^2 + X_2X_3 + X_3^2\big) + 2\big(X_4^2 + X_4X_5 + X_5^2\big)\\
&\quad + Q_4'(X_6, \ldots, X_s),
\end{aligned}$$

where $a, b, c \in \{1, 3, 5, 7\}$, $d \in \{1, 2, 3, 5, 6, 7\}$ and Q_1', Q_2', Q_3', and Q_4' are suitable quadratic forms. Note that we can skip the possibilities $d = 10$ or $d = 14$ because in the following we are working modulo 8. We will now show that in each possible case Q_i and therefore $Q = Q_i[T^{-1}]$ represents 1 over $\mathbf{Z}_2$. To this end, by Hensel's lemma it suffices to show that the congruence

$$Q_i(x_1, \ldots, x_s) \equiv 1 \pmod 8 \tag{4·1}$$

has a solution with $4 \not| \nabla Q_i(x_1, \ldots, x_s)$.

Case I. $Q' = Q_1$: First suppose that one of a, b, c, d is 1, say $a = 1$. Then $x_1 = 1$, $x_2 = \cdots = x_s = 0$ does the job. Next suppose that one of a, b, c, d is 5, say $a = 5$. Then $a + 4b \equiv 1 \pmod 8$ since b is odd, so we may take $x_1 = 1$, $x_2 = 2$, and $x_3 = \cdots = x_s = 0$. So we may assume that $a, b, c \in \{3, 7\}$ and that $d \in \{2, 3, 6, 7\}$. If three of the numbers a, b, c, d are 3, say $a = b = c = 3$, then we set $x_1 = x_2 = x_3 = 1$, $x_4 = \cdots = x_s = 0$. If one of the numbers a, b, c, d is 3 and two are 7, say $a = 3$ and $b = c = 7$, then again we may take $x_1 = x_2 = x_3 = 1$ and $x_4 = \cdots = x_s = 0$. When two of the three numbers a, b, c are 3, one is 7, say $a = b = 3$, $c = 7$, and d is 2, then $(x_1, \ldots, x_s) = (0, 0, 1, 1, 0, \ldots, 0)$ is a solution of (4·1) with $4 \not| \nabla Q_4(x_1, \ldots, x_s)$. If two of the three numbers a, b, c are 3, one is 7, say $a = b = 3$, $c = 7$, and d is 6, then we may take $(x_1, \ldots, x_s) = (1, 0, 0, 1, 0, \ldots, 0)$. For $a = b = c = 7$ and $d = 2$ we set $x_1 = x_4 = 1$, $x_2 = x_3 = x_5 = \cdots = x_s = 0$, and for $a = b = c = 7$ and $d = 6$ we take $x_1 = x_4 = 1$, $x_2 = 2$, $x_3 = x_5 = \cdots = x_s = 0$. Finally, if $a = b = c = d = 7$, which is the last remaining possibility, then we set $x_1 = 2$, $x_2 = x_3 = x_4 = 1$ and $x_5 = \cdots = x_s = 0$.

Case II. $Q' = Q_2$: Since the forms $aX_1^2 + 2(X_3^2 + X_3X_4 + X_4^2)$ and $a(3X_1^2 - X_3^2 - X_4^2)$ are $\mathbf{Z}_2$-equivalent (see [**1**, page 118, formula (4·8)]), we are immediately reduced to Case I.

Case III. $Q' = Q_3$: Here $x_1 = x_2 = 1$, $x_3 = 5 - (a + 1)/2$, $x_4 = \cdots = x_s = 0$ is a solution of (4·1).

Case IV. $Q' = Q_4$: Since the forms $2(X_2^2 + X_2X_3 + X_3^2) + 2(X_4^2 + X_4X_5 + X_5^2)$ and $2X_2X_3 + 2X_4X_5$ are $\mathbf{Z}_2$-equivalent (see [**1**, page 118, formula (4·9)]), this case immediately reduces to Case III.

The following lemma will prove useful when 'completing the square' in order to obtain a form in one variable less still not having only even coefficients on the diagonal.

LEMMA 5. *Let $Q \in \mathbf{Z}[X_1, \ldots, X_s]$ be a classically integral quadratic form with $s \geqslant 5$, $2 \nmid Q$ and $4 \nmid \det Q$. Let $n \in \{-1, 1\}$. Then there is an $T \in \mathbf{Z}_2^{s \times s}$ with $2 \nmid \det T$ such that $Q[T]$ is of the form*

$$Q[T] = \begin{pmatrix} n & \mathbf{0} \\ \mathbf{0} & R \end{pmatrix}$$

where $R \in \mathbf{Z}_2^{(s-1)\times(s-1)}$ has $2 \nmid R$.

Proof. Our aim is to find a quadratic form Q' which is $\mathbf{Z}_2$-equivalent to Q and which is of the form

$$Q'(X_1, \ldots, X_s) = nX_1^2 + R(X_2, \ldots, X_s) \qquad (4\cdot2)$$

where $2 \nmid R$. We first show that such Q' (possibly with $2 \mid R$) exists: Since Q represents n over $\mathbf{Z}_2$ by Lemma 4, we may find a form Q' which is $\mathbf{Z}_2$-equivalent to Q and which is of the form

$$Q'(X_1, \ldots, X_s) = nX_1^2 + 2X_1L(X_2, \ldots, X_s) + M(X_2, \ldots, X_s)$$

where L is a linear and M is a quadratic form. By completing the square (compare Lemma 2) we then arrive at the shape (4·2). Note that $4 \nmid \det Q$ implies that $4 \nmid \det Q'$. If $2 \nmid R$, then we are done so let us suppose that $2 \mid R$. Then by using [**1**, lemma 4·1, chapter 8] and replacing R by an $\mathbf{Z}_2$-equivalent form if necessary we may assume that R is a sum of forms of the type $2X^2$, $6X^2$, $10X^2$, $14X^2$, $2^a(X^2+XY+Y^2)$, and 2^bXY where $a, b \in \{1, 2, 3, \ldots\}$. Clearly all a and all b are 1 because of $4 \nmid \det Q'$. Moreover, for the same reason at most one form of type $2X^2$, $6X^2$, $10X^2$, or $14X^2$ is possible. Since $s \geqslant 5$ and by [**1**, page 118, formula (4·9)], the forms

$$(2X^2 + 2XY + 2Y^2) + (2Z^2 + 2ZW + 2W^2)$$

and

$$2XY + 2ZW$$

are $\mathbf{Z}_2$-equivalent, we may assume that R is of the form

$$R(X_2, \ldots, X_s) = 2X_2X_3 + R'(X_4, \ldots, X_s)$$

for a suitable quadratic form $R' \in \mathbf{Z}_2[X_4, \ldots, X_s]$. Now by [**1**, p. 118, formula (4·7)], the forms

$$nX_1^2 + 2X_2X_3$$

and

$$nX_1^2 + X_2^2 - X_3^2$$

are $\mathbf{Z}_2$-equivalent. So finally we arrive at a form Q' being $\mathbf{Z}_2$-equivalent to Q and of the shape (4·2) with $2 \nmid R$.

By injecting Lemma 3 and Lemma 4 in [**1**, theorem 1·5, chapter 9] we obtain the following result, which is crucial for our investigation.

Lemma 6. *Let $Q \in \mathbf{Z}[X_1, \ldots, X_s]$ be an indefinite classically integral quadratic form where $s \geqslant 4$, and let $n \in \{-1, 1\}$. Suppose further that* $\det Q$ *is cubefree, not divisible by four, and that $2 \not| Q$. Then there is an $\mathbf{x} \in \mathbf{Z}^s$ with $Q[x] = n$. Moreover, the following approximation property holds true: if $\mathbf{y} \in \mathbf{Z}_2^s$ is any solution of $Q[\mathbf{y}] = n$, then there is $\mathbf{x} \in \mathbf{Z}^s$ with $Q[\mathbf{x}] = n$ and $\mathbf{x} \equiv \mathbf{y} \pmod 2$.*

5. *Genera of indefinite quadratic forms*

Let $Q_1, Q_2 \in \mathbf{Z}[X_1, \ldots, X_s]$ be two non-singular classically integral quadratic forms given by (1·1). Then Q_1 and Q_2 are in the same genus if and only if they are real-equivalent and $\mathbf{Z}_p$-equivalent for every rational prime p. Fortunately, this infinite collection of conditions can be captured by one congruence condition as shown by the following lemma.

Lemma 7. *Let $Q_1, Q_2 \in \mathbf{Z}[X_1, \ldots, X_s]$ be two classically integral quadratic forms given by* (1·1). *Suppose that Q_1 and Q_2 are real-equivalent, that Q_1 and Q_2 have the same determinant $\Delta \neq 0$, and that*

$$A \equiv B \pmod{4|\Delta|}.$$

Then Q_1 and Q_2 are in the same genus.

Proof. This is [**1**, lemma 4·3, chapter 9].

Unfortunately, there is generally no local-global principle for integral equivalence of quadratic forms: two forms Q_1, Q_2 may be in the same genus, thus locally equivalent everywhere, but not integrally equivalent. However, under some extra conditions a local-global principle holds.

Lemma 8. *Let $Q_1 \in \mathbf{Z}[X_1, \ldots, X_s]$ be an indefinite classically integral quadratic form where $s \geqslant 3$. Furthermore, suppose that* $\det Q_1$ *is cubefree and not divisible by four. Then every classically integral quadratic form $Q_2 \in \mathbf{Z}[X_1, \ldots, X_s]$ in the same genus than Q_1 is integrally equivalent to Q_1.*

Proof. This follows from [**1**, theorem 1·5, chapter 11].

Note that we again meet the restriction to cubefree determinant in a key lemma. The other constraint to indefinite forms is unimportant for our application, because search bounds in the definite case are easily established by elementary methods.

6. *Local-global for unimodular matrices*

As a further 'local-global tool' we need an approximation result for unimodular matrices. We start with some preparation.

Lemma 9. *Let $s \geqslant 2$, let $\eta \in \mathbf{N}$, and let $\mathbf{x} \in \mathbf{Z}^s$ be a vector such that p does not divide all x_i $(1 \leqslant i \leqslant s)$ for all primes p dividing η. Then there is a primitive vector $\mathbf{r} \in \mathbf{Z}^s$ with* $\mathbf{r} \equiv \mathbf{x} \pmod \eta$ *and $\|\mathbf{r}\| \ll \eta^2$.*

Proof. Clearly without loss of generality we may assume that $\|\mathbf{x}\| \ll \eta$. Let $r_i = x_i$ $(2 \leqslant i \leqslant s)$. It is our aim to choose r_1 in such a way that $r_1 \equiv x_1 \pmod \eta$ and $r_1 \ll \eta^2$. Let d be the greatest common divisor of $r_2, \ldots, r_s$. Then $d \ll \max_{2 \leqslant i \leqslant s} |r_i| \ll \eta$. It is possible to choose $a \in \mathbf{N}$ such that $x_1 + a\eta$ is coprime to d: let p be a prime divisor of d. If $p \mid x_1$, then by hypothesis $p \not| \eta$, so $x_1 + a\eta$ is not for all $a \in \mathbf{N}$ divisible by p. If $p \not| x_1$, then again $x_1 + a\eta$ cannot always be divisible by p. So by the Chinese remainder theorem, there is an $a \in \mathbf{N}$ such that $x_1 + a\eta$ is coprime to d, and clearly there is such a with $a \leqslant d \ll \eta$. Then setting $r_1 = x_1 + a\eta$ we conclude that $\mathbf{r}$ is primitive, $\mathbf{r} \equiv \mathbf{x} \pmod{\eta}$, and $\|\mathbf{r}\| \ll \eta^2$.

We are now ready to state and prove the main result of this section.

LEMMA 10. *Let η be a positive integer, and let $R \in \mathbf{Z}^{s\times s}$ have*

$$|\det R| \equiv 1 \pmod{\eta}. \qquad (6{\cdot}1)$$

Moreover, let $\mathbf{y}_1$ be the first column of R and let $\mathbf{r} \in \mathbf{Z}^s$ be a primitive vector with

$$\mathbf{r} \equiv \mathbf{y}_1 \pmod{\eta}. \qquad (6{\cdot}2)$$

Then there is a unimodular $R' \in \mathbf{Z}^{s\times s}$ with $R' \equiv R \pmod{\eta}$, first column $\mathbf{r}$ and

$$||R'|| \ll ||\mathbf{r}||\eta^{2(s-1)}. \qquad (6{\cdot}3)$$

Proof. We will prove the lemma by induction on s. The base case $s = 1$ of the induction is trivial, so let us assume that $s \geqslant 2$ and that the lemma has already been proved for $s-1$. By Lemma 1 in [5] there is an unimodular $T \in \mathbf{Z}^{s\times s}$ with first column $\mathbf{r}$ and

$$||T|| \ll ||\mathbf{r}||. \qquad (6{\cdot}4)$$

However, T need not satisfy the imposed congruence condition $T \equiv R \pmod{\eta}$, so we use column operations on T to achieve this. Write $T = (\mathbf{r}\,\mathbf{x}_2 \cdots \mathbf{x}_s)$ for column vectors $\mathbf{x}_i \in \mathbf{Z}^s$ $(2 \leqslant i \leqslant s)$. Since T is unimodular, there are integers a_{ij} $(2 \leqslant i \leqslant s, 1 \leqslant j \leqslant s)$ such that

$$M := \left(\mathbf{r}, a_{21}\mathbf{r} + \sum_{i=2}^{s} a_{2i}\mathbf{x}_i, \ldots, a_{s1}\mathbf{r} + \sum_{i=2}^{s} a_{si}\mathbf{x}_i\right) \equiv R \pmod{\eta}. \qquad (6{\cdot}5)$$

Clearly, we may suppose that

$$|a_{ij}| \leqslant \eta \ (2 \leqslant i \leqslant s, 1 \leqslant j \leqslant s). \qquad (6{\cdot}6)$$

Moreover,

$$\det M = d \det(\mathbf{r}\,\mathbf{x}_2 \ldots \mathbf{x}_s) = d \det T \qquad (6{\cdot}7)$$

where

$$d = \begin{vmatrix} a_{22} & \ldots & a_{2s} \\ \vdots & & \vdots \\ a_{s2} & \ldots & a_{ss} \end{vmatrix}.$$

Now $|\det T| = 1$ because T is unimodular. Hence (6·1), (6·5) and (6·7) yield $|d| \equiv 1 \pmod{\eta}$. In particular, the vector $(a_{22} \cdots a_{s2})^T$ satisfies the hypothesis of Lemma 9. Thus there is a primitive $\mathbf{p} \in \mathbf{Z}^{s-1}$ with $\mathbf{p} \equiv (a_{22} \cdots a_{s2})^T \pmod{\eta}$ and $||\mathbf{p}|| \ll \eta^2$. Using the induction hypothesis for $s-1$, we find an unimodular matrix $U \in \mathbf{Z}^{(s-1)\times(s-1)}$ with

$$U = \begin{pmatrix} u_{22} & \ldots & u_{2s} \\ \vdots & & \vdots \\ u_{s2} & \ldots & u_{ss} \end{pmatrix} \equiv \begin{pmatrix} a_{22} & \ldots & a_{2s} \\ \vdots & & \vdots \\ a_{s2} & \ldots & a_{ss} \end{pmatrix} \pmod{\eta} \qquad (6{\cdot}8)$$

and

$$||U|| \ll \eta^2\, \eta^{2(s-2)} = \eta^{2(s-1)}. \tag{6·9}$$

Let

$$R' := \left(\mathbf{r}, a_{21}\mathbf{r} + \sum_{i=2}^{s} u_{2i}\mathbf{x}_i, \ldots, a_{s1}\mathbf{r} + \sum_{i=2}^{s} u_{si}\mathbf{x}_i\right). \tag{6·10}$$

Then like in (6·7), $\det R' = \det U \det T$, so R' again is unimodular. Moreover, $R' \equiv R$ (mod η) by (6·2), (6·5), (6·8) and (6·10). Finally, (6·4), (6·6), (6·9) and (6·10) give the bound (6·3). This finishes the proof of the lemma.

7. *Proof of Theorem* 3

Our proof of Theorem 3 will be by induction on the number of variables s, Theorem 2 being the induction hypothesis at the beginning. So we shall now assume the theorem to be proved for $s - 1 \geqslant 3$ in order to prove it for s in place of $s - 1$. Let $R_1 \in \mathbf{Z}^{s\times s}$ be unimodular with $B = A[R_1]$. If A is definite, then [**5**, lemma 10] immediately gives the bound $|R_1\| \ll \|A\|^{(s-1)/2}||B||^{1/2}$, which is much better than the bound claimed in Theorem 3, so we may assume that A (and hence B) is indefinite. Write (p, q) for the signature of A, which is also the signature of B, p counting the number of positive eigenvalues and q counting the number of negative ones. By assumption, $p \geqslant 1$ and $q \geqslant 1$. We define n to be 1 if $p \geqslant q$ and -1 otherwise. Consequently, if one eigenvalue having the same sign than n is removed, the remaining eigenvalues still belong to an indefinite quadratic form. This observation will be important later. We now distinguish two cases.

Case I. $s = 4$: In this case we note that by Lemma 6 the number n is represented by A over $\mathbf{Z}$. Thus by Lemma 1 there is a necessarily primitive $\mathbf{x} \in \mathbf{Z}^s$ with $A[x] = n$ and

$$\|\mathbf{x}\| \ll \begin{cases} H^{10+\epsilon}|\det A|^{12+\epsilon} & \text{for } s = 4 \\ H^{(s^2-3s+2)/(s-4)+\epsilon}|\det A|^{(3s+1)/(s-4)+\epsilon} & \text{for } s \geqslant 5 \end{cases} \tag{7·1}$$

where we have put $H = \|A\| + \|B\|$. We apply [**5**, lemma 1] to find a unimodular $R_2' \in \mathbf{Z}^{s\times s}$ with first row $\mathbf{x}$ and $\|R_2'\| \leqslant \|\mathbf{x}\|$. We finish our observations in Case I by setting $R_2 = R_2'^T$.

Case II. $s \geqslant 5$: In this case we first note that by Lemma 5 there is a $T \in \mathbf{Z}_2^{s\times s}$ such that $A[T]$ is of the form

$$A[T] = \begin{pmatrix} n & \mathbf{0}^T \\ \mathbf{0} & R \end{pmatrix} \tag{7·2}$$

where $2\ \not|\, R$. In particular, $A[\mathbf{t}] = n$ where $\mathbf{t} \in \mathbf{Z}_2^s$ is the first column of T. Hence by Lemma 1 and Lemma 6 there is a necessarily primitive $\mathbf{x} \in \mathbf{Z}^s$ with $A[\mathbf{x}] = n, \mathbf{x} \equiv \mathbf{t} \pmod 2$ and satisfying the bound (7·1). Using Lemma 10 we obtain an unimodular $R_2 \in \mathbf{Z}^{s\times s}$ with first column $\mathbf{x}$, bounded above by $||R_2|| \ll ||\mathbf{x}||$ and satisfying

$$R_2 \equiv T \pmod 2. \tag{7·3}$$

By (7·2) and (7·3) we have

$$A[R_2] \equiv \begin{pmatrix} n & \mathbf{0}^T \\ \mathbf{0} & \tilde{R} \end{pmatrix} \pmod 2 \tag{7·4}$$

for a symmetric matrix $\tilde{R} \in \mathbf{Z}^{(s-1)\times(s-1)}$ with $2 \not| \tilde{R}$. This finishes Case II. We resume the general path of proof by noting that in both cases R_2 has first column $\mathbf{x}$ and

$$\|R_2\| \ll \|\mathbf{x}\|. \tag{7·5}$$

Let

$$A' = A[R_2], \tag{7·6}$$

then

$$A' = B\big[R_1^{-1}R_2\big] \tag{7·7}$$

and $a'_{11} = n$, because $A[\mathbf{x}] = n$ and $\mathbf{x}$ is the first column of R. Writing $\mathbf{y}$ for the first column of $R_1^{-1}R_2$, we conclude that $B[\mathbf{y}] = n$. Let

$$\eta = 4|\det A|. \tag{7·8}$$

We again apply Lemma 1 to obtain a $\mathbf{z} \in \mathbf{Z}^s$ with $B[\mathbf{z}] = n$,

$$\mathbf{z} \equiv \mathbf{y} \pmod{\eta}$$

and

$$\|\mathbf{z}\| \ll \begin{cases} H^{10+\epsilon}|\det A|^{23+\epsilon} & \text{for } s = 4 \\ H^{(s^2-3s+2)/(s-4)+\epsilon}|\det A|^{(7s-5)/(s-4)+\epsilon} & \text{for } s \geqslant 5 \end{cases} \tag{7·9}$$

(note that $\det B = \det A$). Since $n \in \{-1, 1\}$, the vector $\mathbf{z}$ must be primitive. Using Lemma 10 we get a unimodular R_3 with first column $\mathbf{z}$,

$$R_3 \equiv R_1^{-1}R_2 \pmod{\eta} \tag{7·10}$$

and

$$\|R_3\| \ll \|\mathbf{z}\|\eta^{2(s-1)}. \tag{7·11}$$

Let

$$B' = B[R_3], \tag{7·12}$$

then $b'_{11} = n$, and by (7·7) and (7·10) we have

$$B' \equiv B\big[R_1^{-1}R_2\big] \equiv A' \pmod{\eta}. \tag{7·13}$$

Clearly both A' and B' satisfy the hypothesis of Lemma 2, so by applying this lemma we find unimodular R_4, R_5 in $\mathbf{Z}^{s\times s}$ with

$$R_4 \equiv R_5 \pmod{\eta}, \tag{7·14}$$

$$\|R_4\| \ll \|A'\|, \ \|R_5\| \ll \|B'\| \tag{7·15}$$

and

$$A'' := A'[R_4] = \begin{pmatrix} n & \mathbf{0}^T \\ \mathbf{0} & C \end{pmatrix}, \ B'' := B'[R_5] = \begin{pmatrix} n & \mathbf{0}^T \\ \mathbf{0} & D \end{pmatrix} \tag{7·16}$$

for some symmetric $C, D \in \mathbf{Z}^{(s-1)\times(s-1)}$ with

$$\|C\| \ll \|A'\|^2, \ \|D\| \ll \|B'\|^2. \tag{7·17}$$

Now $|\det C| = |\det A|$ and $|\det D| = |\det B|$, so both C and D have cubefree determinant since the same is true for A and B. For the same reason both $\det C$ and $\det D$ are not divisible by 4. Moreover, by (3·1), (7·4) and (7·6) we know that $2 \nmid C$ for $s \geqslant 5$. Furthermore, by construction of n the symmetric matrices C and D belong to indefinite quadratic forms which are real-equivalent, and clearly $\det C = \det D$. In addition, by (7·13), (7·14) and (7·16) we obtain $A'' \equiv B'' \pmod{\eta}$. In particular, $C \equiv D \pmod{\eta}$. Using (7·8) and Lemma 7, we conclude that C and D are in the same genus of quadratic forms. So all the assumptions of Lemma 8 are satisfied, and consequently there is a unimodular $R_6 \in \mathbf{Z}^{(s-1)\times(s-1)}$ with $C = D[R_6]$. By applying our induction hypothesis for $s - 1$ in place of s, we may assume that R_6 is bounded by

$$\|R_6\| \ll \begin{cases} |\det A|^{162+\epsilon}(\|C\| + \|D\|)^{231+\epsilon} & \text{when } s = 4 \\ |\det A|^{27200}(\|C\| + \|D\|)^{9900} & \text{when } s = 5 \\ |\det A|^{(5(s+8))^{s-1}} & \\ \quad \times(\|C\| + \|D\|)^{(4(s+4))^{s-1}} & \text{when } s \geqslant 6. \end{cases} \tag{7·18}$$

Note that the bound for $s = 6$ corresponds to the case $s = 5$ of Theorem 3, which may be bounded above by setting $s = 5$ in the case $s \geqslant 6$. Let

$$R_7 = \begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & R_6 \end{pmatrix}. \tag{7·19}$$

Then clearly $R_7 \in \mathbf{Z}^{s\times s}$ is unimodular with $\|R_7\| = \|R_6\|$ and

$$B''[R_7] = A''. \tag{7·20}$$

Let $R_8 = R_3 R_5 R_7 R_4^{-1} R_2^{-1}$. Then by (7·6), (7·12), (7·16) and (7·20) we have $B[R_8] = A$. Moreover, R_8 is unimodular with

$$\|R_8\| \ll \|R_3\|\,\|R_5\|\,\|R_7\|\,\left\|R_4^{-1}\right\|\,\left\|R_2^{-1}\right\|. \tag{7·21}$$

We now have to bound the terms on the right-hand side of (7·21). First, by (7·8), (7·9) and (7·11) we have

$$\|R_3\| \ll \begin{cases} H^{10+\epsilon}|\det A|^{29+\epsilon} & \text{when } s = 4 \\ H^{12+\epsilon}|\det A|^{38+\epsilon} & \text{when } s = 5 \\ H^{s+4+\epsilon}|\det A|^{20+2(s-1)} & \text{when } s \geqslant 6. \end{cases} \tag{7·22}$$

Next, (7·12), (7·15) and (7·22) give

$$\|R_5\| \ll \|B'\| \ll \|B\|\,\|R_3\|^2 \ll \begin{cases} H^{21+\epsilon}|\det A|^{58+\epsilon} & \text{when } s = 4 \\ H^{25+\epsilon}|\det A|^{76+\epsilon} & \text{when } s = 5 \\ H^{2s+9+\epsilon}|\det A|^{40+4(s-1)} & \text{when } s \geqslant 6. \end{cases} \tag{7·23}$$

Let us now bound $\|R_7\|$, which gives the main contribution. Using (7·5), (7·6) and (7·17) we obtain

$$\|C\| \ll \|A'\|^2 \ll \|A\|^2\,\|R_2\|^4 \ll H^2\|\mathbf{x}\|^4.$$

Similarly, by (7·11), (7·12) and (7·17) we have

$$\|D\| \ll \|B'\|^2 \ll \|B\|^2\|R_3\|^4 \ll H^2\left(\|\mathbf{z}\|\eta^{2(s-1)}\right)^4.$$

Hence

$$\begin{aligned} \|C\| + \|D\| &\ll H^2\left(\|\mathbf{x}\| + \|\mathbf{z}\|\eta^{2(s-1)}\right)^4 \\ &\ll \begin{cases} H^{42+\epsilon}|\det A|^{116+\epsilon} & \text{when } s = 4 \\ H^{50+\epsilon}|\det A|^{152+\epsilon} & \text{when } s = 5 \\ H^{4(s+5)}|\det A|^{8(s+9)} & \text{when } s \geqslant 6 \end{cases} \end{aligned}$$

by (7·1), (7·8) and (7·9). Thus (7·18) and (7·19) give

$$\|R_7\| = \|R_6\| \ll \begin{cases} |\det A|^{26958+\epsilon} H^{9702+\epsilon} & \text{when } s = 4 \\ |\det A|^{1532000+\epsilon} H^{495000+\epsilon} & \text{when } s = 5 \\ H^{4^s(s+5)(s+4)^{s-1}} & \\ \quad \times |\det A|^{5^{s-1}(s+8)^{s-1}+2(s+9)4^s(s+4)^{s-1}} & \text{when } s \geqslant 6. \end{cases} \tag{7·24}$$

Furthermore, by (7·1), (7·5), (7·6), (7·15) and Cramer's rule

$$\begin{aligned} \left\|R_4^{-1}\right\| &\ll \|R_4\|^{s-1} \ll \|A'\|^{s-1} \ll \|A\|^{s-1}\,\|R_2\|^{2(s-1)} \\ &\ll H^{s-1}\|\mathbf{x}\|^{2(s-1)} \\ &\ll \begin{cases} H^{63+\epsilon}|\det A|^{72+\epsilon} & \text{when } s = 4 \\ H^{100+\epsilon}|\det A|^{128+\epsilon} & \text{when } s = 5 \\ H^{2(s-1)(s+5)}|\det A|^{20(s-1)} & \text{when } s \geqslant 6. \end{cases} \end{aligned} \tag{7·25}$$

In the same way, Cramer's rule and (7·5) give

$$\begin{aligned} ||R_2^{-1}|| &\ll ||R_2||^{s-1} \\ &\ll \begin{cases} H^{30+\epsilon}|\det A|^{36+\epsilon} & \text{when } s = 4 \\ H^{48+\epsilon}|\det A|^{64+\epsilon} & \text{when } s = 5 \\ H^{(s-1)(s+4)+\epsilon}|\det A|^{10(s-1)} & \text{when } s \geqslant 6. \end{cases} \end{aligned} \tag{7·26}$$

Inserting (7·22)–(7·26) in (7·21), we obtain

$$\|R_8\| \ll \begin{cases} H^{9827}|\det A|^{27154} & \text{when } s = 4 \\ H^{500000}|\det A|^{1540000} & \text{when } s = 5 \\ H^{4^s(s+5)^s}|\det A|^{5^s(s+9)^s} & \text{when } s \geqslant 6. \end{cases}$$

So R_8 is unimodular, has $B[R_8] = A$ and satisfies the bound claimed in the theorem.

REFERENCES

[1] J. W. S. CASSELS. *Rational Quadratic Forms* (Academic Press, London, 1978).

[2] R. DIETMANN. Small solutions of quadratic Diophantine equations. *Proc. London Math. Soc.* **86** (2003), 545–582.

[3] F. GRUNEWALD and D. SEGAL. How to solve a quadratic equation in integers. *Math. Proc. Camb. Phil. Soc.* **89** (1981), 1–5.

[4] D. M. KORNHAUSER. On the smallest solution to the general binary quadratic equation. *Acta Arith.* **55** (1990), 83–94.

[5] D. M. KORNHAUSER. On small solutions of the general nonsingular quadratic Diophantine equation in five and more unknowns. *Math. Proc. Camb. Phil. Soc.* **107** (1990), 197–211.

[6] D. W. MASSER. Search bounds for Diophantine equations. *A Panorama of Number Theory or the View from Baker's Garden* (Zürich, 1999), 247–259.

[7] O. T. O'MEARA. *Introduction to Quadratic Forms*. Reprint of the 1973 edition. Classics in Mathematics (Springer-Verlag, 2000).

[8] C. L. SIEGEL. Zur Theorie der quadratischen Formen. *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* (1972), 21–46.

[9] S. STRAUMANN. Das Äquivalenzproblem ganzer quadratischer Formen: Einige explizite Resultate. Diplomarbeit. Universität Basel (1999).