Journal of Number Theory 129 (2009) 2457–2473

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Isospectral definite ternary $\mathbf{F}_q[t]$-lattices

Jean Bureau, Jorge Morales *

Mathematics Department, Louisiana State University, Baton Rouge, LA 70803-4918, USA

ARTICLE INFO

Article history:
Received 31 August 2008
Revised 24 February 2009
Available online 29 May 2009
Communicated by John S. Hsia

MSC:
11T06
11E12
11E16
11E20

ABSTRACT

We prove that the representations numbers of a ternary definite integral quadratic form defined over $\mathbf{F}_q[t]$, where $\mathbf{F}_q$ is a finite field of odd characteristic, determine its integral equivalence class when q is large enough with respect to its successive minima. Equivalently, such a quadratic form is determined up to integral isometry by its theta series.

1. Introduction

It has been a long-standing question to determine whether integral definite $\mathbf{Z}$-lattices are determined up to isometry by their theta series. In 1979, Watson [16] proved that definite binary $\mathbf{Z}$-lattices are determined by their primitive representations. The case of ternary lattices had to wait until 1997 to be solved by Schiemann [15] by means of extensive computations. He proved that definite ternary $\mathbf{Z}$-lattices are indeed determined by their representation numbers. This is not the case for forms of rank $\geqslant 4$, where counterexamples have been found (cf. [3,8,14]).

In this paper we prove the analogue of Schiemann's theorem for definite ternary $\mathbf{F}_q[t]$-lattices, where $\mathbf{F}_q$ is a finite field of odd characteristic. We show first that the representation numbers determine invariants such as the successive minima and the genus (Sections 3 and 4). Our proof that the representation numbers determine the equivalence class requires different arguments according to different configurations of the successive minima (Section 6). When the successive minima have alternating parity, we use a theorem of Carlitz based on Fourier inversion and we are able to conclude equivalence under the hypothesis that the ground field $\mathbf{F}_q$ is large enough (see Theorem 6.17 for a precise statement). This condition is not required in the two other cases (Theorems 6.5 and 6.9).

* Corresponding author.
E-mail addresses: jbureau@math.lsu.edu (J. Bureau), morales@math.lsu.edu (J. Morales).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2009.03.008

2. Notation and terminology

The following notation will be in force throughout the paper:

$\mathbf{F}_q$: The finite field of order q. We always assume q odd.
A: The polynomial ring $\mathbf{F}_q[t]$.
K: The field of rational functions $\mathbf{F}_q(t)$.
δ: A fixed non-square of $\mathbf{F}_q^\times$.

Let L be an A-lattice of finite rank n and let Q be a quadratic form on L. The form Q is *definite* if it is anisotropic over the field $K_\infty = \mathbf{F}_q((1/t))$. This implies in particular that $n \leqslant 4$.

Let $B(\mathbf{x}, \mathbf{y}) = Q(\mathbf{x} + \mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y})$ be the associated symmetric bilinear form. Djoković [5] showed that if (L, Q) is definite, then there exists an A-basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of L such that the Gram matrix $M = (m_{ij})$, where $m_{ij} = \frac{1}{2}B(\mathbf{v}_i, \mathbf{v}_j)$, satisfies

$$\deg m_{ii} \leqslant \deg m_{jj} \quad \text{for } i \leqslant j \quad \text{and} \quad \deg m_{ij} < \deg m_{ii} \quad \text{for } i < j. \tag{1}$$

Such a basis is called *reduced*. Gerstein [6, Theorem 2] showed that if $\mathbf{v}'_1, \ldots, \mathbf{v}'_n$ is another reduced basis for (L, Q), then

$$\mathbf{v}'_j = \sum_{i=1}^{n} u_{ij}\mathbf{v}_i,$$

where $u_{ij} \in \mathbf{F}_q$.

In particular, the increasing sequence of degrees of the diagonal terms of a reduced Gram matrix

$$(\deg m_{11}, \deg m_{22}, \ldots, \deg m_{nn})$$

is an invariant of the equivalence class of the quadratic form. This sequence is called the *sequence of successive minima* of Q and will be denoted by

$$\big(\mu_1(L, Q), \mu_2(L, Q), \ldots, \mu_n(L, Q)\big).$$

The *representation numbers* of (L, Q) are defined by

$$R(L, Q, a) = \big|\big\{\mathbf{v} \in L\colon\ Q(\mathbf{v}) = a\big\}\big| \quad (a \in K). \tag{2}$$

It is easy to see that if (L, Q) is definite, the above numbers are finite. Clearly they depend only on the isometry class of (L, Q).

Definition 1. Two definite quadratic forms (L, Q) and (L', Q') are called *isospectral*[1] if $R(L, Q, a) = R(L', Q', a)$ for all $a \in K$.

Following Conway's [4] terminology, we shall call an invariant of (L, Q) *audible* if it is determined by the representation numbers. The main goal of this paper is to show that the equivalence class of a ternary definite quadratic form over A is audible. We shall do this in several steps.

[1] The terminology comes from the fact that for quadratic forms over $\mathbf{Z}$ the representation numbers are naturally the dimensions of the eigenspaces of a Laplace operator, see [9].

3. The successive minima

Let (L, Q) be a definite quadratic form over A. For $m \in \mathbf{Z}$, define

$$L_m = \{\mathbf{v} \in L\colon \deg Q(\mathbf{v}) \leqslant m\}. \tag{3}$$

It is easy to see that the L_m are finite-dimensional $\mathbf{F}_q$-subspaces of L and that they form an increasing sequence whose union is L. We encode their successive dimensions into the formal power series

$$\mathbf{S}_L(u) = \sum_{m\in\mathbf{Z}} \dim(L_m/L_{m-1})u^m \quad \text{and} \quad \mathbf{T}_L(u) = \sum_{m\in\mathbf{Z}} \dim(L_m)u^m. \tag{4}$$

Notice that both $\mathbf{S}_L(u)$ and $\mathbf{T}_L(u)$ are Laurent series in u since $L_m = \{0\}$ for $m \ll 0$ (we do not assume that Q takes integral values on L). It is clear from their definition that both series are audible.

Proposition 3.1. *With the notation above we have*

$$\mathbf{S}_L(u) = \frac{u^{\mu_1} + u^{\mu_2} + u^{\mu_3}}{1-u^2} \quad \textit{and} \quad \mathbf{T}_L(u) = \frac{u^{\mu_1} + u^{\mu_2} + u^{\mu_3}}{(1-u^2)(1-u)},$$

where (μ_1, μ_2, μ_3) are the successive minima of (L, Q). In particular the sequence (μ_1, μ_2, μ_3) is audible.

Proof. Let $\mathbf{v}_2, \mathbf{v}_2, \mathbf{v}_3$ be a reduced basis of L. Notice that since Q is definite, μ_1, μ_2, μ_3 cannot all have the same parity.

Suppose first that $\mu_1 \equiv \mu_2 \pmod 2$. If $m < \mu_1$, then clearly L_m is trivial. When $m \equiv \mu_1 \pmod 2$ and $\mu_1 \leqslant m < \mu_2$, the quotient space L_m/L_{m-1} is 1-dimensional (with basis $\{t^{(m-\mu_1)/2}\mathbf{v}_1\}$). When $m \equiv \mu_1 \pmod 2$ and $m \geqslant \mu_2$, the quotient L_m/L_{m-1} is 2-dimensional (with basis $\{t^{(m-\mu_1)/2}\mathbf{v}_1, t^{(m-\mu_2)/2}\mathbf{v}_2\}$). When $m \equiv \mu_3 \pmod 2$, the quotient L_m/L_{m-1} is trivial if $m < \mu_3$ and 1-dimensional if $m \geqslant \mu_3$ (with basis $\{t^{(m-\mu_3)/2}\mathbf{v}_3\}$).

Putting this information into the series, we get

$$\begin{aligned}\mathbf{S}_L(u) &= \sum_{k=0}^{(\mu_2-\mu_1)/2-1} u^{\mu_1+2k} + 2\sum_{k=0}^{\infty} u^{\mu_2+2k} + \sum_{k=0}^{\infty} u^{\mu_3+2k} \\ &= \frac{u^{\mu_1} + u^{\mu_2} + u^{\mu_3}}{1-u^2}.\end{aligned}$$

The case when $\mu_1 \not\equiv \mu_2 \pmod 2$ is computed similarly. We spare the reader the details. The second identity follows from the obvious relation $\mathbf{S}_L(u) = (1-u)\mathbf{T}_L(u)$. □

4. The genus

Let $\mathfrak{p}$ be a prime ideal of A and let ξ be a root (in an algebraic closure of $\mathbf{F}_q$) of a generator of $\mathfrak{p}$. The *canonical character* $\chi_{\mathfrak{p}} : K_{\mathfrak{p}} \to \mathbb{C}^\times$ is the homomorphism defined by

$$\chi_{\mathfrak{p}}(f) = \exp\bigl(2\pi i \operatorname{Tr}\bigl(\operatorname{Res}_\xi(f)\bigr)/p\bigr),$$

where $\operatorname{Res}_\xi(f) \in \mathbf{F}_q(\xi)$ is the residue of f at ξ (i.e. the coefficient of $(T-\xi)^{-1}$ in the Laurent series expansion of f at ξ) and $\operatorname{Tr} : \mathbf{F}_q(\xi) \to \mathbf{F}_p$ is the trace to the prime field $\mathbf{F}_p$. Clearly the definition is independent of the choice of the root ξ, since residues at different roots are conjugate over $\mathbf{F}_q$. Notice that $\chi_{\mathfrak{p}}$ is trivial on $A_{\mathfrak{p}}$; in fact $A_{\mathfrak{p}}$ is the largest fractional ideal of $K_{\mathfrak{p}}$ on which $\chi_{\mathfrak{p}}$ is trivial.

Let (W, Q) be a definite quadratic space over K and let $L \subset W$ be an A-lattice, not necessarily integral with respect to Q.

Define

$$\mu(L, Q, \chi_{\mathfrak{p}}) = \lim_{m\to\infty} \frac{1}{|L_m|} \sum_{\mathbf{x}\in L_m} \chi_{\mathfrak{p}}\big(Q(\mathbf{x})\big).$$

We shall see below that this is a stabilizing limit. We first notice that this "average", $\mu(L, Q, \chi_{\mathfrak{p}})$, is audible. Indeed, we have

$$\begin{aligned}\mu(L, Q, \chi_{\mathfrak{p}}) &= \lim_{m\to\infty} \frac{1}{|L_m|} \sum_{\mathbf{x}\in L_m} \chi_{\mathfrak{p}}\big(Q(\mathbf{x})\big)\\ &= \lim_{m\to\infty} \frac{1}{|L_m|} \sum_{\deg(a)\leqslant m} R(L, a)\chi_{\mathfrak{p}}(a).\end{aligned}$$

We now express $\mu(L, Q, \chi_{\mathfrak{p}})$ in terms of local data. Let $L^\sharp$ be the dual of L with respect to Q. Since L is the union of the L_m, for m large enough, the restriction $L_m \to L/(L^\sharp \cap L)$ of the canonical projection is surjective. Thus

$$\begin{aligned}\frac{1}{|L_m|} \sum_{\mathbf{x}\in L_m} \chi_{\mathfrak{p}}\big(Q(\mathbf{x})\big) &= \frac{|L_m \cap L^\sharp|}{|L_m|} \sum_{\mathbf{x}\in L_m/L_m\cap L^\sharp} \chi_{\mathfrak{p}}\big(Q(\mathbf{x})\big)\\ &= \frac{1}{|L : L \cap L^\sharp|} \sum_{\mathbf{x}\in L/L\cap L^\sharp} \chi_{\mathfrak{p}}\big(Q(\mathbf{x})\big)\\ &= \frac{1}{|L_{\mathfrak{p}} : L_{\mathfrak{p}} \cap L_{\mathfrak{p}}^\sharp|} \sum_{\mathbf{x}\in L_{\mathfrak{p}}/L_{\mathfrak{p}}\cap L_{\mathfrak{p}}^\sharp} \chi_{\mathfrak{p}}\big(Q(\mathbf{x})\big). \qquad (5)\end{aligned}$$

Theorem 4.1. *Let π be a monic generator of $\mathfrak{p}$. The sequence $\mu(L, \pi^{-k}Q, \chi_{\mathfrak{p}})$ $(k = 0, 1, 2, \ldots)$ determines completely the local class $(L_{\mathfrak{p}}, Q)$.*

Proof. Let $(L_{\mathfrak{p}}, Q) = (M_1, Q_1) \perp (M_2, Q_2) \perp \cdots \perp (M_r, Q_r)$ be the Jordan decomposition. Each M_i is $\mathfrak{p}$-modular, i.e. $M_i^\sharp = \pi^{-\nu_i} M_i$, and we assume $\nu_1 < \nu_2 < \cdots < \nu_r$. We define μ for local lattices using the last line of (5). Then we have

$$\mu\big(M_i, \pi^{-k}Q_i, \chi_{\mathfrak{p}}\big) = \begin{cases} [M_i : \pi^{k-\nu_i} M_i]^{-1} \sum_{\mathbf{x}\in M_i/\pi^{k-\nu_i}M_i} \chi_p(\pi^{-k}Q(\mathbf{x})) & \text{if } k \geqslant \nu_i;\\ 1 & \text{if } k < \nu_i.\end{cases}$$

We can express this further using the invariant $\gamma_{\mathfrak{p}}$ defined in [13, Ch. V, §8] (see also [17, §24]). Then we have

$$\mu\big(M_i, \pi^{-k}Q_i, \chi_{\mathfrak{p}}\big) = \begin{cases} [M_i : \pi^{k-\nu_i} M_i]^{-1/2} \gamma_{\mathfrak{p}}(\pi^{-k}Q_i) & \text{if } k \geqslant \nu_i;\\ 1 & \text{if } k < \nu_i.\end{cases} \qquad (6)$$

The invariant $\gamma_{\mathfrak{p}}(\pi^{-k}Q_i)$ is a 4th root of unity and depends only on the class of $\pi^{-k}Q_i$ over the field $K_{\mathfrak{p}}$ (actually, only on its Witt class) [13, Chapter 5]. In particular $|\gamma_{\mathfrak{p}}(\pi^{-k}Q_i)| = 1$, thus

$$\log_q \left|\mu\left(M_i, \pi^{-k} Q_i, \chi_{\mathfrak{p}}\right)\right| = -\frac{m_i \deg \pi}{2} \sup\{0, k - \nu_i\},$$

where m_i is the rank of M_i and $\log_q$ is the logarithm in base q. Using the obvious fact that μ is compatible with orthogonal sums, we get

$$\log_q \left|\mu\left(L, \pi^{-k} Q, \chi_{\mathfrak{p}}\right)\right| = -\sum_{i=1}^{r} \frac{m_i \deg \pi}{2} \sup\{0, k - \nu_i\}. \tag{7}$$

As observed earlier, the left-hand side of (7) is audible as a function of k, then so is the right-hand side. The functions $f_\nu : \mathbf{Z} \to \mathbf{R}$ given by $f_\nu(k) = \sup\{0, k - \nu\}$ are linearly independent, so the expression of $\log_q |\mu(L, \pi^{-k} Q, \chi_{\mathfrak{p}})|$ in (7) as linear combination of these functions is unique; it follows that the numbers $\nu_1, \nu_2, \ldots, \nu_r$ and the ranks $m_1, m_2, \ldots, m_r$ of the Jordan factors of $L_{\mathfrak{p}}$ are audible.

It is left to show that $\det(M_i, Q_i)$ is audible. Consider the case $i = 1$ and $k = \nu_1 + 1$. Let $F = \pi^{-\nu_1} Q_1$ (note that F is unimodular on M_1). By (6), we have

$$\begin{aligned} \mu\left(L, \pi^{-\nu_1 - 1} Q, \chi_{\mathfrak{p}}\right) &= \mu\left(M_1, \pi^{-1} F, \chi_{\mathfrak{p}}\right) \\ &= q^{-m_1 \deg \pi / 2} \gamma_{\mathfrak{p}}\left(\pi^{-1} F\right). \end{aligned} \tag{8}$$

The invariant $\gamma_{\mathfrak{p}}$ satisfies $\gamma_{\mathfrak{p}}(\langle a \rangle)\gamma_{\mathfrak{p}}(\langle b \rangle) = \gamma_{\mathfrak{p}}(\langle ab \rangle)(a, b)_{\mathfrak{p}}$, where $(a, b)_{\mathfrak{p}}$ is the Hilbert symbol [17, §28, p. 176]. Applying this identity, we get

$$\gamma_{\mathfrak{p}}\left(\pi^{-1} F\right) = \gamma_{\mathfrak{p}}\left(\langle \pi \rangle\right)^{m_1} \gamma_{\mathfrak{p}}(F)(\det F, \pi)_{\mathfrak{p}},$$

where $\langle \pi \rangle$ is the rank-one form πX^2. Since F is unimodular on M_1, $\gamma_{\mathfrak{p}}(F) = 1$, so $\gamma_{\mathfrak{p}}(\pi^{-1} F) = \gamma_{\mathfrak{p}}(\langle \pi \rangle)^{m_1} (\det F, \pi)_{\mathfrak{p}}$. It follows from this and (8) that the class of (M_1, Q_1) is audible. We continue similarly taking successively $k = \nu_2 + 1, \ldots, \nu_r + 1$. □

Theorem 4.1 has two immediate consequences:

Corollary 4.2. *The genus of* (L, Q) *is audible.*

Corollary 4.3. *The discriminant of* (L, Q) *is audible.*

5. The theta series and the adjoint form

Let (L, Q) be a definite ternary A-lattice. We define the theta series of (L, Q) as in Rück [12] and Rosson [11]. We shall refer to these papers for details of some computations.

The analogue of the Poincaré complex half-plane is $\mathfrak{H} = \mathbf{SL}_2(K_\infty)/\mathbf{SL}_2(\mathcal{O}_\infty)$. A complete set of coset representatives for $\mathfrak{H}$ is the set

$$\mathfrak{D} = \left\{ \begin{bmatrix} y & xy^{-1} \\ 0 & y^{-1} \end{bmatrix} : \ y = t^m, \ m \in \mathbf{Z}, \ x \in t^{2m+1} A \right\}. \tag{9}$$

Let $x = \sum_{i=-\infty}^{n} x_i t^i \in K_\infty$. We define a character of $e : K_\infty \to \mathbf{C}^\times$ by

$$e\{x\} = \exp\left(2i\pi \ \mathrm{Tr}(x_1)/p\right),$$

where Tr stands for the trace of $\mathbf{F}_q$ to its prime subfield and p is the characteristic of $\mathbf{F}_q$. Let Ψ denote the characteristic function of $\mathcal{O}_\infty$. For $z = \left(\begin{smallmatrix} y & xy^{-1} \\ 0 & y^{-1} \end{smallmatrix}\right) \in \mathfrak{H}$ and for a lattice L, we define the theta series of L by

$$\begin{aligned}\theta_L(z) &= \sum_{\mathbf{v}\in tL} \Psi\left(y^2 Q(\mathbf{v})\right) e\left\{xQ(\mathbf{v})\right\} \\ &= \sum_{w\in L} \Psi\left(t^2 y^2 Q(\mathbf{w})\right) e\left\{t^2 xQ(\mathbf{w})\right\}.\end{aligned}$$

It is readily checked that θ_L is a function on $\mathfrak{H}$, i.e. does not depend on the chosen matrix representatives. The theta series determines the representation numbers and conversely. Indeed, for $y = t^{-m}$, we have

$$\theta_L(z) = \sum_{v_\infty(a)\geqslant 2m-2} R(L,a)\, e\left\{xt^2 a\right\}. \tag{10}$$

It is clear from this that the representation numbers $R(L,a)$ can be recovered from $\theta_L(z)$ by Fourier inversion.

Let $d\mathbf{v}$ be an additive Haar measure on V_∞. For a locally constant compactly supported function f on V_∞, we define its Fourier transform by

$$\hat{f}(\mathbf{w}) = \int_{V_\infty} f(\mathbf{v}) e\left\{-B(\mathbf{v},\mathbf{w})\right\} d\mathbf{v},$$

where B is the bilinear form associated to Q. We shall further assume that the Haar measure $d\mathbf{v}$ is self-dual, i.e. it has been normalized so that

$$\hat{\hat{f}}(\mathbf{v}) = f(-\mathbf{v}). \tag{11}$$

This is equivalent to saying that the volume with respect to $d\mathbf{v}$ of any O_∞-lattice $M \subset V_\infty$ satisfies

$$\operatorname{vol}(M)\operatorname{vol}(M^*) = 1,$$

where $M^* = \{\mathbf{w} \in V_\infty :\ B(\mathbf{w}, M) \subset O_\infty\}$.

Proposition 5.1. *Let $G, H \in K_\infty$, $H \neq 0$, be such that $v_\infty(G) = g > h = v_\infty(H)$. Let $\varphi : V_\infty \to \mathbf{C}$ be the function defined by $\varphi(\mathbf{v}) = \Psi(Q(\mathbf{v})G) e(Q(\mathbf{v})H)$. Then the Fourier transform of φ is given by*

$$\hat{\varphi}(\mathbf{w}) = I\Psi\left(\frac{G}{H^2} Q(\mathbf{w})\right) e\left(-\frac{1}{H} Q(\mathbf{w})\right), \tag{12}$$

where $I = |H|_\infty^{-3/2} \gamma_\infty(HQ)$.

Proof. Essentially the same computation as in [11, Theorem 3.2], shows (12) with

$$I = \int_{V_\infty} \Psi\left(Q(\mathbf{v})G\right) e\left(Q(\mathbf{v})H\right) d\mathbf{v}.$$

We shall evaluate I explicitly. Since Q is definite, there exists a unique O_∞-lattice $M \subset V_\infty$ maximal with respect to the property $GQ(M) \subset O_\infty$. Then

$$I = \int_M e\big(Q(\mathbf{v})H\big)\,d\mathbf{v}.$$

We shall now see that the form HQ is integral on $H^{-1}M^*$. On the one hand, since $g > h$ we have $H^{-1}M^* = (H^{-1}G)(G^{-1}M^*) \subset t^{-1}G^{-1}M^*$. On the other hand, since M is maximal integral with respect to GQ, we have $t^{-1}G^{-1}M^* \subset M$. Thus

$$I = \operatorname{vol}\big(H^{-1}M^*\big)\big[M : H^{-1}M^*\big]^{1/2}\gamma_\infty(HQ).$$

To finish the computation, we observe

$$\begin{aligned}\operatorname{vol}\big(H^{-1}M^*\big)\big[M : H^{-1}M^*\big]^{1/2} &= \operatorname{vol}\big(H^{-1}M^*\big)^{1/2}\operatorname{vol}(M)^{1/2}\\ &= |H|_\infty^{-3/2}\big[\operatorname{vol}\big(M^*\big)\operatorname{vol}(M)\big]^{1/2}\\ &= |H|_\infty^{-3/2}.\end{aligned}$$

Notice that the last line uses the chosen normalization (11) for the Haar measure. □

Corollary 5.2. *Let* $z = \left[\begin{smallmatrix} y & xy^{-1} \\ 0 & y^{-1}\end{smallmatrix}\right] \in \mathfrak{D}$ *with* $x \neq 0$ *and let* $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0\end{smallmatrix}\right]$. *Then*

$$\theta_L(z) = |D|_\infty^{-1/2} I(z)\theta_{L^\sharp}(S\cdot z),$$

where $I(z) = |x|_\infty^{-3/2}\gamma_\infty(xQ)$.

Proof. Let $G = y^2$ and $H = x$. Since $z \in \mathfrak{D}$ we have $v_\infty(y^2) > v_\infty(x)$, so G and H satisfy the hypotheses of Proposition 5.1. Moreover

$$S\cdot z \sim \begin{bmatrix} 0 & -1 \\ 1 & 0\end{bmatrix}\begin{bmatrix} y & xy^{-1} \\ 0 & y^{-1}\end{bmatrix}\begin{bmatrix} 1 & 0 \\ -y^2x^{-1} & 1\end{bmatrix} = \begin{bmatrix} yx^{-1} & -x^{-1}y^{-1}x \\ 0 & y^{-1}x\end{bmatrix},$$

so applying Proposition 5.1 to the function

$$\varphi_z(\mathbf{v}) = \Psi\big(Q(\mathbf{v})y^2\big)e\big(Q(\mathbf{v})x\big)$$

we get

$$\hat{\varphi}_z(\mathbf{v}) = I(z)\varphi_{S\cdot z}(\mathbf{v}).$$

Applying the Poisson summation formula, we obtain

$$\sum_{\mathbf{v}\in tL}\varphi_z(\mathbf{v}) = \operatorname{vol}(V_\infty/tL)^{-1}\sum_{\mathbf{w}\in tL^\sharp}\hat{\varphi}_z(\mathbf{v}),$$

hence

$$\theta_L(z) = |D|_\infty^{-1/2} I(z) \theta_{L^\sharp}(S \cdot z).$$

(Notice that $\mathrm{vol}(V_\infty/tL) = |D|_\infty^{1/2}$.) □

Recall that for a ternary lattice (L, Q), its *adjoint* $(L^{\mathrm{ad}}, Q^{\mathrm{ad}})$ is defined by

$$L^{\mathrm{ad}} = L^\sharp \quad \text{and} \quad Q^{\mathrm{ad}} = DQ,$$

where $D = \det(L, Q)$. Alternatively, $(L^{\mathrm{ad}}, Q^{\mathrm{ad}}) = (\bigwedge^2 L, \bigwedge^2 Q)$, where $\bigwedge^2$ is the second exterior power operator.

Theorem 5.3. *Let (L, Q) and (L', Q') be isospectral definite ternary lattices. Then $(L^{\mathrm{ad}}, Q^{\mathrm{ad}})$ and $(L'^{\mathrm{ad}}, Q'^{\mathrm{ad}})$ are isospectral.*

Proof. Notice that $R(L^\sharp, Q, a) = R(L^{\mathrm{ad}}, Q^{\mathrm{ad}}, Da)$ for all $a \in K$, so it is enough to prove that $\theta_{L^\sharp} = \theta_{L'^\sharp}$.

Since L and L' are in the same genus by Corollary 4.2, we have $\det(L, Q) = \det(L', Q')$ and $\gamma_\infty(xQ) = \gamma_\infty(xQ')$. So, by Corollary 5.2, $\theta_{L^\sharp}(z) = \theta_{L'^\sharp}(z)$ for $x \neq 0$.

It remains to prove that $\theta_{L^\sharp}(z) = \theta_{L'^\sharp}(z)$ when $x = 0$. In this case, letting $y = t^{-m}$ we have, by (10),

$$\theta_{L^\sharp}(z) = \left|L^\sharp_{2m-2}\right|.$$

These numbers are determined by the series $\mathbf{T}_{L^\sharp}(u)$ defined in (4), which in turn depends only on the successive minima of $L^\sharp$ by Proposition 3.1. The successive minima of $L^\sharp$ are readily seen to be $(-\mu_3, -\mu_2, -\mu_1)$, where (μ_1, μ_2, μ_3) are the successive minima of L. We conclude by Proposition 3.1 that $|L^\sharp_{2m-2}| = |L'^\sharp_{2m-2}|$. Thus $\theta_{L^\sharp}(z) = \theta_{L'^\sharp}(z)$ for all z. □

6. Equivalence

Let (L, Q) and (L', Q') be two isospectral definite ternary lattices over A. Our aim in this section is to prove that they are equivalent.

We already proved in previous sections that they have the same successive minima (μ_1, μ_2, μ_3) and belong to the same genus – in particular they have the same determinant – and that their adjoints are also isospectral.

Proposition 6.1. *Assume $\mu_3 > \mu_2$. Then L_{μ_2} and L'_{μ_2} span equivalent binary A-lattices.*

Proof. Let $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ and $(\mathbf{v}'_1, \mathbf{v}'_2, \mathbf{v}'_3)$ and be reduced bases of L and L' respectively. Let $M = A\mathbf{v}_1 + A\mathbf{v}_2$ and $M' = A\mathbf{v}'_1 + A\mathbf{v}'_2$. Notice that $\det(M, Q)$ and is a minimal value for $(L^{\mathrm{ad}}, Q^{\mathrm{ad}})$, and that it is unique (up to a square in $\mathbf{F}_q$) with this property since $\mu_1 + \mu_2 < \mu_1 + \mu_3$.

Since $(L^{\mathrm{ad}}, Q^{\mathrm{ad}})$ and $(L'^{\mathrm{ad}}, Q'^{\mathrm{ad}})$ are isospectral by Theorem 5.3, we conclude that $\det(M, Q) = \det(M', Q')$. Since $\mu_3 > \mu_2$, $M_{\mu_2} = L_{\mu_2} = L'_{\mu_2} = M'_{\mu_2}$. Thus M and M' represent the same values up to degree μ_2 and have the same determinant. By [1, Theorem 4.1], we conclude that (M, Q) and (M', Q') are equivalent. □

Corollary 6.2. *If (L, Q) and (L', Q') are isospectral lattices with $\mu_3 > \mu_2$, then they have reduced bases such that the corresponding reduced Gram matrices have the form*

$$S = \begin{bmatrix} a & b & e \\ b & c & f \\ e & f & g \end{bmatrix} \quad \text{and} \quad S' = \begin{bmatrix} a & b & e' \\ b & c & f' \\ e' & f' & g' \end{bmatrix}. \tag{13}$$

Furthermore, g and g' may be assumed to have the same leading coefficient.

Proof. Immediate from Proposition 6.1. □

Lemma 6.3. *Let S and S' be matrices as in* (13) *representing isospectral forms and assume in addition $\mu_1 < \mu_2 < \mu_3$. Replacing if necessary the pair (e, f) by $(-e, -f)$ in the matrix S, the coefficients of S and S' satisfy the relation $a(g - g') = e^2 - e'^2$ and $b(e - e') = a(f - f')$. In particular,* $\deg(g - g') < \deg(e - e')$ *and* $\deg(f - f') < \deg(e - e')$.

Proof. The Gram matrix S^{ad} of the adjoint $(L^{\mathrm{ad}}, Q^{\mathrm{ad}})$ with respect to the reversed dual basis $\{\mathbf{v}_3^*, \mathbf{v}_2^*, \mathbf{v}_1^*\}$ is also reduced [6, Lemma 4] and has the form

$$S^{\mathrm{ad}} = \begin{bmatrix} ac - b^2 & be - af & * \\ be - af & ag - e^2 & * \\ * & * & * \end{bmatrix}.$$

By Theorem 5.3, the adjoints $(L^{\mathrm{ad}}, Q^{\mathrm{ad}})$ and $(L'^{\mathrm{ad}}, Q'^{\mathrm{ad}})$ are isospectral, so, by Proposition 6.1, the binary lattices $M = A\mathbf{v}_3^* + A\mathbf{v}_2^*$ and $M' = A\mathbf{v}_3'^* + A\mathbf{v}_2'^*$ are equivalent. Since their successive minima are distinct, the only automorphisms of these lattices are of the form $\mathrm{diag}(\pm 1, \pm 1)$, so we must have in particular

$$ag - e^2 = ag' - e'^2 \quad \text{and} \quad be - af = \pm(be' - af'). \tag{14}$$

Replacing $\mathbf{v}_3$ by $-\mathbf{v}_3$ if necessary, we can assume that the second equality holds with the $+1$ sign. So we get

$$a(g - g') = e^2 - e'^2 \quad \text{and} \quad b(e - e') = a(f - f'). \tag{15}$$

The degree inequalities follow immediately from the fact that $\deg(e + e') < \deg a$ and $\deg b < \deg a$ since S and S' are reduced. □

Lemma 6.4. *Let $M = A\mathbf{v}_1 + A\mathbf{v}_2 \subset L$. Then for every $\mathbf{w} \in M \setminus \{0\}$ we have*

$$\deg B(\mathbf{w}, \mathbf{v}_3) < \deg Q(\mathbf{w}).$$

Proof. Write $\mathbf{w} = r\mathbf{v}_1 + s\mathbf{v}_2$ with $r, s \in A$. Then

$$\begin{aligned} \deg B(\mathbf{w}, \mathbf{v}_3) &\leqslant \sup\{\deg r + \deg e, \deg s + \deg f\} \\ &< \sup\{2\deg r + \mu_1, 2\deg s + \mu_2\} \\ &= \deg Q(\mathbf{w}). \qquad \square \end{aligned}$$

Our next task is to show that by modifying suitably the reduced bases, the last columns of the matrices in (13) can be made equal.

The case $\mu_1 < \mu_2 < \mu_3$, $\mu_1 \equiv \mu_2 \pmod 2$.

Theorem 6.5. *Let (L, Q) and (L', Q') be isospectral ternary lattices with strictly increasing minima sequence $\mu_1 < \mu_2 < \mu_3$ and $\mu_1 \equiv \mu_2 \pmod 2$. Then they are equivalent.*

Proof. Let S and S' be their corresponding Gram matrices as in (13). Let $M = A\mathbf{v}_1 + A\mathbf{v}_2 \subset L$. Since Q represents g', there exists $\mathbf{v} \in L$ such that $Q(\mathbf{v}) = g'$. Note that for parity reasons $\mathbf{v} \notin M$, so it is of the form $\mathbf{v} = \lambda\mathbf{v}_3 + \mathbf{w}$ with $\lambda \in \mathbf{F}_q^\times$ and $\mathbf{w} \in M$ with $\deg Q(\mathbf{w}) < \mu_3$. We have

$$g' = Q(\mathbf{v}) = \lambda^2 g + \lambda B(\mathbf{w}, \mathbf{v}_3) + Q(\mathbf{w}).$$

Comparing leading coefficients we have $\lambda^2 = 1$. Hence

$$g' - g = Q(\mathbf{w}) \pm B(\mathbf{w}, \mathbf{v}_3).$$

If $\mathbf{w} \neq 0$, then by Lemma 6.4 we get $\deg(g' - g) = \deg Q(\mathbf{w}) \geqslant \mu_1$, which contradicts the inequality $\deg(g' - g) < \deg(e' - e) < \mu_1$ of Lemma 6.3.

Thus $g = g'$ and $e^2 = e'^2$. If $e = e'$, then $f = f'$ by (15) and we are done. So assume $e' = -e \neq 0$ and fix $z \in \mathbf{F}_q^\times$ such that $b + ze \neq 0$ (the reason for this choice of z will become apparent below). Since Q and Q' represent in particular the same polynomials, for each $x \in \mathbf{F}_q$ the equation

$$Q(x\mathbf{v}_1 + \mathbf{v}_2 + z\mathbf{v}_3) = Q'(u\mathbf{v}_1 + v\mathbf{v}_2 + z\mathbf{v}_1) \tag{16}$$

has a polynomial solution (u, v). Subtracting $z^2 g$ from both sides and using Lemma 6.4 we conclude that $\deg Q'(u\mathbf{v}_1 + v\mathbf{v}_2) = \mu_2$, so $v \in \mathbf{F}_q$.

Suppose first that for some $x \in \mathbf{F}_q$, there is a solution (u, v) to (16) with $v = 1$. Then we have

$$\big(x^2 - u^2\big)a + 2(x - u)b + 2(f - f') + 2e(x + u)z = 0. \tag{17}$$

Since $\deg(f - f') < \deg e$ by Lemma 6.3, the above equality implies $x^2 = u^2$. If $x = u$, then (17) reduces to

$$f - f' = -2eu$$

and for degree reasons we must have $f = f'$. By (15) we get $b = 0$ and the transformation $\mathbf{v}_2 \mapsto -\mathbf{v}_2$ takes S into S'. If $x = -u$, then (17) reduces to

$$f - f' = 2bu$$

which similarly implies $f = f'$ since $\deg(f - f') < \deg b$ by (15). We conclude as in the previous case.

Assume now that for all x all solutions (u, v) to (16) have $v \neq 1$. Then, by the pigeonhole principle, there must be a pair $(x_1, x_2) \in \mathbf{F}_q^2$, $x_1 \neq x_2$, such that the equations

$$\begin{cases} Q(x_1\mathbf{v}_1 + \mathbf{v}_2 + z\mathbf{v}_3) = Q'(u_1\mathbf{v}_1 + v\mathbf{v}_2 + z\mathbf{v}_1), \\ Q(x_2\mathbf{v}_1 + \mathbf{v}_2 + z\mathbf{v}_3) = Q'(u_2\mathbf{v}_1 + v\mathbf{v}_2 + z\mathbf{v}_1) \end{cases} \tag{18}$$

have solutions (u_1, v) and (u_2, v) (with a common v). Taking the difference of the two equations in (18), we get

$$(x_1 - x_2)\big[a(x_1 + x_2) + 2b + 2ez\big] = (u_1 - u_2)\big[a(u_1 + u_2) + 2bv - 2ez\big], \tag{19}$$

and comparing degrees we see that $u_1^2 - u_2^2 = x_1^2 - x_2^2$. In particular u_1 and u_2 must be constant. Taking $u_1 = u \in \mathbf{F}_q$ in (16) we get

$$\big(v^2 - 1\big)c = a\big(x^2 - u^2\big) + 2b(x - uv) + 2(f - f'v)z + 2e(u + 2)z.$$

Since all the terms on the right-hand side have degree $< \mu_2 = \deg c$, we must have $v^2 = 1$. Having already excluded the case $v = 1$, the only allowed value is $v = -1$. Substituting this value in (19), cancelling the equal terms and bringing all terms to one side of the equation, we get

$$(u_1 - u_2 + x_1 - x_2)(b + ez) = 0.$$

Since we have taken the precaution of choosing $z \in \mathbf{F}_q^\times$ so that $b + ez \neq 0$, we conclude $u_1 - u_2 = -x_1 + x_2$, which combined with the previously established equality $u_1^2 - u_2^2 = x_1^2 - x_2^2$ yields $u_1 = -x_1$ and $u_2 = -x_2$. Substituting in the first equation of (18) we get $f = -f'$. Then the transformation $\mathbf{v}_3 \mapsto -\mathbf{v}_3$ takes S into S'. □

The case $\mu_1 = \mu_2 < \mu_3$. Assume that (L, Q) and (L', Q') are isospectral with $\mu_1 = \mu_2$ and let S and S' be their Gram matrices as in Corollary 6.2.

The first step is to show after a suitable change of basis we can also assume $g = g'$. Since Q represents g', we can write $Q(r\mathbf{v}_1 + s\mathbf{v}_2 + t\mathbf{v}_3) = g'$. Comparing leading coefficients, we see $t^2 = 1$, so there is no loss of generality in assuming $t = 1$. Consider the transformation

$$U = \begin{bmatrix} 1 & 0 & r \\ 0 & 1 & s \\ 0 & 0 & 1 \end{bmatrix}.$$

Then the matrix $S'' = USU^t$ has the form

$$\begin{bmatrix} a & b & E \\ b & c & F \\ E & F & g' \end{bmatrix}.$$

Since $\det(S'') = \det(S')$, we have

$$Q_0(-F, E) = Q_0(-f', e'),$$

where $Q_0(X, Y) = aX^2 + 2bXY + cZ^2$. Since Q_0 is definite, $\deg Q_0(-F, E) = \max\{2\deg E + \mu_1, 2\deg F + \mu_1\}$ and since S' is reduced, $\deg Q_0(-f', e') < 3\mu_1$ and hence $\deg E < \mu_1$ and $\deg F < \mu_1$. This shows that S'' is reduced, i.e., we can assume henceforth $g = g'$ without loss of generality.

For each $(x, y, z) \in \mathbf{F}_q^3$, the equation

$$Q(x\mathbf{v}_1 + y\mathbf{v}_2 + z\mathbf{v}_3) = Q'(x'\mathbf{v}_1 + y'\mathbf{v}_2 + z'\mathbf{v}_3) \tag{20}$$

has a solution (x', y', z'), where (x', y', z') are *a priori* polynomials. By taking leading coefficients, we see $z^2 = z'^2$, so z' is in $\mathbf{F}_q$. Subtracting the term $z^2 g = z'^2 g'$ on both sides of (20), and applying Lemma 6.4, we get

$$\deg Q(x\mathbf{v}_1 + y\mathbf{v}_2) = \deg Q'(x'\mathbf{v}_1 + y'\mathbf{v}_2),$$

which immediately implies $x', y' \in \mathbf{F}_q$.

Lemma 6.6. *Assume that* Q *and* Q' *are ternary definite isospectral quadratic forms with* $\mu_1 = \mu_2$, *Gram matrices as in Corollary* 6.2 *and the additional condition* $g = g'$. *Then* $\operatorname{span}\{e, f\} = \operatorname{span}\{e', f'\}$.

Proof. We shall show $\operatorname{span}\{e, f\} \subset \operatorname{span}\{e', f'\}$ and conclude by symmetry. If $e = f = 0$ there is nothing to prove, so assume $(e, f) \neq (0, 0)$. Fix $(x, y) \in \mathbf{F}_q^2$ such that $xe + yf \neq 0$. Then, for all $z \in \mathbf{F}_q$, the equation

$$Q(x, y, z) = Q'(u, v, z) \tag{21}$$

has a solution $(u, v) \in \mathbf{F}_q^2$. Taking leading coefficients, we see that (u, v) must satisfy $u^2 - \delta v^2 = x^2 - \delta y^2$, that is, there are at most $q + 1$ possible pairs (u, v). Up to sign, there are at most $(q + 1)/2$ possibilities for (u, v). Since $q > (q + 1)/2$, and the left-hand side of (21) takes q different values as z runs over $\mathbf{F}_q$, there must be $z_1 \neq z_2$ in $\mathbf{F}_q$ and $(u, v) \in \mathbf{F}_q^2$ such that

$$Q(x, y, z_1) = Q'(u, v, z_1) \quad \text{and} \quad Q(x, y, z_2) = Q'(\epsilon u, \epsilon v, z_2), \tag{22}$$

where $\epsilon = \pm 1$. Subtracting the two equations we get

$$(z_1 - z_2)(xe + yf) = (z_1 - \epsilon z_2)(ue' + vf'), \tag{23}$$

which shows $xe + yf \in \operatorname{span}\{e', f'\}$. □

Lemma 6.7. *Let Q_0 be a binary definite quadratic form with $\mu_1 = \mu_2$ and let a be a polynomial of degree μ_1 represented by Q_0. Then $\operatorname{Aut}(Q_0)$ acts transitively on the set $\{(x, y) \in \mathbf{F}_q^2 \colon\ Q_0(x, y) = a\}$.*

Proof. We can assume $Q_0 = aX^2 + 2bXY + cY^2$, where a, b, c are relatively prime and $\deg(a) = \deg(c) > \deg(b)$.

If a, b, c are linearly independent over $\mathbf{F}_q$, then $Q_0(x, y) = a$ implies $x = \pm 1$ and $y = 0$. We get a similar conclusion if $b = 0$ and a, c are linearly independent. If $b = 0$ and a is proportional to c, Q_0 is a multiple of a form over $\mathbf{F}_q$ and the result is well known. The only case left is when a, b, c are linearly dependent and $b \neq 0$. In this case, write $c = -\delta a - 2mb$, where δ is a non-square and $m \in \mathbf{F}_q$, $m \neq 0$. Suppose $Q_0(x, y) = a$. If $y = 0$ we are done, so we may assume $y \neq 0$. We have $Q_0(x, y) = a(x^2 - \delta y^2) + 2by(x - my)$, so by linear independence of a and b we get the relations

$$x^2 - \delta y^2 = 1 \quad \text{and} \quad x - my = 0,$$

which ensure that $U = \left[\begin{smallmatrix} x & \delta y \\ y & x \end{smallmatrix}\right]$ is an automorphism of Q_0. □

Lemma 6.8. *Let $F, G \in \mathbf{F}_q[X]$ be polynomials of degree 2 such that $F(x) \equiv G(x) \pmod{\mathbf{F}_q^{*2}}$ for all $x \in \mathbf{F}_q$. Then $F = u^2 G$, where $u \in \mathbf{F}_q$.*

Proof. The hypothesis implies in particular that the polynomials F and G have the same roots in $\mathbf{F}_q$ (if any) so there is no loss of generality in assuming that they are irreducible.

If F and G are relatively prime, then the equation $Y^2 = F(X)G(X)$ defines an elliptic curve with at least $2q$ points over $\mathbf{F}_q$. This contradicts Hasse's bound [10, Chapter V] if $q > 5$. For $q = 3, 5$ the assertion is easily verified by direct computation. □

Theorem 6.9. *If two Q and Q' ternary definite quadratic forms are isospectral with $\mu_1 = \mu_2$ or $\mu_2 = \mu_3$, then they are equivalent.*

Proof. If $\mu_2 = \mu_3$, we replace (L, Q) and (L', Q') by their adjoints which in this case satisfy $\mu_1(Q^{\mathrm{ad}}) = \mu_1 + \mu_2 = \mu_1 + \mu_3 = \mu_2(Q'^{\mathrm{ad}})$. So we can limit ourselves to the case $\mu_1 = \mu_2$.

With the notation and hypotheses of Lemma 6.6, let $E = \operatorname{span}\{e, f\} = \operatorname{span}\{e', f'\}$. If $\dim E = 0$, there is nothing to prove; we will deal with the other two cases.

Suppose first $\dim E = 1$. Let $h \in E$ be a monic polynomial of degree d and write $e = e_d h$, $f = f_d h$, $e = e'_d h$, $f = f'_d h$, where e_d, f_d, e'_d, f'_d, are in $\mathbf{F}_q$.

Let $Q_0(X, Y) = Q(X, Y, 0) = Q'(X, Y, 0)$. The equality $\det(Q) = \det(Q')$ implies $Q_0(-f, e) = Q_0(-f', e')$. Dividing by h^2 we get $Q_0(-f_d, e_d) = Q_0(-f'_d, e'_d)$. Applying Lemma 6.7, there is an automorphism U of Q_0 such that $U\left[\begin{smallmatrix} -f \\ e \end{smallmatrix}\right] = \left[\begin{smallmatrix} -f' \\ e' \end{smallmatrix}\right]$. Then

$$W = \begin{bmatrix} U & 0 \\ 0 & 1 \end{bmatrix}$$

satisfies $QW = Q'$, as desired.

Suppose now $\dim E = 2$. By Lemma 6.6, there exists a matrix $M \in \mathbf{GL}_2(\mathbf{F}_q)$ such that

$$\begin{bmatrix} -f \\ e \end{bmatrix} = M \begin{bmatrix} -f' \\ e' \end{bmatrix}.$$

We shall prove that M is an automorphism of Q_0. Let $(x, y) \in \mathbf{F}_q^2$, $(x, y) \neq (0, 0)$, and let $(u, v) \in \mathbf{F}_q^2$ and z_1, z_2 as in the proof of Lemma 6.6. We get from (23)

$$\begin{bmatrix} u \\ v \end{bmatrix} = h_{x,y} M \begin{bmatrix} x \\ y \end{bmatrix}$$

with $h_{x,y} = (z_1 - z_2)/(z_1 - \epsilon z_2) \in \mathbf{F}_q^\times$ (depending *a priori* on (x, y)).

Let $R = X^2 - \delta Y^2$. Since $R(x, y) = R(u, v)$, substituting we have $R(x, y) = h_{x,y}^2 (RM)(x, y)$. Thus the quadratic forms R and RM represent the same elements of $\mathbf{F}_q$ up to squares, i.e. the quadratic polynomials $F(t) = R(t, 1)$ and $G(t) = (RM)(t, 1)$ satisfy the hypothesis of Lemma 6.8, hence $R = s^2 RM$ for some $s \in \mathbf{F}_q^\times$, i.e. $h_{x,y}^2 = s^2$ for all $(x, y) \in \mathbf{F}_q^2$.

Now from the equality $\det(Q) = \det(Q')$, we get $Q_0(-f, e) = Q_0(-f', e')$. Let $d = \max\{\deg e, \deg f\}$ and take coefficients of degree $\mu_1 + 2d$ in this equality. Then

$$R(-f_d, e_d) = R\big(-f'_d, e'_d\big) \neq 0,$$

and therefore $s^2 = 1$ and $R = RM$.

If $h_{x,y} = 1$, we conclude from the first equation in (22) that $Q_0(x, y) = Q_0(u, v)$. If $h_{x,y} = -1$, then $\epsilon = -1$ and $z_1 = 0$ and we conclude again from (22) that $Q_0(x, y) = Q_0(u, v)$. Thus $Q_0 = Q_0 M$; this condition ensures that

$$N := \begin{bmatrix} M & 0 \\ 0 & 1 \end{bmatrix}$$

satisfies $Q' = QN$. □

The case $\mu_1 < \mu_2 < \mu_3$, $\mu_1 \equiv \mu_3 \pmod 2$. Let (W, ϕ) be a quadratic space over $\mathbf{F}_q$ of dimension n and rank r. Recall that the Gauss sum associated to (W, ϕ) is defined by

$$\Gamma(W, \phi) = \sum_{w \in W} \chi\big(\phi(w)\big),$$

where $\chi : \mathbf{F}_q \to \mathbf{C}^\times$ is the character defined by $\chi(u) = \exp(2\pi i \operatorname{Tr}(u)/p)$ and $\operatorname{Tr} : \mathbf{F}_q \to \mathbf{F}_p$ is the trace to the prime field $\mathbf{F}_p$.

It is immediate from the definition that Γ is multiplicative on orthogonal sums. Let $W_1 = \operatorname{rad}(W,\phi)$ and let $W_0 \subset W$ be a complement of W_1. Then $\Gamma(W,\phi) = \Gamma(W_0,\phi_0)\Gamma(W_1,0)$, where $\phi_0 = \phi|_{W_0}$. Clearly $\Gamma(W_1,0) = q^{n-r}$. Writing $\phi_0 = \sum_{i=1}^{r} a_i X_i^2$ in some orthogonal basis of W_0, we get $\Gamma(W_0,\phi_0) = \Gamma(\mathbf{F}_q,\langle a_1\rangle)\cdots\Gamma(\mathbf{F}_q,\langle a_r\rangle)$. Using further the property that $\Gamma(\mathbf{F}_q,\langle a_i\rangle) = \psi(a_i)G$, where $G = \Gamma(\mathbf{F}_q,\langle 1\rangle)$ and $\psi : \mathbf{F}_q^\times \to \{\pm 1\}$ is the quadratic character (see e.g. [7, Proposition 6.3.1]), we get

$$\Gamma(W,\phi) = q^{n-r}\psi(\det\phi_0)G^r. \tag{24}$$

Note that in particular, $\Gamma(W,\phi) = \Gamma(W,\phi')$ if and only if $(W,\phi) \simeq (W,\phi')$.

Definition 2. Let $\Phi = (\phi_1,\phi_2,\dots,\phi_m)$ and $\Phi' = (\phi_1',\phi_2',\dots,\phi_m')$ be systems of quadratic forms on W, i.e. quadratic mappings $W \to \mathbf{F}_q^m$. We shall say that Φ and Φ' are *isospectral* if $|\Phi^{-1}(\mathbf{y})| = |\Phi'^{-1}(\mathbf{y})|$ for all $\mathbf{y} \in \mathbf{F}_q^m$.

The following theorem is a particular case of a result by Carlitz [2, Theorems 3.2–3.3] on systems of polynomial equations.

Theorem 6.10 *(Carlitz). Two systems of quadratic forms Φ and Φ' as above are isospectral if and only if*

$$\Gamma\left(\sum_{i=1}^{m} x_i\phi_i\right) = \Gamma\left(\sum_{i=1}^{m} x_i\phi_i'\right)$$

for all $(x_1,x_2,\dots,x_m) \in \mathbf{F}_q^m$.

Let Q, Q' be isospectral definite quadratic forms with successive minima (μ_1,μ_2,μ_3) on L and let $W = L_{\mu_3}$. Write $Q(\mathbf{x}) = \sum_{i=0}^{\mu_3} Q_i(\mathbf{x})t^i$ (respectively $Q'(\mathbf{x}) = \sum_{i=0}^{\mu_3} Q_i'(\mathbf{x})t^i$). Then the systems $\Phi = (Q_0,\dots,Q_{\mu_3})$ and $\Phi' = (Q_0',\dots,Q_{\mu_3}')$ are isospectral. Let B, B_i, B', B_i' be the symmetric bilinear forms associated to Q, Q_i, Q', Q_i'. By Theorem 6.10 and (24), we have in particular

$$\det\left(\sum_{i=0}^{\mu_3} x_i B_i\right) \equiv \det\left(\sum_{i=0}^{\mu_3} x_i B_i'\right) \pmod{\mathbf{F}_q^{\times 2}} \tag{25}$$

for all $(x_0,x_2,\dots,x_{\mu_3}) \in \mathbf{F}_q^{\mu_3+1}$.

Let $k_1 = (\mu_3-\mu_1)/2$ and $k_2 = (\mu_3-\mu_2-1)/2$. We fix the basis

$$\left\{\mathbf{v}_1, t\mathbf{v}_1,\dots,t^{k_1}\mathbf{v}_1, \mathbf{v}_2, t\mathbf{v}_2,\dots,t^{k_2}\mathbf{v}_2, \mathbf{v}_3\right\} \tag{26}$$

of W and identify all the symmetric bilinear forms on W with their respective matrices in this basis.

Lemma 6.11. *With the notation above, we have*

$$\det\left(\sum_{i=0}^{\mu_3-1} x_i B_i\right) = \det\left(\sum_{i=0}^{\mu_3-1} x_i B_i'\right)$$

for all $(x_0,x_2,\dots,x_{\mu_3-1}) \in \mathbf{F}_q^{\mu_3}$.

Proof. Fix $(x_0, x_2, \ldots, x_{\mu_3-1}) \in \mathbf{F}_q^{\mu_3}$ and consider $\det(\sum_{i=0}^{\mu_3} x_i B_i)$ and $\det(\sum_{i=0}^{\mu_3} x_i B'_i)$ as polynomials in the variable x_{μ_3}. They have degree two in x_{μ_3}, the same leading coefficient $(= -\delta)$ and are equal up to squares of $\mathbf{F}_q^\times$ by (25), so, by Lemma 6.8, they must be equal as polynomials in x_{μ_3}. We conclude by taking $x_{\mu_3} = 0$. □

Lemma 6.12. *Let $m = (\mu_1 + \mu_3)/2$. Then for all $m \leqslant j \leqslant \mu_3$ we have $B'_j = B_j$.*

Proof. For $\mathbf{x} = (x, y, z) \in W$, we have $Q(\mathbf{x}) - Q'(\mathbf{x}) = 2(e - e')xz + 2(f - f')yz + (g - g')z^2$. By Lemma 6.3, all three terms have degrees $< m$. □

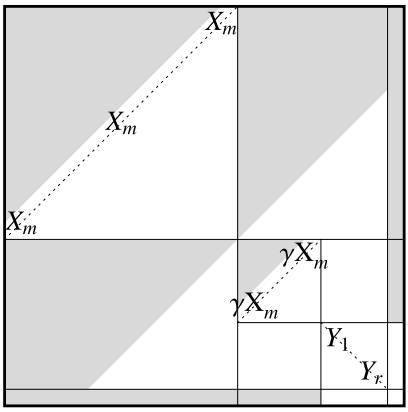
We shall use the following notation henceforth: $n = \dim W$, $s = \max\{m - \mu_2, -1\}$, $r = k_2 - s$. (Note that $n = k_1 + k_2 + 3 = (k_1 + 1) + (s + 1) + r + 1$.)

Lemma 6.13. *The forms B_j have the following properties*

(1) $B_l(t^i\mathbf{v}_1, t^j\mathbf{v}_1) = 0$ *for* $l \geqslant m$ *and* $i + j < k_1$;
(2) $B_m(t^i\mathbf{v}_1, t^j\mathbf{v}_1) = 1$ *for* $i + j = k_1$;
(3) $B_l(t^i\mathbf{v}_1, t^j\mathbf{v}_2) = 0$ *for* $l - i - j \geqslant \mu_1$;
(4) $B_l(t^i\mathbf{v}_2, t^j\mathbf{v}_2) = 0$ *for* $l \geqslant m$ *and* $i + j < s$;
(5) $B_m(t^i\mathbf{v}_2, t^j\mathbf{v}_2) = c_{\mu_2}$ *for* $i + j = s$;
(6) $B_l(t^i\mathbf{v}_1, \mathbf{v}_3) = 0$ *for* $l \geqslant m$ *and* $i \leqslant k_1$;
(7) $B_l(t^i\mathbf{v}_2, \mathbf{v}_3) = 0$ *for* $l \geqslant m$ *and* $i \leqslant s$.

Proof. The lemma follows immediately from the fact that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a reduced basis for $Q(\mathbf{x})$. □

Let $\mathcal{B} = X_m B_m + \sum_{j=0}^{r-1} X_{\mu_3-1-2j} B_{\mu_3-1-2j}$. It follows from Lemma 6.13 that the matrix of $\mathcal{B}$ in the basis (26) has the form



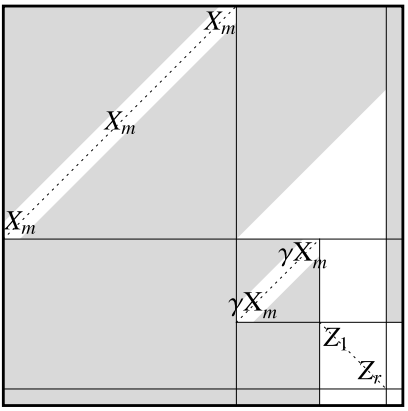
where the greyed areas consist entirely of zeros and the sizes of the blocs correspond to the partition $n = (k_1 + 1) + (s + 1) + (r) + (1)$. Here $Y_j = \mathcal{B}(t^{k_2+j-r}\mathbf{v}_2, t^{k_2+j-r}\mathbf{v}_2)$ for $j = 1, \ldots, r$ and $\gamma = c_{\mu_2}$.

Lemma 6.14. *Let $\mathcal{C} = (\rho_{ij})$ be the adjoint of the matrix $\mathcal{B}$ and let $M = X_m^{k_1+k_2+2-r} \prod_{j=0}^{r-1} X_{\mu_3-1-2j}$.*

(1) *When $i < n$, the coefficient of M in ρ_{ni} is equal to 0.*
(2) *The coefficient of M in ρ_{nn} is equal to $\pm\gamma^{k_2+1}$.*

(*Note that the entries of $\mathcal{C}$ are homogeneous polynomials of degree $n - 1$ in the variables X_j.*)

Proof. Leaving the bottom row untouched, we apply elementary row operations to clear the entries below the "diagonals" containing X_m. This can be accomplished in the ring $\mathbf{F}_q[X_m^{\pm 1}][X_{\mu_3-2r+1},\ldots,X_{\mu_3-1}]$. We get a matrix of the form



Note that all the coefficients above (and to the left of) Y_j are linear combinations of variables X_i with $i < 2j+2m-\mu_2$, so Z_j and Y_j have the same term in $X_{2j+2m-\mu_2}$, namely $\gamma X_{2j+2m-\mu_2}$.

The elementary row operations have not altered the minors of $\mathcal{B}$ along the bottom row (i.e. the determinants of the submatrices obtained by removing the bottom row and a column). It is clear from the shape of the above matrix that in these minors, only the product $Y_1\cdots Y_r$ can yield a term divisible by $\prod_{j=0}^{r-1} X_{\mu_3-1-2j}$. Thus the minors ρ_{ni} obtained by removing a column different from the last one ($i<n$) do not contain monomials divisible by $\prod_{j=0}^{r-1} X_{\mu_3-1-2j}$. The coefficient of M in the minor ρ_{nn} is $\pm\gamma^{r+s+1}$. □

Lemma 6.15. *For all $0 \leqslant i < m$ we have*

$$\det\bigl(X_iB_i'+\mathcal{B}\bigr)-\det(X_iB_i+\mathcal{B})=\pm\bigl(g_i'-g_i\bigr)\gamma^{r+s+1}X_iM+N,$$

where $M = X_m^{k_1+k_2+2-r}\prod_{j=0}^{r-1} X_{\mu_3-1-2j}$ and N is divisible by X_i^2.

Proof. Expanding as polynomials in X_i and separating the linear part, we have

$$\det\bigl(X_iB_i'+\mathcal{B}\bigr)-\det(X_iB_i+\mathcal{B})=\operatorname{Tr}\bigl(\mathcal{C}\bigl(B_i'-B_i\bigr)\bigr)X_i+\text{terms divisible by } X_i^2. \tag{27}$$

The matrix of $B_i'-B_i$ with respect to the basis (26) has zeros everywhere except possibly on the last row and the last column and $(B_i'-B_i)_{nn}=g_i'-g_i$. Combining this with Lemma 6.14 we get that the coefficient of M in $\operatorname{Tr}(\mathcal{C}(B_i'-B_i))$ is $\pm\gamma^{r+s+1}(g_i'-g_i)$. The lemma follows now immediately from (27). □

Corollary 6.16. *If $q > k_1+k_2+2-r$, then $g=g'$.*

Proof. A monomial of N that is equal to X_jM as functions on $\mathbf{F}_q$ must be of the form $X_j^{q^s}P$, where P is divisible by *all* the variables other than X_j. In particular $\deg P \geqslant r+1$, so $q^s \leqslant \dim L_{\mu_3}-(r+1) = k_1+k_2+2-r$, which implies $s=0$. Since $\det(X_iB_i'+\mathcal{B})=\det(X_iB_i+\mathcal{B})$ as functions, we must have $g_i=g_i'$ for $0\leqslant i<m$. Since $\deg(g-g')<\mu_1<m$ by Lemma 6.3, we must have $g=g'$. □

Theorem 6.17. *If $q > \max\{2+\mu_3-\mu_2, 2+\mu_2-\mu_1\}$ then Q and Q' are isometric.*

Proof. The condition on q ensures that both pairs (Q, Q') and $(Q^{\mathrm{ad}}, Q'^{\mathrm{ad}})$ satisfy the hypotheses of Corollary 6.16. Applying Corollary 6.16 to (Q, Q') we get $g = g'$ and hence $e^2 = e'^2$. Applying it to $(Q^{\mathrm{ad}}, Q'^{\mathrm{ad}})$, we get $cg - f^2 = cg' - f'^2$ and hence $f^2 = f'^2$.

There is no loss of generality in assuming $e = e'$. If $f = f'$ we are done, so assume $f = -f' \neq 0$. Comparing determinants we get $be = 0$. If $b = 0$, then the transformation $\mathbf{v}_2 \mapsto -\mathbf{v}_2$ changes f into $-f$ and leaves the rest alone. Similarly, if $e = 0$, the transformation $\mathbf{v}_3 \mapsto -\mathbf{v}_3$ changes f into $-f$ and leaves the other coefficients unaltered. □

Acknowledgment

We thank the referee for his/her careful reading and useful comments.

References

[1] Jean Bureau, Jorge Morales, Representations of definite binary $\mathbf{F}[t]$-lattices, Illinois J. Math., in press.
[2] L. Carlitz, Invariant theory of systems of equations in a finite field, J. Anal. Math. 3 (1954) 382–413.
[3] J.H. Conway, N.J.A. Sloane, Four-dimensional lattices with the same theta series, Int. Math. Res. Not. (4) (1992) 93–96.
[4] John H. Conway, The Sensual (Quadratic) Form, Carus Math. Monogr., vol. 26, Mathematical Association of America, Washington, DC, 1997, with the assistance of Francis Y.C. Fung.
[5] Dragomir Ž. Djoković, Hermitian matrices over polynomial rings, J. Algebra 43 (2) (1976) 359–374.
[6] Larry J. Gerstein, Definite quadratic forms over $\mathbb{F}_q[x]$, J. Algebra 268 (1) (2003) 252–263.
[7] Kenneth F. Ireland, Michael I. Rosen, A classical introduction to modern number theory, Grad. Texts in Math., vol. 84, Springer-Verlag, New York, 1982, revised edition of ıt Elements of number theory, MR MR661047 (83g:12001).
[8] Yoshiyuki Kitaoka, Positive definite quadratic forms with the same representation numbers, Arch. Math. (Basel) 28 (5) (1977) 495–497.
[9] J. Milnor, Eigenvalues of the Laplace operator on certain manifolds, Proc. Natl. Acad. Sci. USA 51 (1964) 542.
[10] Michael Rosen, Number Theory in Function Fields, Grad. Texts in Math., vol. 210, Springer-Verlag, New York, 2002.
[11] Holly J. Rosson, Theta series of quaternion algebras over function fields, J. Number Theory 94 (1) (2002) 49–79.
[12] Hans-Georg Rück, Theta series of imaginary quadratic function fields, Manuscripta Math. 88 (3) (1995) 387–407.
[13] Winfried Scharlau, Quadratic and Hermitian Forms, Grundlehren Math. Wiss. (Fundamental Principles of Mathematical Sciences), vol. 270, Springer-Verlag, Berlin, 1985.
[14] Alexander Schiemann, Ein Beispiel positiv definiter quadratischer Formen der Dimension 4 mit gleichen Darstellungszahlen, Arch. Math. (Basel) 54 (4) (1990) 372–375.
[15] Alexander Schiemann, Ternary positive definite quadratic forms are determined by their theta series, Math. Ann. 308 (3) (1997) 507–517.
[16] G.L. Watson, Determination of a binary quadratic form by its values at integer points, Mathematika 26 (1) (1979) 72–75.
[17] André Weil, Sur certains groupes d'opérateurs unitaires, Acta Math. 111 (1964) 143–211.