Definite Quadratic Forms over $\mathbb{F}_q[x]$

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

Version: September 30, 2002

ABSTRACT. Let R be a principal ideal domain with quotient field F. An **R-lattice** is a free R-module of finite rank spanning an inner product space over F. The **classification problem** asks for a reasonably effective set of criteria to determine when two given R-lattices are isometric; that is, when there is an inner-product preserving isomorphism carrying one lattice onto the other. In this paper R is the polynomial ring $\mathbb{F}_q[x]$, where $\mathbb{F}_q$ is a finite field of odd order q. For $\mathbb{F}_q[x]$-lattices as for $\mathbb{Z}$-lattices the theory splits into "definite" and "indefinite" cases, and this paper settles the classification problem in the definite case.

The classification of definite quadratic forms over the rational integers is a notoriously intractable problem. An exception is the binary case: Gauss showed that every definite binary form over $\mathbb{Z}$ is equivalent to a unique "reduced" form that can be found algorithmically; and two binary forms are equivalent if and only if they have the same reduced form. But for forms of rank $n \geq 3$, while there are a number of reduction theories developed by Minkowski and others, none has proved entirely satisfactory. For example, a given form may be equivalent to more than one reduced form; and determining whether two given reduced forms are equivalent may be computationally daunting. We refer the reader to Nipp [11] for a concrete exposition of these matters, and to Conway–Sloane [2], Chapter 15, for a broad survey of the classification problem over $\mathbb{Z}$.

The ring $\mathbb{Z}$ is a close cousin of the polynomial rings $\mathbb{F}_q[x]$ (here $\mathbb{F}_q$ is a finite field with q elements), and it is often interesting and fruitful to explore the $\mathbb{F}_q[x]$-analogues of problems originally stated over $\mathbb{Z}$. (See Effinger–Hayes [4] for an extensive bibliography on work of this kind.) The goal of this paper is to classify definite quadratic forms over $\mathbb{F}_q[x]$ when q is odd.

From here on we will use the language of lattices on quadratic spaces rather than the more classical language of quadratic polynomial forms. Let R be a principal ideal domain of characteristic not 2 with quotient field F, and let V be an n-dimensional quadratic F-space with symmetric bilinear form B and associated quadratic form Q given by $Q(x) = B(x, x)$. An

R**-lattice** L on V is a free R-module spanning V. If $\mathbb{B} = \{v_1, \ldots, v_n\}$ is a basis for L then the **Gram matrix** for L in $\mathbb{B}$ is the associated symmetric matrix $A = \big(B(v_i, v_j)\big)$; we write $L \cong A$ in $\mathbb{B}$. We say L is **unimodular** if A is a unimodular R-matrix. A $\mathbb{Z}$-lattice on a quadratic $\mathbb{Q}$-space V is **definite** if the extended space $V_\infty = V \otimes_{\mathbb{Q}} \mathbb{Q}_\infty = V \otimes_{\mathbb{Q}} \mathbb{R}$ is anisotropic; that is, $Q(v) \neq 0$ whenever $0 \neq v \in V_\infty$. Similarly, an $\mathbb{F}_q[x]$-lattice on a quadratic $\mathbb{F}_q(x)$-space V is said to be definite if $V_\infty = V \otimes \mathbb{F}_q(x)_\infty$ is anisotropic.

An expectation that classifying lattices up to isometry might be far more approachable over $\mathbb{F}_q[x]$ than it is over $\mathbb{Z}$ arises immediately from the unimodular case. The number of isometry classes of definite unimodular $\mathbb{Z}$-lattices of rank n grows extremely rapidly with n. (See Milnor–Husemoller [10], Chapter II, §6, or Gerstein [5].) But a theorem of G. Harder shows that every unimodular $\mathbb{F}_q[x]$-lattice, definite or not, is extended from a quadratic $\mathbb{F}_q$-space. (See Knebusch [8]; or for a more elementary treatment see Lam [9], pp. 180–187; Scharlau [14], Chapter 6, §3; or Gerstein [6], Theorem 3.1.) Hence, in matrix language: two symmetric unimodular $\mathbb{F}_q[x]$-matrices are congruent over $\mathbb{F}_q[x]$ if and only if their matrices of constant terms are congruent over $\mathbb{F}_q$. It follows that for each $n \geq 1$ there are only two classes of unimodular $\mathbb{F}_q[x]$-lattices of rank n; in fact, a given quadratic $\mathbb{F}_q(x)$-space supports at most one such class.

What happens when we drop the unimodularity condition? We will see that classification no longer amounts to a question over $\mathbb{F}_q$, and in particular the constant terms no longer tell the story. But we will exploit a reduction process due to D. Djoković [3] for lattices over polynomial rings (obtaining a so-called "reduced basis") and show in Theorem 2 that *after applying Djoković's reduction* the classification of definite lattices again boils down to a problem over $\mathbb{F}_q$.

In the present context, the "size" of a vector $v \neq 0$ is given by the degree of $Q(v)$. We will see in Theorem 1 that the ascending sequence of these degrees for vectors in a reduced basis is an invariant of a definite lattice L; moreover, the minimal vectors of L are precisely the nonzero $\mathbb{F}_q$-linear combinations of the minimal vectors in a reduced basis. Thus for definite $\mathbb{F}_q[x]$-lattices, the "shortest vector" problem is completely solved by reduction; whereas for definite $\mathbb{Z}$-lattices this is not the case for lattices of rank ≥ 3.

Differences between the present work over $\mathbb{F}_q[x]$ and the corresponding theory over $\mathbb{Z}$ come primarily from the nonarchimedean behavior of the degree function and the associated "infinite prime" on $\mathbb{F}_q(x)$. In particular, all the completions of $\mathbb{F}_q(x)$ at its nontrivial primes are nondyadic local fields, so every $\mathbb{F}_q(x)$-space of dimension $n \geq 5$ is isotropic. Thus only dimensions $n \leq 4$ need to be considered in handling definite lattices over $\mathbb{F}_q[x]$.

Our notation and terminology will generally follow that of O'Meara's book [12]. In what follows, the symbol ∂ denotes the degree function on

a rational function field $k(x)$, with the usual conventions that $\partial\big(\frac{f(x)}{g(x)}\big) = \partial f(x) - \partial g(x)$ for $f(x), g(x) \in k[x]$, and $\partial 0 = -\infty < m$ for all integers m. The symbol R^* denotes the group of units of a ring R. Finally, $\langle \alpha_1, \ldots, \alpha_n \rangle$ denotes a lattice or space having the diagonal matrix $\mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ as Gram matrix.

I thank Dragomir Djoković for some very helpful comments on his reduction theorem. And I also want to express my thanks to the Department of Mathematics at Dartmouth College, where I was a visitor and began this work during the 1999–2000 academic year.

1. REDUCTION

In this section k can be any field of characteristic not 2.

Definition 1. A symmetric matrix $A = (a_{ij}) \in M_n\big(k(x)\big)$ is **reduced** if (i) A has a **dominant diagonal**, in the sense that $\partial a_{ii} > \partial a_{ij}$ whenever $i \neq j$; and (ii) $\partial a_{11} \leq \ldots \leq \partial a_{nn}$.

Definition 2. A basis $\{v_1, \ldots, v_n\}$ for a $k[x]$-lattice L on a quadratic $k(x)$-space is a **reduced basis** for L if the associated Gram matrix $\big(B(v_i, v_j)\big)$ is reduced. An indexed subset S of L is **reduced** if S is a reduced basis for the sublattice of L that it spans.

DJOKOVIĆ'S THEOREM [3]. *Every anisotropic $k[x]$-lattice has a reduced basis.*

The following algorithm is extracted from the proof of Djoković's theorem. It is expressed here in the language of lattices rather than in terms of matrix operations.

LATTICE REDUCTION ALGORITHM. Given an ordered basis $\{v_1, \ldots, v_n\}$ for a lattice L with associated Gram matrix $A = (a_{ij}) \in M_n\big(k(x)\big)$, the goal is to produce a reduced basis. There is no loss of generality in assuming that $A \in M_n\big(k[x]\big)$ (scale the form by a common denominator of the a_{ij} if necessary), and we do this. As a preliminary step, arrange the basis vectors so that $\partial a_{11} \leq \ldots \leq \partial a_{nn}$.

Step I. Let t be the largest subscript such that $\{v_1, \ldots, v_t\}$ is reduced. (Clearly $t \geq 1$, since the case $n = 1$ is trivial.) If $t = n$ we are done, so suppose $t < n$.

Let $d = \max_{1 \leq i \leq t}\{\partial a_{i,t+1} - \partial a_{ii}\}$. Then $d \geq 0$, since $\{v_1, \ldots, v_{t+1}\}$ is not reduced. For all i, put $\nu_i = \partial a_{ii}$, and let λ_i denote the leading coefficient of a_{ii}. Note that each λ_i is nonzero, since L is anisotropic. For each i with $1 \leq i \leq t$ we can write

$$a_{i,t+1} = c_i x^{\nu_i + d} + \{\text{lower degree terms}\}$$

for some $c_i \in k$. (Note: possibly $c_i = 0$ for some values of i.) Now define

$$v'_{t+1} = v_{t+1} - \sum_{j=1}^{t} \frac{c_j}{\lambda_j} x^d v_j$$

Then for $1 \le i \le t$ we have

$$B(v_i, v'_{t+1}) = a_{i,t+1} - \frac{c_i}{\lambda_i} x^d a_{ii} - \sum_{\substack{1 \le j \le t \\ j \ne i}} \frac{c_j}{\lambda_j} x^d a_{ij}$$

a polynomial of degree at most $\nu_i + d - 1$. (Each term in the sum at the right has degree at most $\nu_i + d - 1$ because $\{v_1, \ldots, v_t\}$ is reduced.) If $\partial Q(v'_{t+1}) \ge \nu_t$ then replace v_{t+1} by v'_{t+1} in the basis and return to the start of Step I. Otherwise

Step II. Let m be the smallest index such that $\partial Q(v'_{t+1}) < \nu_m$, and insert v'_{t+1} immediately before v_m in the ordered basis for L; that is, update the basis to

$$\{v_1, \ldots, v_{m-1}, v'_{k+1}, v_m, \ldots, v_k, v_{k+2}, \ldots, v_n\}$$

Relabel these vectors as $\{v_1, \ldots, v_n\}$, respectively, and return to Step I.

The procedure eventually halts because each pass through Step II reduces a term in the sequence $\{\nu_1, \ldots, \nu_n\}$ of nonnegative integers, so there can be only finitely many such passes. And if the set $\{v_1, \ldots, v_k\}$ is reduced, while $\{v_1, \ldots, v_{k+1}\}$ is not—because the associated value d is nonnegative—then at most $d + 1$ passes through Step I will be needed before either a reduced set $\{v_1, \ldots, v_{k+1}\}$ is achieved or a pass through Step II is required.

Remark 1. When $n = 2$ the above reduction can be done more directly. As above, we can suppose $\partial a_{11} \le \partial a_{22}$. If $\partial a_{12} \ge \partial a_{11}$, then $a_{12} = a_{11}\sigma + \rho$ for some $\rho, \sigma \in R$, with $\partial \rho < \partial a_{11}$. Replacing v_2 by $v'_2 = v_2 - \sigma v_1$ yields a new Gram matrix $A = (a_{ij})$ in which $\partial a_{12} < \partial a_{11}$; then either we are finished or interchange v_1 and v'_2 and repeat the process as needed.

2. LOCAL RESULTS

LEMMA 1. *[LOCAL SQUARE THEOREM]. (See [12], 63:1.) Let K be a nondyadic local field with valuation $|\cdot|$. If $|\alpha| < 1$ then $1 + \alpha$ is a square in K.*

LEMMA 2. *Let U be an n-dimensional quadratic space over a nondyadic local field K. Suppose $U \cong A = (a_{ij}) \in M_n(K)$, with $|a_{ii}| > |a_{ij}|$ for all $j \ne i$, $1 \le i \le n$. Then*

$$U \cong \langle a_{11}, \ldots, a_{nn} \rangle$$

Proof. We have $a_{ii} \ne 0$ for all i, and

$$dU = |A| = \prod_{i=1}^{n} a_{ii} + \sum_{\sigma \ne e} (\mathrm{sgn}\sigma) \prod_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{a}_{\mathrm{i}\sigma(\mathrm{i})} = \prod_{1}^{\mathrm{n}} \mathrm{a}_{\mathrm{ii}} \left(1 + \sum_{\sigma \ne \mathrm{e}} (\mathrm{sgn}\sigma) \frac{\prod_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{a}_{\mathrm{i}\sigma(\mathrm{i})}}{\prod_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{a}_{\mathrm{ii}}} \right)$$

But if $\sigma \ne e$ then

$$\left| \frac{\prod_{i=1}^{n} a_{i\sigma(i)}}{\prod_{i=1}^{n} a_{ii}} \right| < 1$$

Therefore $dU = \prod_1^n a_{ii}$ by Lemma 1, and from this the result follows by induction on n. ∎

Remark 2. The assumption that K is nondyadic is essential in the preceding lemma. For instance, note that $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \ncong \langle 1, 1 \rangle$ over the dyadic local field $\mathbb{Q}_2$.

LEMMA 3. *Let V be a quadratic $\mathbb{F}_q(x)$-space, and suppose $V \cong A = (a_{ij}) \in M_n(\mathbb{F}_q[x])$, where A has a dominant diagonal. For each i, suppose a_{ii} has leading coefficient λ_i and degree ν_i. Then*

$$V_\infty \cong \langle a_{11}, \ldots, a_{nn} \rangle \cong \langle \lambda_1 x^{\nu_1}, \ldots, \lambda_n x^{\nu_n} \rangle$$

Proof. From Lemma 2 we have $V_\infty \cong \langle a_{11}, \ldots, a_{nn} \rangle$. Now for any $f(x) \in \mathbb{F}_q[x]$, say $f(x) = \sum_{i=0}^m \alpha_i x^i$, we can write

$$f = x^m(\alpha_m + \alpha_{m-1}x^{-1} + \ldots + \alpha_0(x^{-1})^m)$$

But x^{-1} is a prime element in the local field $\mathbb{F}_q(x)_\infty$, and so f is in the square class of $\alpha_m x^m$ by Lemma 1. Applying this observation to each a_{ii} gives the result. ∎

3. CLASSIFICATION

From now on, k denotes a finite field $\mathbb{F}_q$ of odd order q.

Definition 3. The **minimum** of a $k[x]$-lattice L, denoted $\min L$, is the smallest degree of a nonzero element represented by L.

THEOREM 1. *Suppose L is a $k[x]$-lattice on the definite quadratic $k(x)$-space V, and suppose further that $L \cong A = (a_{ij}) \in M_n(k[x])$ in the reduced basis $\{v_1, \ldots, v_n\}$.*
(i) Let $0 \neq v = \sum_{i=1}^n \alpha_i v_i \in L$, with $\alpha_i \in k[x]$. Then the leading term of the polynomial $Q(v)$ is the leading term of $\sum_{i=1}^n \alpha_i^2 a_{ii}$, and $\partial Q(v) = \max_i \partial(\alpha_i^2 a_{ii})$.
(ii) $\partial a_{11} = \min L$; and for $i > 1$,

$$\partial a_{ii} = min\{\, \partial Q(x) \mid x \in L,\ x \text{ linearly independent of } v_1, \ldots, v_{i-1} \,\}$$

(iii) Each element represented by L is represented only a finite number of times, and hence the orthogonal group $O(L)$ is finite.
(iv) The degree sequence $(\partial a_{11}, \ldots, \partial a_{nn})$ is an invariant of L. That is, if also $L \cong C = (c_{ij})$, with C reduced, then $(\partial c_{11}, \ldots, \partial c_{nn}) = (\partial a_{11}, \ldots, \partial a_{nn})$.

Proof. (i) We have $Q(v) = \sum_{i=1}^n \alpha_i^2 a_{ii} + 2\sum_{1 \leq i < j \leq n} \alpha_i \alpha_j a_{ij}$. Let $M = \max_i\{\partial(\alpha_i^2 a_{ii})\}$, and consider the expression $\sum_{i=1}^n \alpha_i^2 a_{ii}$; we claim that its degree is M. This is clear if only one term in the sum has degree M. In fact

at most two terms have degree M; for example, suppose $\partial\alpha_i^2 a_{ii} = M$ for $i = 1, 2, 3$. Then $\partial a_{ii} \equiv M \pmod 2$, and, with λ_i the leading coefficient of a_{ii}, by Lemma 3 we would have

$$\langle a_{11}, a_{22}, a_{33}\rangle \cong \langle x^M\lambda_1, x^M\lambda_2, x^M\lambda_3\rangle \quad \text{over } k(x)_\infty$$

But this would be isotropic, since $\langle\lambda_1, \lambda_2, \lambda_3\rangle$ is isotropic over k, contradicting the fact that V is definite. Therefore, to finish the proof of the claim, we suppose (without loss of generality) that $\partial\alpha_1^2 a_{11} = \partial\alpha_2^2 a_{22} = M$, and let $\varepsilon_1, \varepsilon_2$ be the leading coefficients of α_1, α_2. Then the sum of the leading terms of $\alpha_1^2 a_{11}$ and $\alpha_2^2 a_{22}$ is $(\varepsilon_1^2\lambda_1 + \varepsilon_2^2\lambda_2)x^M$. If this were 0 then $\langle\lambda_1, \lambda_2\rangle$ would be a hyperbolic k-plane, and hence by Lemma 3 $\langle a_{11}, a_{22}\rangle$ would be hyperbolic over $k(x)_\infty$, contradicting definiteness. Therefore $\partial(\sum_{i=1}^n \alpha_i^2 a_{ii}) = M$, as claimed. To finish the proof of statement (i), it suffices to check that $\partial\alpha_i\alpha_j a_{ij} < M$ whenever $i \neq j$. Say $\partial\alpha_i \leq \partial\alpha_j$. Then, since A has dominant diagonal, we have

$$\partial\alpha_i\alpha_j a_{ij} \leq \partial\alpha_j^2 a_{ij} < \partial\alpha_j^2 a_{jj} \leq M$$

Statements (ii) and (iii) now follow immediately from statement (i).

(iv) Write $\{\partial a_{11}, \ldots, \partial a_{nn}\} = \{m_1, \ldots, m_t\}$, with $m_1 < \ldots < m_t$ (so $1 \leq t \leq n$). Let $L_0 = \{0\}$, and if $1 \leq j \leq t$, let L_j be the sublattice of L generated by $\{v \in L \mid \partial Q(v) \leq m_j\}$. Then by statement (i), in fact L_j is generated by $\{v_i \mid \partial a_{ii} \leq m_j\}$. Therefore, exactly rank $L_j -$ rank L_{j-1} diagonal entries a_{ii} have degree m_j. ∎

Another proof of finiteness of $O(L)$ was given by O'Meara using local methods in [13], 3.1.

COROLLARY 1. *If in Theorem 1 the inequality $\partial a_{11} < \partial a_{22}$ holds, then $v \in L$ is minimal (that is, $\partial Q(v) = \min L$) if and only if $v = \alpha v_1$ for some $\alpha \in k^*$.*

Definition 4. In the notation of Theorem 1, the sequence $(m_1, \ldots, m_t)$ defined in the proof of statement (iv) is the sequence of **successive minima** of L.

The preceding definition follows the corresponding terminology for lattices over the ring $\mathbb{Z}$ of integers used in Gerstein [7], §2. (Some may prefer to call $(\partial a_{11}, \ldots, \partial a_{nn})$ the sequence of successive minima. E.g., see Cassels [1], Chapter 12, §2, for this usage over $\mathbb{Z}$.)

Example 1. The purpose of this example is to show that the condition that L is definite is essential in Theorem 1. Suppose L is a binary lattice over $\mathbb{Z}_5[x]$, with

$$L \cong A = \begin{pmatrix} x^4 + x^3 & 1 \\ 1 & x^4 \end{pmatrix} \quad \text{in} \quad \{v_1, v_2\}.$$

Then L is indefinite by Lemma 3 and the fact that $\langle 1,1\rangle$ is isotropic over $\mathbb{Z}_5$. It is easily checked that

$$L \cong C = \begin{pmatrix} x^3+4 & 2x+1 \\ 2x+1 & x^5+x^4+x^2+x \end{pmatrix}$$

in the basis $\{v_1+2v_2, -2xv_1+(-4x+1)v_2\}$. Thus $C = {}^tTAT$, with $T = \begin{pmatrix} 1 & -2x \\ 2 & -4x+1 \end{pmatrix}$. So different reduced Gram matrices for a given indefinite lattice may have different degree sequences for their diagonal entries.

Recall that for a $k[x]$-lattice L on a $k(x)$-space V the **dual lattice** is defined by

$$L^\sharp = \{v \in V \mid B(v,L) \subseteq k[x]\}$$

If L has basis $\mathbb{B} = \{v_1,\dots,v_n\}$ then $L^\sharp$ has the dual basis $\mathbb{B}^\sharp = \{v_1^\sharp,\dots,v_n^\sharp\}$, where $B(v_i, v_j^\sharp) = \delta_{ij}$. If $L \cong A \in M_n\big(k(x)\big)$ in $\mathbb{B}$ then $L \cong A^{-1}$ in $\mathbb{B}^\sharp$. In the following lemma, for a given matrix A the symbol $A(i|j)$ denotes the matrix obtained by deleting row i and column j of A.

LEMMA 4. *If $\{v_1,\dots,v_n\}$ is a reduced basis for the $k[x]$-lattice L then the reversed dual basis $\{v_n^\sharp,\dots,v_1^\sharp\}$ is a reduced basis for the dual lattice $L^\sharp$; in particular, for $2 \le i \le n$ the inequality $\partial Q(v_i^\sharp) \le \partial Q(v_{i-1}^\sharp)$ holds. Moreover,*

$$\partial Q(v_i^\sharp) < \partial Q(v_{i-1}^\sharp) \quad \textit{if and only if} \quad \partial Q(v_{i-1}) < \partial Q(v_i)$$

Proof. Suppose $L \cong A = (a_{ij}) \in M_n\big(k(x)\big)$ in the basis $\{v_1,\dots,v_n\}$. Then $L^\sharp \cong A^{-1}$ in $\{v_1^\sharp,\dots,v_n^\sharp\}$. [Note: The reader who prefers to work with polynomials instead of with rational functions may temporarily scale the form by the discriminant dL, getting $(L^\sharp)^{dL} \cong \operatorname{adj} A$ in $\{v_i^\sharp\}_{1\le i\le n}$.]

Then

$$\partial Q(v_i^\sharp) = \partial \det A(i|i) = \sum_{j\ne i} \partial a_{jj} = -\partial a_{ii} + \sum_{j=1}^{n} \partial a_{jj}$$

Therefore for $2 \le i \le n$ we have

$$\partial Q(v_i^\sharp) - \partial Q(v_{i-1}^\sharp) = \partial a_{i-1,i-1} - \partial a_{ii} \le 0$$

so $\partial Q(v_i^\sharp) \le \partial Q(v_{i-1}^\sharp)$, and the statement on strict inequality is now clear. It remains to check the dominant diagonal property; that is, that $\partial \det A(i|j) < \partial \det A(i|i)$ when $i \ne j$.

Because A has dominant diagonal the term in $\det A(i|i)$ of strictly largest degree is $\prod_{r\ne i} a_{rr}$, while when $i \ne j$ every term in $\det A(i|j)$ has the form $\prod_{r\ne i} a_{rj_r}$, with $j_r \ne r$ at least once (e.g., when $r = j$). So, again by the dominant diagonal, we have $\partial \det A(i|j) < \partial \det A(i|i)$; that is, $\partial B(v_i^\sharp, v_j^\sharp) < \partial Q(v_i^\sharp)$ when $i \ne j$. Thus adj A has dominant diagonal, hence so does A^{-1}. So the gram matrix of $L^\sharp$ in $\{v_n^\sharp,\dots,v_1^\sharp\}$ is reduced. ∎

THEOREM 2. *Let L and M be $k[x]$-lattices on a definite quadratic $k(x)$-space V of dimension n, and suppose L and M have respective Gram matrices $A, C \in M_n(k[x])$. Suppose further that A and C are reduced. Then*

$$L \cong M \quad \text{if and only if} \quad C = {}^tTAT \text{ for some } T \in GL_n(k).$$

Moreover, if for $1 \le i \le t$ the successive minimum m_i occurs with multiplicity n_i, then T has the form

$$\begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_t \end{pmatrix}$$

with $B_i \in GL_{n_i}(k)$.

Proof. Only the necessity requires proof, and for this we can assume without loss of generality that $L = M$. Because V is definite, we have $n \le 4$. Assume $A = (a_{ij})$ and $C = (c_{ij})$ are the Gram matrices for L associated with reduced bases $\mathbb{B}_1 = \{v_1, \dots, v_n\}$ and $\mathbb{B}_2 = \{w_1, \dots, w_n\}$, respectively. We have $w_j = \sum_i t_{ij} v_i$ for $j = 1, \dots, n$, with $T = (t_{ij}) \in GL_n(k[x])$; and so $C = {}^tTAT$. We will be done if we can show that this T has the stated form.

(I) We first show that if T has the form

$$T = \begin{pmatrix} 1 & & & t_{1n} \\ & \ddots & & \vdots \\ & & 1 & t_{n-1,n} \\ & & & t_{n,n} \end{pmatrix} \in GL_n(k[x])$$

then $t_{in} = 0$ for $1 \le i \le n-1$.

If $n = 2$ then $c_{12} = B(v_1, w_2) = t_{12}a_{11} + t_{22}a_{12}$. If $t_{12} \neq 0$ then $\partial c_{12} \ge \partial a_{11} = \partial c_{11}$ since $t_{22} \in k^*$, contradicting the fact that C is reduced.

Now suppose $n = 3$. If $t_{13} = 0$ then the case $n = 2$ applied to the sublattice spanned by $\{v_2, v_3\}$ shows that $t_{23} = 0$, and conversely; so without loss of generality we can suppose $t_{13}t_{23} \neq 0$. We have

$$c_{13} = B(v_1, w_3) = t_{13}a_{11} + t_{23}a_{12} + t_{33}a_{13}$$

and

$$c_{23} = B(v_2, w_3) = t_{13}a_{12} + t_{23}a_{22} + t_{33}a_{23}.$$

Since A and C are reduced, and $t_{33} \in k^*$, it follows that

$$\partial(t_{13}a_{11} + t_{23}a_{12}) < \partial a_{11} \quad \text{and} \quad \partial(t_{13}a_{12} + t_{23}a_{22}) < \partial a_{22}$$

and therefore

$$\partial t_{13} + \partial a_{11} = \partial t_{23} + \partial a_{12} \quad \text{and} \quad \partial t_{13} + \partial a_{12} = \partial t_{23} + \partial a_{22},$$

which in turn yields the contradictory inequalities

$$\partial t_{23} = \partial t_{13} + (\partial a_{11} - \partial a_{12}) > \partial t_{13} \quad \text{and} \quad \partial t_{13} = \partial t_{23} + (\partial a_{22} - \partial a_{12}) > \partial t_{23},$$

finishing the proof of (I) in the case $n = 3$.

Finally, suppose $n = 4$. As in the preceding case, if $t_{14}t_{24}t_{34} = 0$ we are reduced to lower dimensions and hence finished; so there remains only the situation in which $t_{14}t_{24}t_{34} \neq 0$. Then for $i = 1, 2, 3$ we have $c_{i4} = B(v_i, w_4) = \sum_{j=1}^{4} t_{j4}a_{ij}$ and hence

$$(*) \qquad \partial(t_{14}a_{i1} + t_{24}a_{i2} + t_{34}a_{i3}) < \partial a_{ii} \quad \text{for } i = 1, 2, 3.$$

Then from (*) we have

$$\partial(t_{24}a_{12} + t_{34}a_{13}) = \partial t_{14}a_{11}$$
$$\partial(t_{14}a_{21} + t_{34}a_{23}) = \partial t_{24}a_{22}$$
$$\partial(t_{14}a_{31} + t_{24}a_{32}) = \partial t_{34}a_{33}.$$

The first of these three equations, together with the fact that A is reduced, gives that either $\partial t_{24} > \partial t_{14}$ or $\partial t_{34} > \partial t_{14}$. So $\partial t_{14} \neq \max\{\partial t_{14}, \partial t_{24}, \partial t_{34}\}$. Similarly, the other two equations show that neither ∂t_{24} nor ∂t_{34} is equal to $\max\{\partial t_{14}, \partial t_{24}, \partial t_{34}\}$, an absurdity. Therefore the case in which $t_{14}t_{24}t_{34} \neq 0$ cannot occur. This completes the proof of part (I).

(II) Now suppose T is as in the statement of the theorem but otherwise unrestricted in $GL(k[x])$. We will argue inductively. The case $n = 1$ is trivial, so we may assume that $1 < n \leq 4$ and that the theorem has been proved for lattices of rank $\leq n - 1$.

First suppose $\partial a_{nn} > \partial a_{n-1,n-1}$ Then by Theorem 1 the matrix T has the form

$$\begin{pmatrix} & & & t_{1n} \\ & T_0 & & t_{2n} \\ & & & \vdots \\ 0 & 0 & 0 & t_{nn} \end{pmatrix}$$

with $T_0 \in GL_{n-1}(k[x])$. In fact, from the induction hypothesis we have $T_0 \in GL_{n-1}(k)$ (and having the appropriate block decomposition), and hence $\{v_1, \ldots, v_{n-1}, w_n\}$ is also a reduced basis for L. By part (I) of the proof it then follows that $t_{1n} = \cdots = t_{n-1,n} = 0$, and we are done.

If $\partial a_{11} < \partial a_{22}$ the argument reduces to the preceding case by "dualizing" as follows. From Lemma 4, $\{v_n^\sharp, \ldots, v_1^\sharp\}$ and $\{w_n^\sharp, \ldots, w_1^\sharp\}$ are reduced bases for $L^\sharp$, with $\partial Q(v_n^\sharp) \leq \ldots \leq \partial Q(v_2^\sharp) < \partial Q(v_1^\sharp)$. We have

$$L^\sharp \cong PA^{-1}P \text{ in } \{v_n^\sharp, \ldots, v_1^\sharp\} \quad \text{and} \quad L^\sharp \cong PC^{-1}P \text{ in } \{w_n^\sharp, \ldots, w_1^\sharp\},$$

with

$$P = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$$

Thus the preceding argument applies to $L^\sharp$, giving a matrix $S \in GL_n(k)$ such that $PC^{-1}P = {}^tS(PA^{-1}P)S$. Upon taking inverses and setting $T = P({}^tS^{-1})P$ we get $C = {}^tTAT$, with $T \in GL_n(k)$ of the desired form.

It remains to consider the case $\partial a_{11} = \partial a_{22} < \partial a_{33} = \partial a_{44}$. In this situation we have $T = \begin{pmatrix} B_1 & * \\ 0 & B_2 \end{pmatrix}$, with $B_1, B_2 \in GL_2(k)$. Then

$$L \cong D = {}^tSAS = \begin{pmatrix} a_{11} & a_{12} & * & * \\ a_{12} & a_{22} & * & * \\ * & * & c_{33} & c_{34} \\ * & * & c_{34} & c_{44} \end{pmatrix}, \text{ with } S = \begin{pmatrix} 1 & & t_{13} & t_{14} \\ & 1 & t_{23} & t_{24} \\ & & B_2 & \end{pmatrix},$$

in $\{v_1, v_2, w_3, w_4\}$. The matrix D is reduced, because v_1 and v_2 are k-linear combinations of w_1 and w_2. Therefore, without loss of generality we can assume $v_1 = w_1$ and $v_2 = w_2$. We want to show that $\begin{pmatrix} t_{13} & t_{14} \\ t_{23} & t_{24} \end{pmatrix} = 0$. By symmetry it suffices to show that $t_{13} = 0$.

We have

$$\partial a_{11} > \partial B(v_1, w_3) = \partial(t_{13}a_{11} + t_{23}a_{12} + t_{33}a_{13} + t_{43}a_{14}),$$

with $t_{33}, t_{43} \in k$. So if $t_{13} \neq 0$ then $\partial(t_{13}a_{11}) = \partial(t_{23}a_{12})$, from which it follows that $\partial t_{23} > \partial t_{13}$. But then since $\partial a_{11} = \partial a_{22} > \partial B(v_2, w_3)$ we could also deduce the inequality $\partial t_{13} > \partial t_{23}$, a contradiction. So we must have $t_{13} = 0$, as desired. ∎

Remark 3. In light of Lemma 3, the hypothesis in Theorem 2 that V is definite guarantees that each n_i is equal to 1 or 2.

COROLLARY 2. *In the notation of Theorem 2, suppose further that $\partial a_{11} < \ldots < \partial a_{nn}$. Then there is essentially only one reduced basis for L. More precisely, if $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_n\}$ are reduced bases for L then $w_i = \alpha_i v_i$, with $\alpha_i \in k^*$, for $1 \leq i \leq n$. Hence $L \cong M$ if and only if there is a diagonal matrix $T \in GL_n(k)$ such that $C = TAT$.*

Example 2. Strict inequality is essential in the hypothesis of the preceding corollary. For suppose -1 is a nonsquare in k, let

$$A = \begin{pmatrix} x^3 + x + 1 & x \\ x & x^3 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 2x^3 + 3x + 1 & x + 1 \\ x + 1 & 2x^3 - x + 1 \end{pmatrix}$$

and take $k[x]$-lattices lattices L and M with respective Gram matrices A and C. The condition on -1 guarantees that L and M are definite. Then with $T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in GL_2(k)$ we have $C = {}^tTAT$; and clearly no choice of T as a diagonal matrix in $GL_2(k)$ would achieve this result.

Remark 4. For a lattice L as in the preceding corollary, the orthogonal group $O(L)$ satisfies the inclusion

$$O(L) \subseteq \left\{ \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} \right\}$$

(Here we have identified an isometry with its matrix with respect to a reduced basis $\mathbb{B}$.) Consider a graph G with $\mathbb{B}$ as vertex set and an edge $v_i v_j$ if and only if $B(v_i, v_j) \neq 0$. Then $|O(L)| = 2^\nu$, where ν is the number of connected components of G. For example, if $B(v_i, v_{i+1}) \neq 0$ for all i, $1 \leq i \leq n-1$, then the orthogonal group is trivial: $O(L) = \{\pm I\}$; in which case L is indecomposable.

REFERENCES

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

[2] Conway, J.H., and Sloane, N.J.A. (1999), *Sphere Packings, Lattices and Groups*, Third Edition, Springer-Verlag.

[3] Djoković, D.Z. (1976), Hermitian matrices over polynomial rings, *J. Algebra* **43** 359–374.

[4] Effinger, G.W., and Hayes, D.R. (1991), *Additive Number Theory of Polynomials over a Finite Field*, Oxford University Press.

[5] Gerstein, L.J. (1972), The growth of class numbers of quadratic forms, *Amer. J. Math.* **11** 221–236.

[6] Gerstein, L.J. (1979), Unimodular quadratic forms over global function fields, *J. Number Theory* **11** 529–541.

[7] Gerstein, L.J. (1995), Nearly unimodular quadratic forms, *Annals of Mathematics* **142** 597–610.

[8] Knebusch, M. (1969/70), Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen, *Sitzungsber. Heidelberg Akad. Wiss.* 93–157.

[9] Lam, T.-Y. (1978), *Serre's Conjecture*, Lecture Notes in Mathematics **635**.

[10] Milnor, J., and Husemoller, D. (1973), *Symmetric Bilinear Forms*, Springer-Verlag.

[11] Nipp, G.L. (1991), *Quaternary Quadratic Forms*, Springer-Verlag.

[12] O'Meara, O.T. (1963, reprinted in 2000), *Introduction to Quadratic Forms*, Springer-Verlag.

[13] O'Meara, O.T. (1969), The automorphisms of the orthogonal groups and their congruence subgroups over arithmetic domains *J. reine angew. Math.* **238** 169–206.

[14] Scharlau, W. (1985), *Quadratic and Hermitian Forms*, Springer-Verlag.