An algorithm for computing genera of ternary and quaternary quadratic forms

Rainer Schulze-Pillot

Appeared in:
Proceedings of the Int. Symp. on Symbolic and Algebraic Computation Bonn 1991

Introduction

This is a preliminary report on an algorithm for computing genera of ternary and quaternary positive definite quadratic forms over $\mathbb{Z}$.

It is well known that due to the simple shape of the reduction conditions in these dimensions [Mi1, Ca] it is in principle no problem to compute representatives of all classes of such quadratic forms whose discriminant is below a given bound. This has been done by hand in the ternary case for half- discriminant up to 1000 by Brandt and Intrau [BI], for quaternaries see [Ge, To]. It is, however, sometimes desirable to be able to quickly determine representatives of all classes in some fixed genus of quadratic forms of possibly high discriminant without having to generate along the way all forms of smaller discriminant.

An obvious attempt in such a case is to use Kneser's method of neighbouring or adjacent lattices [Kn1] that has proved to be useful for the construction of unimodular lattices in "middle" dimensions like 24 and 32 [Ni, CS, KV]. This report intends to draw attention to the fact that it is indeed not difficult to use this method in dimensions 3 and 4 as the basis of an algorithm that serves our purpose. With almost no extra work one obtains at the same time the "adjacency graph" of the classes determined; this has interesting arithmetic and graph theoretic (see Sect. 1) applications.

In Section 1 we collect some basic facts and notations from the theory of quadratic forms and explain the method of neighbouring lattices.

The very simple algorithm based on this method is described in Section 2 where one also sees which difficulties arise in higher dimensions. We intend to use our algorithm for the experimental investigation of the Fourier and Fourier-Jacobi coefficients of certain linear combinations of Siegel theta series of quaternary quadratic forms; this is still in progress. The underlying problems from the theory of modular forms which were our starting point for this project are briefly sketched in Section 3.

The $C-$programs for the implementation of our algorithm are not included, they can be obtained from the author. I want to thank Britta Habdank who, for the ternary case, translated into C and completed a part of the program which I had originally written in Pascal, Dirk Tubbesing who wrote the program for unique reduction in dimension 3 after Dickson [Di] and a test for equivalence in the quaternary case, and R. Scharlau who supported these works within his project on constructive methods in the theory of quadratic forms.

1 Neighbouring lattices

Let V be an m-dimensional vector space over $\mathbb{Q}$, let $Q : V \to \mathbb{Q}$ a non-degenerate quadratic form with associated bilinear form

$$B(x, y) = 1/2(Q(x + y) - Q(x) - Q(y)),$$

$L = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_m$ a $\mathbb{Z}$-lattice on V of full rank and assume $B(L, L) \subseteq \mathbb{Z}$. The lattice L is then called integral, it is even (type II) if $Q(L) \subseteq 2\mathbb{Z}$, odd (type I) otherwise.

Two lattices L, L' are isometric (or in the same class) if there is a linear isomorphism from L onto L' preserving Q, they belong to the same genus if their p-adic completions L_p, L'_p are isometric for all p. For the notion of spinor genus see [OM, Sect. 102].

Let $A = (B(e_i, e_j))$ be the Gram matrix of $\mathbb{Q}$ relative to the basis $e_1, \ldots, e_m$ of L, put $d(L) = \det A$. If Q has Gram matrix B with respect to some basis $e'_1, \ldots, e'_m$ of some lattice L' on V then L and L' are isometric if and only if there is $T \in GL_m(\mathbb{Z})$ with $T'AT = B$, in which case A and B are called equivalent.

The dual lattice of L is $L^{\#} = \{x \in V | B(x, L) \subseteq \mathbb{Z}\}$, one has $(L^{\#} : L) = d(L)$. One calls L unimodular or self-dual if $L^{\#} = L$.

M. Kneser introduced in [Kn1] the following method for constructing integral lattices L' on V with $d(L') = d(L)$:
Let $p \not| d(L)$ be a prime, $x \in L$ with $p^2 | Q(x)$ and $p^{-1}x \notin L$. Put $L_x = \{y \in L | B(x,y) \in p\mathbb{Z}\} = L \cap (\mathbb{Z}\frac{x}{p} + L)^{\#}$, put $L' = \mathbb{Z}\frac{x}{p} + L_x$.
L' is then called a p-neighbour of(p-adjacent to) L and one has

(i) $d(L') = d(L)$

(ii) *L' is integral*

(iii) *L' is even if and only if L_x is even and $Q(x) \in 2p^2\mathbb{Z}_p$, i.e., if and only if either L is even and $Q(x) \in 2p^2\mathbb{Z}_p$ or L is odd, $p = 2$ and L_x is equal to the even sublattice $L^\circ := \{y \in L | Q(y) \in 2\mathbb{Z}\}$ of L.*

(iv) *L and L' are in the same genus if and only if they are either both even or both odd.*

These properties are well known, see [OM, Sect. 106] and [Kn1]. Properties i) – iii) are immediate consequences of the fact that one has $B(x, L) \supseteq d(L)\mathbb{Z}$ for primitive x (which follows from $(L^{\#} : L) = d(L)$) and hence $(L : L_x) = p = (L' : L_x)$ holds. Property iv) follows from i) – iii) since L' differs from L only in the completion at p and a unimodular lattice over $\mathbb{Z}_p$ is determined (up to isometry) by dimension, discriminant, and type (see e.g. [CS,Ch. 15]).

We list some further properties of the construction. These are certainly not new, but the available references list only small portions of them.

(v) *If $p \| d(L)$ then i) – iv) are also true.*

This is true because one can then write $L_p = \mathbb{Z}_p z \perp K$ with $Q(z) \in p\mathbb{Z}_p^\times$ and unimodular K. If one had $L_x = L$, then $x = \alpha z + x'$ with $x' \in K$ divisible by p and $Q(x) \in p^2\mathbb{Z}_p$ would imply $\alpha \in p\mathbb{Z}_p$ which contradicts $p^{-1}x \notin L$. As above this shows i) – iii). iv) is clear if either L and L' are both even or $p \neq 2$ since in that case L_p and L'_p are $\mathbb{Z}_p$-maximal lattices in Eichler's sense and hence [E2, Satz 9.6] isometric; in the remaining case one can check it with the help of [CS, Ch. 15, Th. 10].

(vi) *Let $x_1, x_2 \in L$ be as above, L_1 and L_2 the respective neighbouring lattices. Then for $p \neq 2$ one has $L_1 = L_2$ if and only if $\mathbb{Z}x_1 + pL = \mathbb{Z}x_2 + pL$. For $p = 2$ one certainly has $L_1 = L_2$ if $\mathbb{Z}x_1 + 4L = \mathbb{Z}x_2 + 4L$. More precisely, if $p = 2$ and L is even, then $L_1 = L_2$ if and only if $Q(x_1) \equiv Q(x_2)$ mod 8 and $\mathbb{Z}x_1 + 2L = \mathbb{Z}x_2 + 2L$. If $p = 2$ and L is odd, assume x_1 and x_2 to be such that $gcd(Q(x_i), 8) \geq gcd(Q(x'), 8)$ for all $x' \in \mathbb{Z}x_i + 2L^\circ$ with $x' \notin 2L$ $(i = 1, 2)$.*
Then again $L_1 = L_2$ if and only if $\mathbb{Z}x_1 + 2L^\circ = \mathbb{Z}x_2 + 2L^\circ$, and all neighbours L' of L can be obtained in this way.

The assertions for $p \neq 2$ and for even L are obvious. For the rest, fix some $x \in L$ and consider $x' = \alpha x + 2z$ for $z \in L$, α odd. If $z \in L^\circ$ then $Q(x') \equiv Q(x) + 4B(x, z)$ mod 8, whereas for $z \in L_x$ one has $Q(x') \equiv Q(x) + 4Q(z)$ mod 8. This shows that $Q(x') \equiv Q(x)$ mod 8 for all $x' \in \mathbb{Z}x + 2L^\circ$ (or $x' \in \mathbb{Z}x + 2L_x$), $x' \notin 2L$, if and only if $L_x = L^\circ$. We notice next that obviously (x_1, x_2 arbitrary) $L_1 = L_2$ if and only if $\mathbb{Z}x_1 + 2L_{x_1} = \mathbb{Z}x_2 + 2L_{x_2}$. Thus if $L' = \mathbb{Z}\frac{x}{2} + L_x$ is a neighbour of L and $\gcd(Q(x), 8)$ is not maximal in $\mathbb{Z}x + 2L^\circ$, then $L^\circ \neq L_x$ and we can replace x by $x' = x + 2z$ with $z \in L_x, z \notin L^\circ$ satisfying $8 | Q(x')$, and we see that indeed all neighbours of L can be constructed using a vector x with $\gcd(Q(x), 8)$ maximal in $\mathbb{Z}x + 2L^\circ$. If now x_1, x_2 are such that $\gcd(Q(x_i), 8)$ is maximal in $\mathbb{Z}x_i + 2L^\circ$ $(i = 1, 2)$, assume first $L_1 = L_2$. Then $x_1 = \alpha x_2 + 2z$ with α odd, $z \in L_{x_2}$. If $z \notin L^\circ$, then $L_{x_2} = L_{x_1} \neq L^\circ$ and the maximality of x_1, x_2 implies $8 | Q(x_i)$ $(i = 1, 2)$, in contradiction to $z \notin L^\circ$. Hence $z \in L_{x_2} \cap L^\circ$ and therefore $\mathbb{Z}x_1 + 2L^\circ = \mathbb{Z}x_2 + 2L^\circ$. If we assume on the other hand $\mathbb{Z}x_1 + 2L^\circ = \mathbb{Z}x_2 + 2L^\circ$ we conclude in the same way $\mathbb{Z}x_1 + 2L_{x_1} = \mathbb{Z}x_2 + 2L_{x_2}$, hence $L_1 = L_2$.

(vii) *If p is odd and $p \not| d(L)$ then $\mathbb{Z}x + pL$ contains p-primitive vectors x' with $Q(x') \in p^2\mathbb{Z}p$ if and only if $Q(x) \in p\mathbb{Z}$. One finds such an x' by choosing $y \in L$ with $B(x, y) = a \notin p\mathbb{Z}$ (e.g. a suitable vector of an arbitrary basis of L), solving the congruence $2\alpha a \equiv \frac{-Q(x)}{p}$ mod p and putting $x' = x + \alpha p y$. If $p = 2$ then $\mathbb{Z}x + 2L^\circ$ contains 2-primitive vectors x' with $Q(x') \in 4\mathbb{Z}$ if and only if $Q(x) \in 4\mathbb{Z}$. If $Q(x) \in 4\mathbb{Z}$ and $L_x \neq L^\circ$ one finds $x' \in \mathbb{Z}x + 2L^\circ$ with $8 | Q(x')$ by choosing $y \in L^\circ$ with $B(x, y)$ odd and putting $x' = x \pm 2y$.*

The two final points are concerned with the question which classes in the genus of L are obtained by successive construction of neighbours.

(viii) *By successive construction of p-neighbouring lattices one obtains all lattices on V of the same discriminant as L which lie in $\mathbb{Z}[\frac{1}{p}]L$. For $p \neq 2$ these lattices are all in the same genus as L. For $p = 2$ and even L one obtains all lattices in the genus of L that are in $\mathbb{Z}[\frac{1}{2}]L$ if one constructs neighbours only with vectors x satisfying $Q(x) \in 8\mathbb{Z}$.*

To see this let $K \subseteq \mathbb{Z}[\frac{1}{p}]L$ with $d(K) = d(L)$, let $(L : L \cap K) = p^r = (K : L \cap K)$ (the indices are equal because of $d(L) = d(K)$). Choose $x' \in K, x' \notin L$, then $p^s x' =: x$ is p-primitive for some $s \in N$ (since by the elementary divisor theorem one has $aK \subseteq L$ for some $a \in \mathbb{N}$). Let $L' = \mathbb{Z}\frac{x}{p} + L_x$ be the neighbour of L constructed from x, then $L' \cap K \supsetneq L \cap K$, $\quad L' \cap K \neq L \cap K$ since $p^{s-1}x' = \frac{x}{p}$ is in $L' \cap K$ but not in $L \cap K$. Hence $(L' : L' \cap K) < (L : L \cap K)$, and iterating this one can connect L and K by a chain of lattices p-neighbouring to each other. Obviously, if $p = 2$ and L and K are even then the same is true for all lattices in the chain and all the vectors used in the construction have length divisible by 8. As noted in iv) the construction of neighbours does not leave the genus except if $p = 2$ and one changes the parity (type) of the lattice. We note at this occasion that K can be constructed as a neighbouring lattice of L if and only if $(L : L \cap K) = (K : K \cap L) = p$, in particular being neighbours is a symmetric relation.

(ix) *If the genus of L consists only of one spinor genus [OM, Sect. 102], the rank m is at least 3 and the completion V_p is isotropic (i.e., there is $0 \neq y \in V_p$ with $Q(y) = 0$) then successive construction of p-neighbouring lattices yields representatives of all classes of lattices in the genus of L.*

If $p = 2$ one can also obtain representatives of the (unique) genus of L containing the 2-neighbours of L whose type (parity) is different from that of L.

The condition that the genus of L should contain only one spinor genus is in particular satisfied if no odd prime divides $d(L)$ to the power $\frac{m(m-1)}{2}$ and if 2 does not divide $d(L)$ to the power

$$\begin{cases} \frac{(3m-2)(m-1)}{2} & \text{if } m \text{ is odd} \\ \frac{m(3m-5)}{2} & \text{if } m \text{ is even.} \end{cases}$$

Our general condition $p^2 \not| d(L)$ implies that V_p is isotropic for odd p, if or $m \geq 4$, for $p = 2$ if L is even or $m \geq 5$. If $m = 3$ and p is odd, V_p is certainly isotropic if $p \not| d(L)$.

The first part of ix) can be found in [Kn1] for $p = 2$, it follows in the same way for arbitrary p. One should notice that it depends on the strong approximation theorem [Kn2, E1] which can be applied only if V_p is isotropic.

The bounds for the power, to which primes may divide $d(L)$ are from [Kn3] (odd p) and [EH] ($p = 2$). The remarks on the isotropy of V_p can easily be checked using the classification of unimodular p-adic lattices [OM, Sect. 92, 93].

If the genus of L happens to contain more than one spinor genus, one can reach (starting from L) the other spinor genera in the genus with the neighbouring lattice construction by carefully selecting some special primes and constructing an arbitrary neighbour of L at each of these primes. Successive construction of p-neighbours of all these lattices for some arbitrary p with $p^2 \not| d(L)$ then gives all classes in the genus of L. We do not go into details here but refer to [BH].

To finish this section we remark that by viii) we can use our construction to define a graph whose vertices are the lattices in $\mathbb{Z}[\frac{1}{p}]L$ of the same discriminant as L (or in the same genus as L), with two lattices joined by an edge if they are neighbours of each other. For $m = 3$ and $p = 2$ or $p \not| d(L)$ this graph is a tree and has been studied in [SP1]. If one identifies isometric lattices and introduces loops and multiple edges, one obtains a finite multigraph, where the multiplicities of the edges are given by Eichler's Anzahlmatrices [E2]. The multigraph obtained for $m = 3$ is closely connected with the "Ramanujan graphs" which recently found much interest in connection with applications in combinatorics and network theory [Pi2, LPS]. We plan to deal with this aspect of the neighbouring lattice construction in another place.

2 The algorithm

We are now going to describe our algorithm, doing this as far as possible for general $m \geq 3$. We assume that the genus of L has only one spinor genus and that $p \neq 2$ or L is even. The necessary modifications for $p = 2$

and L odd can be performed using vi), vii) of Sect. 1 and are left to the reader. We first choose a prime p with $p^2 \not| d(L)$, if $m = 3$ and p is odd we require (because of ix)) even $p \not| d(L)$.

The algorithm has the following main steps (which we will analyze more closely below):

Algorithm (Construct forms in a fixed genus)

Input: An integral positive definite symmetric $m \times m$-matrix A ($m \geq 3$) (Gram-matrix of a lattice L as above) and a prime p as above

Output: A list of Gram matrices of a set of representatives of the classes in the genus of $(\mathbb{Z}^m, x'Ax)$.

Step 1: Replace A by an equivalent reduced matrix, open a list of matrices with A as first element

Step 2: Put $(L, Q) = (\mathbb{Z}^m, x'Ax)$, find the classes $\mathbb{Z}x + pL$ in L/pL which contain p-primitive $x \in L$ with $Q(x) \in 2p^2\mathbb{Z}_p$ and in each class one such x.

Step 3: For each x from step 2 determine a reduced Gram-matrix B_x of the neighbouring lattice $\mathbb{Z}\frac{x}{p} + L_x$; mark A.

Step 4: For each B_x from step 3 compare B_x with the matrices in the list. If B_x is equivalent to a matrix already in the list, take the next B_x. If not, add B_x to the list.

Step 5: If the list contains no unmarked element, terminate. Otherwise let C be the first unmarked matrix, put $A \leftarrow C$, go to step 2.

Of course these steps need some explanation.

Steps 1 and 5: The bookkeeping for the list is conveniently organized using pointers. It turns out to be useful to organize it in two different ways:

Once with pointers pointing to the matrix that has been generated next (this is the order used in step 5), once ordered by some concept of size (e.g., lexicographic order of the diagonal) (this order is useful for the comparison operations of step 4). For the meaning of "reduced" see step 4.

Step 2: This is done using vii) of Sect. 1 by going through the lines in L/pL ($L/2L^\circ$ for $p = 2$). If such a (nonzero) line is represented by x' with $Q(x') \in p\mathbb{Z}$ ($Q(x') \in 4\mathbb{Z}$ for $p = 2$) one can replace it by x representing the same line and satisfying $Q(x) \in p^2\mathbb{Z}$ ($Q(x) \in 8\mathbb{Z}$ for $p = 2$) by the procedure given in vii). The required vector $y \in L$ with $B(x', y) \notin p\mathbb{Z}$ can be chosen to be one of the basis vectors of L; in case $p \neq 2$ and $p|d(L)$ it can happen that $B(x', L) \subseteq p\mathbb{Z}$, in this case there is no primitive vector $x \in \mathbb{Z}x' + pL$ with $Q(x) \in p^2\mathbb{Z}$. Since the number of lines $\neq 0$ in L/pL is $(p^m - 1)/(p - 1)$ this procedure obviously becomes impractical for large m. If L happens to have a large group of automorphisms one can reduce the work by running only through a set of representatives of the orbits under this group. However, it is firstly difficult to control this a priori (without precise knowledge of the lattice and its group) in an algorithmic way, and secondly, in some sense "most" lattices have trivial automorphism group [Bi, Ba]. For this reason the neighbouring lattice method has been used so far for large m only for clever construction by hand of all (in the case of big automorphism group) or some neighbouring lattices.

The number of classes $\mathbb{Z}x + pL$ that are suitable for the method is in case $p \not| d(L)$ or $p = 2$ and m odd given by [Kn4, Sect. 12]:

$$\begin{cases} (p^{m-1} + p^{m/2} - p^{m/2-1} - 1)/(p-1) & m \text{ even, } \left(\frac{(-1)^{m/2}d(L)}{p}\right) = 1 \\ (p^{m-1} - p^{m/2} + p^{m/2-1} - 1)/(p-1) & m \text{ even, } \left(\frac{(-1)^{m/2}d(L)}{p}\right) = -1 \\ (p^{m-1} - 1)/(p-1) & m \text{ odd} \end{cases}$$

and is hence of the order p^{m-2}.

Step 3: Here we have the task of determining a basis $\{e'_i = \sum_{j=1}^{m} t_{ji} e_j\}$ of the neighbouring lattice $\mathbb{Z}\frac{x}{p} + L_x$ ($\{e_i\}$ a basis of L), this gives then $B_x = T'AT$. This basis can be determined using the modified LLL-algorithm ($MLLL$) [PZ, p. 209]: One first finds a basis of $\mathbb{Z}\frac{x}{p} + L$, the dual basis of this is a basis of $(\mathbb{Z}\frac{x}{p} + L)^\#$. Using the elementary divisor algorithm[PZ, 180ff] one finds a basis of $L_x = L \cap (\mathbb{Z}\frac{x}{p} + L)^\#$ and another application of $MLLL$ gives the required basis of $L = \mathbb{Z}\frac{x}{p} + L_x$. In the case $p = 2$, L even (which we have implemented) one can proceed more directly. Following the procedure from vi), vii) of Sect. 1 the vectors x found in step 2 all have at least one coordinate $= \pm 1$, hence can be exchanged for one of the basis vectors. If the new basis of L is $\{e_1, \ldots, e_{m-1}, x\}$, then $\{e_1, \ldots, e_{m-1}, \frac{x}{2}\}$ is a basis of $\mathbb{Z}\frac{x}{2} + L$, and one has $L' = \mathbb{Z}\frac{x}{2} \oplus K$ where

$$K = \{y \in \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_{m-1} | B(x, y) \in 2\mathbb{Z}\}.$$

A basis of K can be determined by a simple distinction of cases, taking account of the parities of the $B(x, e_i)$ $(i = 1, \ldots, m-1)$, which gives the desired basis of L'.
Step 4: This step contains the main practical difficulty in the algorithm because it is in general quite time consuming to decide whether two given Gram matrices A and B are equivalent. In dimensions 3 and 4 we can improve on the general method of [Poh] by making use of reduction theory. Let us describe our method in more detail:
Recall that a basis $\{e_1, \ldots, e_m\}$ of L is called (Minkowski-) reduced if one has for $1 \leq j \leq m$:

$$Q(e_j) = \min\{Q(y) | y = \sum_{i=1}^{m} \alpha_i e_i \text{ with } \gcd(\alpha_j, \ldots, \alpha_m) = 1\}$$

[Mi2, vdW, Ca], the corresponding Gram matrix is then also called Minkowski reduced. For $m \leq 4$ one has in addition [Mi1, Ca]:
If $\{e_1, \ldots, e_m\}$ is not reduced then there exists $y = \sum\limits_{i=1}^{m} \alpha_i e_i$ with $\alpha_i \in \{0, \pm 1\}$ and $Q(y) < Q(e_i)$ for some i with $\alpha_i = \pm 1$. That is, by running through all vectors with coordinates $0, \pm 1$ one can transform any given basis into a Minkowski reduced basis in finitely many steps.
This gives first the following
Algorithm (Minkowski-reduction)
Input: A positive definite integral symmetric $(m \times m)$-matrix A $(m \geq 4)$
Output: A Minkowski reduced matrix equivalent to A.
Step 1: For $j = m, \ldots, 1$: (put $\alpha_j = 1, \alpha_{j+1}, \ldots, \alpha_m = 0$,

```
for $\alpha_{j-1} = -1, 0, 1$
⋮
for $\alpha_1 = -1, 0, 1$
(put $y = \sum_{i=1}^{m} \alpha_i e_i$,
if $Q(y) < Q(e_j)$ then
($T = E_m, t_{ij} \leftarrow y_i \quad (i = 1, \ldots, m)$,
$A \leftarrow T'AT$, go to step 1)))
```

Step 2: Terminate, output A.
Observe that Minkowski reduction is not unique, i.e., we can have Minkowski reduced matrices $A \neq B$ which are equivalent. However [vdW, Ca], if A, B are Minkowski reduced in dimension ≤ 4, the diagonal coefficients are equal to the successive minima and hence $a_{ii} \neq b_{ii}$ for some i implies that A and B are not equivalent. For $m = 3$ one can prescribe additional constraints on the off-diagonal coefficients that make reduction unique; such constraints have been given by Dickson [Di, p. ...], who at the same time shows how to obtain this unique normal form from a given Minkowski reduced matrix. Using Dickson's method our test for equivalence in dimension 3 is then simply a test for equality of the Dickson reduced matrices.
In dimension 4 one does not seem to know such a unique normal form which can be determined in a straightforward algorithmic way, e.g. by exchanging one basis vector at a time as we did for Minkowski reduction; some criteria for inequivalence and some examples of equivalent Minkowski reduced matrices can be found in [Ge].
We tried the following method to reduce the matrix further:
Algorithm (off diagonal reduction)
Input: A Minkowski reduced 4×4-matrix A
Output: A matrix equivalent to A with small sum of the absolute values of the off diagonal coefficients, small maximal absolute value of the off diagonal coefficients, nonnegative last row, minus signs as far left and up as possible.

Step 1: For $j = 4, \dots, 1$

```
$\{\alpha_j \leftarrow 1, \alpha_{j+1} \leftarrow 0, \dots, \alpha_m \leftarrow 0;$
For $\alpha_{j-1} = -1, 0, 1$
$\vdots$
For $\alpha_1 = -1, 0, 1$
$\{y \leftarrow \sum_{i=1}^{4} \alpha_i e_i;$
If $Q(y) = Q(e_j)$ and
$\left( \sum_{\substack{i=1\\i\neq j}}^{4} |B(y, e_i)| < \sum_{\substack{i=1\\i\neq j}}^{4} |a_{ij}| \right.$
or $\left( \sum_{\substack{i=1\\i\neq j}}^{4} |B(y, e_i)| = \sum_{\substack{i=1\\i\neq j}}^{4} |a_{ij}| \right.$
 and $\left. \left. \max_{i\neq j} |B(y, e_i)| < \max_{i\neq j} |a_{ij}| \right) \right)$
$\{T \leftarrow E_4; t_{ij} \leftarrow y_i \quad (i = 1, \dots, 4);$
$A \leftarrow T'AT;$ go to step 1$\}\}\}$.
```

Step 2: Order A by the following critera (in order of their priority, by changing the order of the basis vectors of L).

a) $i \leq j \Rightarrow a_{ii} \leq a_{jj}$

b) $i \leq j \Rightarrow \sum_{\substack{k=1\\k\neq i}}^{4} |a_{ik}| \leq \sum_{\substack{k=1\\k\neq j}}^{4} |a_{jk}|$

c) For $k = 4, \dots, 2$: If $i \leq j$, $|a_{il}| = |a_{jl}|$ for $l = k+1, \dots, 4$, then $|a_{ik}| \leq |a_{jk}|$

Step 3: Order the signs in A by the following criteria (in order of their priority, by setting $e_i \leftarrow -e_i$ for some basis vectors e_i of L and by changing the order of the basis vectors e_i of L):

a) $a_{i4} \geq 0 \quad (i = 1, \dots, 3)$

b) $a_{ij} \geq 0 \quad (i = 1, \dots, 4)$ if $a_{i,j+1} = \dots = a_{i4} = 0 \quad (j = 3, \dots, 1)$

c) $a_{23} \geq 0$ (if this is possible without violating 2 or 3a), 3b)).

Step 4: Output A

The reduction obtained seems to be remarkably close to being unique. For example, we used our algorithm to compute all classes in the genus of quaternary quadratic forms of discriminant 389^2 and level 389; this genus has 319 classes by known results from the theory of quaternion algebras. Using the reduction described above and a test for equality of the reduced matrices as equivalence test the algorithm produced only 10 Gram matrices that were in fact equivalent to other matrices in the list.

On the basis of our experience we propose hence the following test for equivalence in dimension 4 (which worked without excessive use of computing time in our examples):

Algorithm (test for equivalence)

Input: Two positive definite integral symmetric (4×4)-matrices

Output: *eq* or *ineq*

Step 1: Reduce A and B by Minkowski reduction

Step 2: If $a_{ii} \neq b_{ii}$ for some i terminate, output *ineq*

Step 3: Reduce A and B further using off diagonal reduction

Step 4: If $A = B$ terminate, output *eq*

Step 5: Test for equivalence by brute force, i.e., by searching for vectors $x_1, \ldots, x_4 \in \mathbb{Z}^4$ with $x_i' A x_j = b_{ij}$. The vectors $x \in \mathbb{Z}^4$ with $x'Ax \leq b_{44}$ can be found relatively fast using (e.g.) the algorithm from [PZ, p. 190] (this has been programmed for our purpose by Dirk Tubbesing)

It is not difficult to see that our algorithm produces large numbers of equivalent matrices. Most of these already become equal after our reduction procedure and are therefore caught in step 4. On the other hand only a relatively small percentage of the inequivalent matrices agrees in the diagonal coefficients after Minkowski reduction, so that inequivalence is usually detected in step 2. Thus, the relatively time consuming step 5 is not invoked too often.

In further experiments it may prove useful to add between step 4 and 5 one or more of the following inequivalence tests:

a) If $a_{22} < a_{33}$, test the upper left 2×2 blocks of A and B for equivalence

b) If $a_{33} < a_{44}$, test the upper left 3×3 blocks of A and B for equivalence

c) Determine the level N of the genus (the common denominator of the entries of A^{-1} for any A in the genus), test whether
$$r(A, n) \neq r(B, n) = \#\{x \in \mathbb{Z}^4 | x'Bx = n\}$$
for some $n < \frac{1}{6} N \prod\limits_{p|N} (1 + \frac{1}{p})$.

a) and b) have been proposed in [Ge], if they give inequivalence, A and B are certainly inequivalent. Also $r(A, n) \neq r(B, n)$ for some n in step c) certainly proves inequivalence. If these representation numbers are equal for all $n < \frac{1}{6} N \prod\limits_{p|N} (1 + \frac{1}{p})$, then by [He, p. 811] the theta series of degree 1 of both quadratic forms agree. This seems to happen very rarely in dimension 4; examples have only very recently been found [Schi, Shi].

3 Motivation

The motivation for setting up this algorithm comes from [BS, SP]. In these articles we investigated linear combinations of theta series of quaternary integral quadratic forms attached to ideals in definite quaternion algebras. Recall that for an integral positive definite lattice (L, Q) as in Sect. 1 the theta series of degree r is defined as

$$\begin{aligned} \vartheta^{(r)}(L, Q, Z) &= \sum_{(x_1, \ldots, x_r) \in L^r} \exp\left(2\pi i \text{ trace } ((\frac{1}{2} B(x_i, x_j)) Z\right) \\ &= \sum_{T \geq 0} r(L, Q, T) \exp\left(2\pi i \text{ trace } TZ\right), \end{aligned}$$

where $Z \in \mathfrak{H}_r = \{X + iY \in M_r^{sym}(\mathbb{C}) | Y \text{ pos. definite } \}$, $T \in M_r^{sym}(\frac{1}{2}\mathbb{Z})$ is positive semidifinite and $r(L, Q, T) = \#\{(x_1, \ldots, x_r) \in L^r | \frac{1}{2} B(x_i, x_j) = T_{ij}\}$.

In particular we could completely characterize the linear dependence relations between the theta series of degree 2 of the classes in the genus of even quaternary quadratic forms of level q and discriminant q^2 for a prime q. The first q for which such relations occur is $q = 389$.

If $\sum\limits_{i=1}^{H} \alpha_i \vartheta^{(2)}(L_i, Q_i, Z) = 0$ is such a nontrivial linear relation then a theorem of Kitaoka [Ki] implies that $\sum\limits_{i=1}^{H} \alpha_i \vartheta^{(3)}(L_i, Q_i, Z) \neq 0$ and one has reason to suspect that the Fourier coefficients of this modular form of degree 3 satisfy interesting relations, possibly those of Yamazaki [Ya] for forms in the generalized Maa"s space. We have however not been able to prove that such relations do indeed hold.

To check for them, the first step obviously is to obtain a set of representatives of the classes in the genus, the discriminant 389^2 being far out of the range of all existing tables. It will require further work to determine the linear dependencies explicitly and check the Fourier coefficients in question. Algorithms for the computation of these classes (more precisely, of the underlying ideals in the quaternion algebra considered) have been developed by Pizer and by Shiota [Pi1, Shi], however, they produce along the way large numbers of useless lattices belonging to other genera of other discriminants and levels. Our algorithm needed 41 seconds of CPU time on a decsystem 3100 workstation for the computation of all 319 classes in this genus and 4 seconds for the determination of a genus of 28 classes. It thus seems to behave roughly linear in the number of classes to be computed, which is the expected value as long as all coefficients are in the range of single precision. One representative of each genus described above can easily be written down as follows (so that we can start our algorithm) [Pi1, Prop. 5.2.]:

$q \equiv 3 \bmod 4$

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & \frac{1+q}{2} & 0 & 0 \\ 0 & 0 & \frac{1+q}{2} & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

$q \equiv 5 \bmod 8$

$$\begin{pmatrix} \frac{3+q}{4} & 1 & 1 & 0 \\ 1 & \frac{3+q}{2} & 2 & q \\ 1 & 2 & 4 & 0 \\ 0 & q & 0 & 2q \end{pmatrix}$$

$q \equiv 1 \bmod 8$

$$\begin{pmatrix} \frac{1+p}{2} & 0 & \alpha & 1 \\ 0 & \frac{q+pq}{2} & -q & 0 \\ \alpha & -q & \frac{2\alpha^2+2q}{p} & 0 \\ 1 & 0 & 0 & 2 \end{pmatrix}$$

where p is a prime, $p \equiv 3 \bmod 4$, $(\frac{p}{q}) = -1$, $\alpha^2 \equiv -q \bmod p$.

The number H of proper classes (i.e., classes up to isometry with determinant $+1$) in these genera can be determined as follows:

The number h of classes of ideals in the definite quaternion algebra over $\mathbb{Q}$ of discriminant q that have a fixed maximal left order is given by [Vi, p. 152]

$$h = \frac{q-1}{12} + \frac{1}{4}(1 - (\frac{-4}{q})) + \frac{1}{3}(1 - (\frac{-3}{q})),$$

the number of types of maximal orders in that quaternion algebra by [Vi, p. 152]

$$t = \frac{1}{2}\left[(1 - (\frac{-4}{q})) + \beta h(-q)\right]$$

where

$$\beta = \begin{cases} 1 & q \equiv -1 \bmod 4 \\ 2 & q \equiv 7 \bmod 8 \text{ or } q = 3 \\ 4 & q \equiv 3 \bmod 8, q \neq 3 \end{cases}$$

and $h(-q)$ is the number of ideal classes in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-q})$.

By [Pon] the number of proper classes in the genus is then given by $t^2 + (h-t)^2$; this can also be proved in an elementary way using the description of isometries between ideal classes from [BS, Sect. 5] or [Shi]. In the same way the number of classes is then seen to be $\dfrac{t^2 + (h-t)^2 + h}{2}$.

References:

[Ba] E. Bannai: Positive definite unimodular lattices with trivial automorphism group, Memoirs of the AMS 429 (1990)

[Bi] J. Biermann: Gitter mit kleiner Automorphismengruppe in Geschlechtern von $\mathbb{Z}$-Gittern mit positiv definiter quadratischer Form, Dissertation G"ottingen 1981

[BH] J.W. Benham, J.S. Hsia: Spinor equivalence of quadratic forms, J. of Number Th. 17, 337-342 (1983)

[BS] S. B"ocherer, R. Schulze-Pillot: Siegel modular forms and theta series attached to quaternion algebras, Preprint 1989 (Preprint Nr. A89-16 FU Berlin)

[BI] H. Brandt, O. Intrau: Tabellen reduzierter positiver tern"arer quadratischer Formen, Abh. S"achs. Akad. Wiss. Math.-Nat. Kl. 45 (1958)

[Ca] J.W.S. Cassels: Rational Quadratic Forms, London ... 1978. Academic Press

[CS] J.H. Conway, N.J.A. Sloane: Sphere Packings, Lattices and Groups, New York ... 1988. Springer

[Di] L.E. Dickson: Theory of Numbers, New York 1930. Chelsea

[EH] A.G. Earnest, J.S. Hsia: Spinor norms of local integral rotations II, Pac. J. Math. 61, 71-86 (1975), correction: Pac. J. Math. 115, 493-494 (1984)

[E1] M. Eichler: Die "Ahnlichkeitsklassen indefiniter Gitter, Math. Z. 55, 216-252 (1951/52)

[E2] M. Eichler: Quadratische Formen und Orthogonale Gruppen, G"ottingen ... 1952. Springer

[Ge] K. Germann: Tabellen reduzierter, positiver quatern"arer quadratischer Formen, Comm. Math. Helv. 38, 56-83

[He] E. Hecke: Mathematische Werke, G"ottingen 1970. Vandenhoeck u. Ruprecht

[Kn1] M. Kneser: Klassenzahlen definiter quadratischer Formen, Arch. Math. 8, 241-250 (1957)

[Kn2] M. Kneser: Starke Approximation in algebraischen Gruppen I, J. f. d. reine u. angew. Math. 218, 190-203 (1965)

[Kn3] M. Kneser: Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen, Arch. Math. 7, 323-332 (1956)

[Kn4] M. Kneser: Quadratische Formen, Vorlesungsausarbeitung
G"ottingen 1973/74

[KV] H. Koch, B.B. Venkov: "Uber ganzzahlige unimodulare euklidische Gitter, J. f. d. reine u. angew. Math. 398, 144-168 (1989)

[LPS] A. Lubotzky, R. Phillips, P. Sarnak: Ramanujan graphs, Combinatorica 8, 261-277 (1988)

[Mi1] H. Minkowski: Sur la réduction des formes quadratiques positives quaternaires, Comptes rendus de l'Acad. Sci. Paris 96, 1205-1210 (1883)

[Mi2] H. Minkowski: Diskontinuit"atsbereich f"ur arithmetische "Aquivalenz, J. f. d. reine u. angew. Math. 129, 220-274 (1905)

[Ni] H.-V. Niemeier: Definite quadratische Formen der Dimension 24 und Diskriminante 1, J. of Number Th. 5, 142-178 (1973)

[OM] O.T. O'Meara: Introduction to Quadratic Forms, Berlin ... 1971. Springer

[Pi1] A. Pizer: An algorithm for computing modular forms on $\Gamma_0(N)$, J. of Algebra 64, 340-390 (1980)

[Pi2] A. Pizer: Ramanujan graphs and Hecke operators, Bull. AMS 23, 127-138 (1990)

[PZ] M. Pohst, H. Zassenhaus: Algorithmic Algebraic Number Theory, Cambridge 1989. Cambridge University Press

[Poh] M. Pohst: Computation of integral solutions of a special type of quadratic equations, p.203-213 in Computer Algebra, Lect. Notes in Comp. Sc. 162, Berlin...1983, Springer.

[Pon] P. Ponomarev: Class numbers of definite quaternary forms with square discriminant, J. of Number Th. 6, 291-317 (1974)

[Schi] A. Schiemann: Ein Beispiel positiv definiter quadratischer Formen der Dimension 4 mit gleichen Darstellungszahlen, Arch.Math 54, 372-375 (1990)

[SP1] R. Schulze-Pillot: Darstellung durch definite tern"are quadratische Formen, J. of Number Th. 14, 237-250 (1982)

[SP2] R. Schulze-Pillot: A linear relation between theta series of degree and weight 2, p. 197-201 in Number Theory, Ulm 1987, Lect. Notes in Math. 1380, New York ... 1989. Springer

[Shi] K.-I. Shiota: On theta series and the splitting of $S_2(\Gamma_0(q))$, Preprint

[To] S.B. Townes: Table of reduced positive quaternary quadratic forms, Ann. of Math. 41, 57-58 (1940)

[Vi] M.F. Vigneras: Arithmétiques des Algèbres de Quaternions, Lect. Notes Math. 800, Berlin ... 1980. Springer

[vdW] B.L. v. d. Waerden: Die Reduktionstheorie der positiven quadratischen Formen, Acta Math. 96, 265-309 (1956)

[Ya] T. Yamazaki: Jacobi forms and a Maass relation for Eisenstein series (2), Preprint 1988 (Math. Gottingensis Heft 31)

R. Schulze-Pillot
Fakultät f. Mathematik
SFB 343
Universität Bielefeld
D-4800 Bielefeld