Invariants of ternary quadratic forms

Irene I. Bouw

This note provides details on [2, Section 4]. The main goal is to define and compute the Gross–Keating invariants a_1, a_2, a_3 of ternary quadratic forms over $\mathbb{Z}_\ell$ (Definition 1.2). If $a_1 \equiv a_2 \bmod 2$ and $a_3 > a_2$ we define an additional invariant $\varepsilon \in \{\pm 1\}$ (Definition 2.7, Definition 4.8). If $\ell \neq 2$ every quadratic form over $\mathbb{Z}_\ell$ is diagonalizable, and it is easy to determine these invariants from the diagonal form (Section 2). If $\ell = 2$ not every quadratic form in diagonalizable. We determine a normal form in Section 3 and compute the invariants in terms of this normal form (Section 4). In Section 5 we determine explicitly when a ternary quadratic form is anisotropic. A complete table can be found in Proposition 5.2 (non diagonalizable case) and Theorem 5.7 (diagonalizable case). In Section 6, we give an alternative definition of the Gross–Keating invariants for anisotropic quadratic forms. The results of Section 6 are due to Stefan Wewers, following a hint in [2, Section 4].

Our main reference on quadratic forms over $\mathbb{Z}_\ell$ is [1, Chapter 8]. Most of the of the result of this paper can also be found in the work of Yang, in a somewhat different form. The Gross–Keating invariants are computed in [4, Appendix B]. The question whether a given form over $\mathbb{Z}_2$ is isotropic or not (Section 5) is discussed in [5].

I would like to thank M. Rapoport for comments on an earlier version.

1 Definition of the invariants a_i

In this section we give the general definition of the Gross–Keating invariants a_i of quadratic forms over $\mathbb{Z}_\ell$ which are used in [2].

Let L be a free $\mathbb{Z}_\ell$-module of rank n and choose a (for the moment) arbitrary basis $\boldsymbol{\psi} = \{\psi_1, \psi_2, \ldots, \psi_n\}$. For the application to [2] we are only interested in the case $n = 3$ of ternary quadratic forms. Let (L, Q) be an integral quadratic form over $\mathbb{Z}_\ell$, that is,

$$Q(x) = Q(\sum x_i \psi_i) = \sum_{i \leq j} b_{ij} x_i x_j, \qquad \text{with } b_{ij} \in \mathbb{Z}_\ell.$$

Put $b_{ji} = b_{ij}$ for $j > i$. If we want to stress the dependence of the b_{ij} on the basis, we write $b_{ij}(\boldsymbol{\psi})$ for b_{ij}. We write $(x, y) = Q(x + y) - Q(x) - Q(y)$ for the corresponding symmetric bilinear form and $B = ((\psi_i, \psi_j))$ for the corresponding matrix. Note that

$$B = \left(B_{ij}\right), \qquad \text{where} \qquad B_{ij} = \begin{cases} b_{ij}, & \text{if } i < j, \\ 2b_{ij}, & \text{if } i = j. \end{cases}$$

In the rest of the paper we only use the b_{ij} and not the B_{ij}, for simplicity. We denote by ord the ℓ-adic valuation on $\mathbb{Z}_\ell$. We always suppose that Q is regular, that is, $\det(B) \neq 0$.

Changing the basis multiplies the determinant of B by an element of $(\mathbb{Z}_\ell^\times)^2$. Therefore the determinant is a well defined element of $\mathbb{Z}_\ell/(\mathbb{Z}_\ell^\times)^2$.

Lemma 1.1 *Suppose that either $\ell \neq 2$ or n is odd. Define*

$$\Delta = \Delta(Q) = \frac{1}{2}\det(B).$$

Then $\Delta \in \mathbb{Z}_\ell$.

Proof: The lemma is obvious if $\ell \neq 2$. Suppose that $\ell = 2$ and n odd. Write $\Delta = \sum_{\sigma\in S_n} 2^{\delta(\sigma)} d(\sigma)$, where $d(\sigma) = (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=1}^n b_{i\sigma(i)}$ and $\delta(\sigma)+1$ is the number of $i \in \{1,2,\ldots,n\}$ which are fixed by σ. The only problematic terms are those with $\delta(\sigma) = -1$. Suppose that σ acts without fixed points on $\{1,2,\ldots,n\}$. Then $\sigma^{-1} \neq \sigma$, since n is odd. The matrix $((\psi_i, \psi_j))$ is symmetric. It follows that $d(\sigma) = d(\sigma^{-1})$, hence $2^{\delta(\sigma)}d(\sigma) + 2^{\delta(\sigma^{-1})}d(\sigma^{-1}) \in \mathbb{Z}_\ell$. $\square$

We now come to the definition of the Gross–Keating invariants of a quadratic form. Let $\boldsymbol{\psi} = (\psi_1, \psi_2, \ldots, \psi_n)$ be a basis of L. We write $S(\boldsymbol{\psi})$ for the set of tuples $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}^n$ such that

$$y_1 \leq y_2 \leq \ldots \leq y_n, \qquad \frac{y_i + y_j}{2} \leq \mathrm{ord}(b_{ij}(\boldsymbol{\psi})) \quad \text{for } 1 \leq i \leq j \leq n. \tag{1}$$

Let $S = \cup S(\boldsymbol{\psi})$. We order tuples $(y_1, \ldots, y_n) \in S$ lexicographically, as follows. For given $(y_1, \ldots, y_n)$, $(z_1, \ldots, z_n) \in S$, let j be the largest integer such that $y_i = z_i$ for all $i < j$. Then $(y_1, \ldots, y_n) > (z_1, \ldots, z_n)$ if $y_j > z_j$.

Definition 1.2 The *Gross–Keating invariants* $a_1, \ldots, a_n$ are the maximum of $(y_1, \ldots, y_n) \in S$. A basis $\boldsymbol{\psi}$ is called *optimal* if $(a_1, \ldots, a_n) \in S(\boldsymbol{\psi})$.

If $\boldsymbol{\psi}$ is optimal, then

$$a_i + a_j \leq 2\mathrm{ord}(b_{ij}(\boldsymbol{\psi})) \quad \text{for} \quad 1 \leq i \leq j \leq n, \quad \text{and} \quad a_1 \leq a_2 \leq \cdots \leq a_n. \tag{2}$$

Since Δ is well defined up to $(\mathbb{Z}_\ell^\times)^2$, the integer $\mathrm{ord}(\Delta)$ is well defined. The following lemma will be useful in computing the Gross–Keating invariants.

Lemma 1.3 *(a) Suppose that n is odd, then*

$$\mathrm{ord}(\Delta) \geq a_1 + a_2 + \cdots + a_n.$$

(b) We have

$$a_1 = \min_{x,y\in L} \mathrm{ord}\,(x,y)\,.$$

(c) Define $\rho := \min_A \mathrm{ord}(\det(A))$, where A runs through the 2 by 2 minors of B. Then

$$a_1 + a_2 \leq \rho.$$

Proof: This lemma is proved in [4, Lemma B.1, Lemma B.2]. Note that the matrix T in [4] differs by a factor 2 from our matrix B. Let $\boldsymbol{\varphi}$ be an optimal basis. We use the notation of the proof of Lemma 1.1.

First suppose that $\ell = 2$. Write $\mathbb{S}$ for the set of equivalence classes in S_n under the equivalence relation $\sigma \sim \sigma^{-1}$. The proof of Lemma 1.1 shows that $\Delta = \sum_{\sigma\in\mathbb{S}} (-1)^{\mathrm{sgn}(\sigma)} 2^{\delta'(\sigma)} d(\sigma)$, where $\delta'(\sigma) \geq 0$. The choice of $\boldsymbol{\varphi}$ implies that

$$\mathrm{ord}(2^{\delta'(\sigma)} d(\sigma)) = \delta'(\sigma) + \mathrm{ord}(\prod_i b_{i\sigma(i)}) \geq \sum_{i=1}^n \frac{a_i + a_{\sigma(i)}}{2} = \sum_{i=1}^n a_i.$$

This proves (a) in this case.

If $\ell \neq 2$, define $\delta'(\sigma) = 0$ for all $\sigma \in S_n$. Then the proof works also in this case.

Since $a_1 \leq a_2 \leq \cdots \leq a_n$, it follows from (2) that $\mathrm{ord}(b_{ij}(\boldsymbol{\varphi})) \geq a_1$ for all $i \leq j$. On the other hand, it is obvious that $a_1 \geq \min_{x,y\in L} \mathrm{ord}\,(x,y)$. This implies (b).

Part (c) is similar to (a), compare to Lemma B1.ii in [4]. Let $i_1, i_2, j_1, j_2 \in \{1, 2, \ldots, n\}$ be integers such that $i_1 \neq i_2$ and $j_1 \neq j_2$. Write $B(i_1, i_2; j_1, j_2)$ for the corresponding minor of

B. After renumbering, we may suppose that $i_1 \neq j_2$ and $i_2 \neq j_1$. Then $\det(B(i_1, i_2; j_1, j_2)) = \pm(2^\alpha b_{i_1,j_1} b_{i_2,j_2} - b_{i_1,j_2} b_{i_2 j_1})$, where $\alpha \in \{0,1,2\}$ is the number of equalities $i_1 = j_1, i_2 = j_2$ that hold. We conclude that $\mathrm{ord}(\det(B(i_1, i_2; j_1, j_2)) \geq (a_{i_1} + a_{i_2} + a_{j_1} + a_{j_2})/2 \geq a_1 + a_2$. (Here we use that $a_1 \leq a_2 \leq \cdots \leq a_n$ and $i_1 \neq i_2$ and $j_1 \neq j_2$.) This proves (c).

□

2 Definition of the Gross–Keating invariants for $\ell \neq 2$

We start this section with an elementary lemma which holds without assumption on ℓ.

Lemma 2.1 *Choose a basis $\boldsymbol{\psi} = (\psi_1, \ldots, \psi_n)$ of L. Let $\gamma_1, \ldots, \gamma_m \in L$ be linearly independent. The following are equivalent.*

(a) There exists $\gamma_{m+1}, \ldots, \gamma_n \in L$ such that the (γ_i) form a basis.

(b) The matrix $(\gamma_1, \ldots, \gamma_m)$, expressing the γ_i in terms of the basis $\boldsymbol{\psi}$, contains a $m \times m$ minor whose determinant is a p-adic unit.

(c) If $\sum_{i=1}^n v_i \gamma_i \in L$ for some $v_i \in \mathbb{Q}_\ell$, then $v_i \in \mathbb{Z}_\ell$.

Proof: This is straightforward. See also [1, Chapter 8, Lemma 2.1]. □

In particular, a vector $\alpha = \sum_i \alpha_i \psi_i \in L$ is part of a basis of L if and only if $\min_j \mathrm{ord}(\alpha_j) = 0$. We call such vectors *primitive*.

We have that

$$2\,(x, y) = 2[Q(x + y) - Q(x) - Q(y)] = (x + y, x + y) - (x, x) - (y, y)\,. \tag{3}$$

If $\ell \neq 2$, this implies that

$$\min_{x,y \in L} \mathrm{ord}\,(x, y) = \min_{x \in L} \mathrm{ord}\,(x, x)\,. \tag{4}$$

In the rest of this section, we suppose that $\ell \neq 2$. There is a $x \in L$ for which the minimum in (4) is attained. This vector x is primitive. Lemma 2.1 implies that x can be extended to a basis of L. We will see in Section 4 that (4) does not hold for $\ell = 2$; this is the main reason why things are more difficult for $\ell = 2$.

Proposition 2.2 *Suppose that $\ell \neq 2$. Then there exists a basis $\boldsymbol{\psi}$ of L such that*

$$Q(x) = Q(\sum x_i \psi_i) = \sum_i b_{ii} x_i^2, \qquad \textit{where} \quad \mathrm{ord}(b_{11}) \leq \mathrm{ord}(b_{22}) \leq \ldots \leq \mathrm{ord}(b_{nn}).$$

Proof: Our proof follows [1, Chapter 8, Theorem 3.1].

The discussion before the statement of the theorem shows that we may choose φ_1 such that

$$\mathrm{ord}(Q(\varphi_1)) = \mathrm{ord}\,(\varphi_1, \varphi_1) = \min_{x,y \in L} \mathrm{ord}\,(x, y)\,.$$

Here we use the equality (4).

Choose $\varphi_2, \ldots, \varphi_n \in L$ such that $\boldsymbol{\varphi} = \{\varphi_1, \varphi_2 \ldots, \varphi_n\}$ is a basis of L. As before we write $Q(\sum_i x_i \varphi_i) = \sum_{1 \leq i \leq j \leq n} b_{ij}(\boldsymbol{\varphi}) x_i x_j$. Then

$$Q(x) = b_{11} \left(x_1 + \frac{b_{12}}{2b_{11}} x_2 + \cdots \frac{b_{1n}}{2b_{11}} x_n \right)^2 + \tilde{Q}(x_2, \ldots, x_n),$$

for some integral quadratic form $\tilde{Q}$ in $n - 1$ variables.

We define a new basis by $\psi_1 = \varphi_1$, and $\psi_i = \varphi_i - (b_{1i}/2b_{11})\varphi_1$ for $i \neq 1$. The choice of ψ_1 ensures that $\psi_i \in L$, since $e = \mathrm{ord}(2b_{11}) \leq \mathrm{ord}(b_{1i})$. With respect to this new basis, the quadratic form is

$$Q(x) = b_{11}(\boldsymbol{\psi})x_1^2 + \tilde{Q}(\sum_{i\geq 2} x_i\psi_i).$$

The proposition follows by induction. $\square$

Remark 2.3 Cassels ([1, Chapter 8, Theorem 3.1]) proves a stronger statement than Proposition 2.2. Namely, he gives a list of pairwise nonisomorphic quadratic forms such that every integral quadratic form is isomorphic to one of these. This stronger statement implies that the definition of the invariants a_i of Proposition 2.6 does not depend of the choice of the orthogonal basis.

We can give a simpler definition of the invariants a_i in terms of a basis $\boldsymbol{\psi}$ as in Proposition 2.2. If $\gamma \in L$ is an element such that $Q(\gamma) \neq 0$, we may define a reflection τ_γ by

$$\tau_\gamma(x) = x - \frac{2\,(x,\gamma)}{(\gamma,\gamma)}\gamma.$$

This is the reflection in the orthogonal complement of γ. Clearly, τ_γ is defined over $\mathbb{Z}_\ell$ if and only if $\mathrm{ord}\,(\gamma,\gamma) = \min_{x\in L} \mathrm{ord}\,(x,x)$. (In fact, this also holds for $\ell = 2$.) Since τ_γ is a reflection, it is clearly invertible. The following lemma is a partial analog of Witt's Lemma ([1, Corollary to Theorem 2.4.1]) which holds for quadratic forms over fields.

Lemma 2.4 *Suppose that $\psi, \varphi \in L$ satisfy*

$$Q(\psi) = Q(\varphi), \qquad \mathrm{ord}(Q(\psi)) = \mathrm{ord}(Q(\varphi)) = \min_{x\in L} \mathrm{ord}(Q(x)).$$

Then there exists an integral isometry σ of (L, Q) such that $\sigma(\psi) = \varphi$. Moreover, σ may be taken as a product of reflections τ_γ.

Proof: This is [1, Lemma 8.3.3]. Our assumptions on ψ and φ imply that $Q(\psi+\varphi)+Q(\psi-\varphi) = 2Q(\psi) + 2Q(\varphi) = 4Q(\psi)$. Since $\mathrm{ord}(Q(\psi)) = \mathrm{ord}\,(\psi,\psi) = \min_{x\in L} \mathrm{ord}\,(x,x) =: e$, it follows that one of the following holds:

(a) $\mathrm{ord}Q(\psi + \varphi) = e$,

(b) $\mathrm{ord}Q(\psi - \varphi) = e$.

Since $\ell \neq 2$, it is also possible that both hold. If (a) holds, then $\tau_{\psi+\varphi}$ is integral and sends ψ to φ. If (b) holds, define $\sigma = \tau_{\psi-\varphi} \circ \tau_\psi$. $\square$

Lemma 2.5 *Suppose $u, v \in \mathbb{Z}_\ell^\times$. Then $ux_1^2 + vx_2^2 \sim_{\mathbb{Z}_\ell} x_1^2 + uvx_2^2$.*

Proof: This is proved in the second corollary to [1, Lemma 8.3.3]. We give the idea. Since $\ell \neq 2$, there exists $a, c \in \mathbb{Z}_\ell$ such that $a^2u + c^2v = 1$. We may assume that a is a unit. Then

$$C = \begin{pmatrix} a & -cv \\ c & au \end{pmatrix}$$

defines the equivalence of the lemma. $\square$

Proposition 2.6 *(a) Let $\boldsymbol{\psi} = (\psi_1, \psi_2, \dots, \psi_n)$ be an orthogonal basis of L as in Proposition 2.2. Write $Q(x) = \sum_i b_i x_i^2$. Then the invariants a_i (Definition 1.2) satisfy*

$$a_i = \mathrm{ord}(b_i).$$

In particular, $\boldsymbol{\psi}$ is optimal.

(b) Suppose that n is odd. Then

$$\mathrm{ord}(\Delta) = a_1 + \cdots + a_n.$$

Proof: Let $\boldsymbol{\varphi}$ be a basis such that the inequalities (2) hold. We claim that $\mathrm{ord}\,(\varphi_1, \varphi_1) = a_1$. Part (b) of Lemma 1.3 implies that $a_1 = \min_{x\in L} \mathrm{ord}\,(x,x)$. The choice of $\boldsymbol{\varphi}$ implies moreover that $\mathrm{ord}\,(\varphi_1,\varphi_1) = \min_{x\in L}\mathrm{ord}\,(x,x)$. The definition of a_1 implies therefore that $a_1 = (\varphi_1, \varphi_1)$.

We apply the diagonalization process of the proof of Proposition 2.2 to the basis $\boldsymbol{\varphi}$. Define $\psi_1 = \varphi_1$ and $\psi_i = \varphi_i - (b_{1i}/2b_{11})\varphi_1$ for $i \neq 1$. One computes that

$$(\psi_j, \psi_1) = 0, \qquad (\psi_j, \psi_j) = \frac{b_{1j}^2}{2b_{11}} + 2b_{jj}, \qquad (\psi_i, \psi_j) = -\frac{b_{1i}b_{1j}}{2b_{11}} + b_{ij},$$

for $j \neq 1$ and $i \neq 1, j$. The inequalities (2) imply that $\mathrm{ord}\,(\psi_j, \psi_j) \geq a_j$ and $2\mathrm{ord}\,(\psi_i, \psi_j) \geq a_i + a_j$. Therefore the new basis also satisfies the inequalities (2). This implies that there exists an orthogonal basis $\boldsymbol{\psi}$ which satisfies (2). It follows that the Gross–Keating invariants $(a_1, \dots, a_n)$ are the maximum of $\cup S(\boldsymbol{\psi})$, where the union is taken over the orthogonal bases and $\cup S(\boldsymbol{\psi})$ is as in (1).

Let $\boldsymbol{\varphi}$ and $\boldsymbol{\psi}$ be two orthogonal bases. Write $Q(x) = b_1x_2^2 + b_2x_2^2 + \cdots + b_nx_n^2$ with respect to the basis $\boldsymbol{\psi}$ and $Q(x) = d_1x_1^2 + d_2x_2^2 + \cdots + d_nx_n^2$ with respect to the basis $\boldsymbol{\varphi}$. We suppose that $\mathrm{ord}(b_1) \leq \mathrm{ord}(b_2) \leq \cdots \leq \mathrm{ord}(b_n)$ and $\mathrm{ord}(d_1) \leq \mathrm{ord}(d_2) \leq \cdots \leq \mathrm{ord}(d_n)$. We suppose moreover that $\boldsymbol{\varphi}$ satisfies (2). (Such $\boldsymbol{\varphi}$ exists by the above argument.) We have to show that $\boldsymbol{\psi}$ satisfies (2), also. Write $C = (c_{ij})$ for the change of basis matrix expressing $\boldsymbol{\varphi}$ in terms $\boldsymbol{\psi}$. As before, Lemma 1.3.(b) implies that $\mathrm{ord}(b_1) = \mathrm{ord}(d_1) = a_1$. Write $b_1 = ud_1$, for some unit u.

Suppose that $\mathrm{ord}(b_2) > \mathrm{ord}(b_1)$. Then

$$d_1 = \sum_{j=1}^n c_{j1}^2 b_j \equiv c_{11}^2 b_1 \pmod{\ell^{a_1+1}}.$$

This implies that u is a quadratic residue. To prove the claim, we may therefore assume that $Q(\psi_1) = Q(\varphi_1)$ in this case.

Suppose that $\mathrm{ord}(b_1) = \mathrm{ord}(b_2)$. Then Lemma 2.5 implies that Q is $\mathbb{Z}_\ell$-equivalent to $d_1x_1^2 + ub_2x_2^2 + b_3x_3^2 + \cdots$. Hence also in this case we may assume that $Q(\psi_1) = Q(\varphi_1)$.

Lemma 2.4 implies that there exists an isometry σ of Q which sends ψ_1 to φ_1. Then $D := \sigma^{-1}C$ fixes ψ_1. Write

$$D = \begin{pmatrix} 1 & D_1 \\ 0 & D_2 \end{pmatrix}, \qquad B := \begin{pmatrix} 2b_1 & & 0 \\ & \ddots & \\ 0 & & 2b_n \end{pmatrix}$$

where D_2 is an $(n-1)\times(n-1)$ matrix. One computes that

$$D^tBD = \begin{pmatrix} 2\gamma^2 b_1 & 2\gamma D_1 \\ 2\gamma D_1^t & * \end{pmatrix}.$$

Our assumption implies that D^tBD is a diagonal matrix, with diagonal entries $2d_i$. This implies that $D_1 = (0, \dots, 0)$. We conclude that D restricts to an integral and invertible map from the sublattice of L spanned by $\psi_2, \dots, \psi_n$ to the sublattice spanned by $\varphi_2, \dots, \varphi_n$. This implies (a).

Part (b) follows immediately from (a). $\square$

Definition 2.7 Suppose that $n = 3$ and $\ell \neq 2$. Assume $a_1 \equiv a_2 \bmod 2$, and $a_3 > a_2$. Choose a basis $\boldsymbol{\psi} = (\psi_1, \psi_2, \psi_3)$ of L as in Proposition 2.2. Write $b_{ii} = \ell^{a_i}\epsilon_i$. We define an invariant $\varepsilon = \varepsilon(\boldsymbol{\psi})$ by the Legendre symbol

$$\varepsilon = \left(\frac{-\epsilon_1\epsilon_2}{\ell}\right). \tag{5}$$

Lemma 2.8 *Assumptions and notations are as in Definition 2.7.*

(a) The invariant $\varepsilon(\boldsymbol{\psi})$ does not depend on the choice of the orthogonal basis $\boldsymbol{\psi}$.

(b) We have that $\varepsilon = 1$ if and only if the subspace of $L \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ spanned by ψ_1 and ψ_2 is isotropic.

Proof: Let $\boldsymbol{\psi} = (\psi_1, \psi_2, \psi_3)$ be a basis of L as in Proposition 2.6, in particular $\boldsymbol{\psi}$ is orthogonal and the valuation of $b_i = (\psi_i, \psi_i)/2$ is equal to a_i, for $i = 1, 2, 3$.

Suppose that $a_2 \equiv a_1 \bmod 2$ and $a_3 > a_2$. Write $a_2 = a_1 + 2\gamma$. Write Q' for the restriction of Q to the sublattice of L spanned by ψ_1 and ψ_2. Then $Q'(x) = b_1x_1^2 + b_2x_2^2$ is equivalent to $\ell^{a_1}(x_1^2 + \epsilon_1\epsilon_2\ell^{2\gamma}x_2^2)$ (Lemma 2.5). It follows that Q' is isotropic if $\varepsilon = 1$ and anisotropic if $\varepsilon = -1$. This proves (b).

Let $\boldsymbol{\varphi}$ be another orthogonal basis and write $Q(\sum_i x_i\varphi_i) = d_1x_1^2 + d_2x_2^2 + d_3x_3^2$. We assume that $\operatorname{ord}(d_i) = a_i$. Write C for the matrix expressing $\boldsymbol{\varphi}$ in terms of $\boldsymbol{\psi}$. The argument of the proof of Proposition 2.6 together with the assumption that $a_2 < a_3$ implies that there exists an isometry σ such that

$$\sigma^{-1}C = \begin{pmatrix} u_1 & 0 & 0 \\ 0 & u_2 & 0 \\ 0 & 0 & u_3 \end{pmatrix},$$

where the u_i are units. This shows that $d_i = u_i^2 b_i$. The lemma follows. □

3 A normal form for quadratic forms over $\mathbb{Z}_2$

Not every quadratic form over $\mathbb{Z}_2$ is diagonalizable. In this section we give a normal form for ternary quadratic forms over $\mathbb{Z}_2$, following [1, Section 8.4]. Cassels uses a slightly stronger notion of integrality, namely he supposes that $b_{ij}/2 \in \mathbb{Z}_\ell$, for all $i \neq j$. However, this does not make any difference.

Lemma 3.1 *Suppose $\ell = 2$. Let Q be a regular quadratic form over $\mathbb{Z}_2$. Then Q is $\mathbb{Z}_2$-equivalent to a sum of quadratic forms of the form*

$$2^e ux^2, \tag{6}$$

for $e \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}_2^\times$, and

$$2^e(b_1x_1^2 + ux_1x_2 + b_2x_2^2), \tag{7}$$

with $e \in \mathbb{Z}_{\geq 0}$, and $u \in \mathbb{Z}_2^\times$.

The equality (3) holds for $\ell = 2$, but (4) does not. However, (3) implies that

$$\min_{x,y\in L} \operatorname{ord}(x, y) + 1 \geq \min_{x\in L} \operatorname{ord}(x, x).$$

Therefore $\min_{x,y\in L} \operatorname{ord}(x, y)$ equals either $\min_{x\in L} \operatorname{ord}(x, x)$ or $\min_{x\in L} \operatorname{ord}(x, x) - 1$.

Proof: Let $e = \min_{x,y\in L} \operatorname{ord}(x, y)$. We distinguish two cases.

(a) There exists a $\gamma \in L$ such that $\operatorname{ord}(\gamma, \gamma) = e$.

(b) For all $\gamma \in L$ we have that $\mathrm{ord}\,(\gamma,\gamma) > e$.

Suppose we are in case (a). Then $\mathrm{ord}\,(\psi_1,\psi_i) \geq e$, by definition. We can now proceed as in the proof of Proposition 2.2. Namely, $2b_{11} = 2Q(\psi_1) = (\psi_1,\psi_1)$. Therefore b_{11} has valuation $e-1$. For $i \neq 1$, we have that $\mathrm{ord}(b_{1i}) = \mathrm{ord}\,(\psi_1,\psi_i) \geq e$. Therefore

$$\varphi_i = \psi_i - \left(\frac{b_{1i}}{2b_{11}}\right)\psi_1.$$

is an element of L and $\psi_1,\varphi_2,\ldots,\varphi_n$ form a basis. With respect to this basis the quadratic form Q becomes $Q(x) = b_{11}x_1^2 + \tilde{Q}(x_2,\ldots,x_n)$, for some quadratic form $\tilde{Q}$ in $n-1$ variables.

Suppose we are in case (b). Then $\mathrm{ord}\,(\gamma,\gamma) > e$ for all $\gamma \in L$. We may choose $\psi_1,\psi_2 \in L$ such that $\mathrm{ord}\,(\psi_1,\psi_2) = e$. The definition of e implies that $(\psi_1+\psi_2)/2 \notin L$. Lemma 2.1 implies therefore that ψ_1,ψ_2 can be extended to a basis $\psi_1,\ldots,\psi_n$ of L.

The choice of ψ_1 and ψ_2 implies that the determinant of the matrix

$$\begin{pmatrix} 2b_{11}2^{-e} & b_{12}2^{-e} \\ b_{12}2^{-e} & 2b_{22}2^{-e} \end{pmatrix}$$

is a unit in $\mathbb{Z}_\ell$. Therefore we can find λ_1^j,λ_2^j such that

$$-2\lambda_1^j b_{11} - \lambda_2^j b_{12} + b_{1j} = 0, \qquad -2\lambda_2^j b_{22} - \lambda_1^j b_{12} + b_{2j} = 0,$$

for $j = 3,\ldots,n$. Define $\varphi_j = \psi_j - \lambda_1^j\psi_1 - \lambda_2^j\psi_2$. The choice of the λ_i^j implies that $(\varphi_j,\psi_1) = (\varphi_j,\psi_2) = 0$, for $j = 3,\ldots,n$.

With respect to the basis $(\psi_1,\psi_2,\varphi_3,\ldots,\varphi_n)$ the quadratic form Q becomes

$$Q(x) = 2^e(b_{11}x_1^2 + b_{12}x_1x_2 + b_{22}x_2^2) + \tilde{Q}(x_3,\ldots,x_n).$$

This proves the lemma. □

Lemma 3.2 *Let $Q_2(x) = b_{11}x_1^2 + b_{12}x_1x_2 + b_{22}x_2^2$ be a binary quadratic form over $\mathbb{Z}_2$ and L_2 the corresponding free $\mathbb{Z}_2$-lattice of rank two.*

(a) If $\min(\mathrm{ord}(b_{11}),\mathrm{ord}(b_{22})) < \mathrm{ord}(b_{12})$ then Q_2 is diagonalizable.

(b) Suppose that Q_2 is not diagonalizable. Then Q_2 is anisotropic if and only if $\mathrm{ord}(b_{12}) = \mathrm{ord}(b_{11}) = \mathrm{ord}(b_{22})$.

(c) Suppose Q_2 is anisotropic and not diagonalizable. Then Q_2 is equivalent to

$$2^e(x_1^2 + x_1x_2 + x_2^2),$$

for some e.

(d) Suppose that Q_2 is isotropic and not diagonalizable. Then Q_2 is equivalent to

$$2^e x_1x_2,$$

for some e.

Proof: Part (a) follows from the proof of Lemma 3.1.

Suppose that Q_2 is not diagonalizable. Then $\mathrm{ord}(b_{12}) \leq \min(\mathrm{ord}(b_{11}),\mathrm{ord}(b_{22}))$, by (a). Part (b) is an elementary Hilbert-symbol computation using [3, Theorem IV.6].

Suppose that Q_2 is anisotropic and not diagonalizable. Then (b) implies that $e := \mathrm{ord}(b_{12}) = \mathrm{ord}(b_{11}) = \mathrm{ord}(b_{22})$. Part (c) now follows from an elementary computation.

Suppose that Q_2 is isotropic and not diagonalizable. There exists a primitive vector ψ_1 such that $Q(\psi_1) = 0$. Lemma 2.1 together with the fact that the quadratic form is nondegenerate, implies that there exists a vector $\psi_2 \in L_2$ such that ψ_1, ψ_2 form a basis of L_2 and $(\psi_1, \psi_2) \neq 0$. After multiplying ψ_2 with a unit, we may suppose that $(\psi_1, \psi_2) = 2^e$, for some $e \geq 0$.

We claim that $\mathrm{ord}\,(\psi_2, \psi_2) > \mathrm{ord}\,(\psi_1, \psi_2)$. Namely, if $\mathrm{ord}\,(\psi_2, \psi_2) \leq \mathrm{ord}\,(\psi_1, \psi_2)$ then Q_2 is diagonalizable by (a), but this contradicts our assumptions. Therefore

$$\psi_2' := \psi_2 - \frac{(\psi_2, \psi_2)}{2\,(\psi_1, \psi_2)}\psi_1 \in L_2.$$

Now ψ_1, ψ_2' form a basis of L and $(\psi_2', \psi_2') = 0$. This proves (d). □

Proposition 3.3 *Let (L, Q) be a ternary quadratic form over $\mathbb{Z}_2$. One of the following two possibilities occurs.*

(a) The form Q is diagonalizable; there exists a basis such that

$$Q(x) = b_1x_1^2 + b_2x_2^2 + b_3x_3^3, \qquad \textit{with} \qquad 0 \leq \mathrm{ord}(b_1) \leq \mathrm{ord}(b_2) \leq \mathrm{ord}(b_3).$$

(b) The form Q is not diagonalizable; there exists a basis such that

$$Q(x) = \epsilon_1 2^{\mu_1}x_1^2 + 2^{\mu_2}(ux_2^2 + x_2x_3 + ux_3^2), \qquad \textit{with} \qquad u \in \{0,1\}, \quad \mu_i \geq 0 \quad \textit{and} \quad \epsilon_1 \in \mathbb{Z}_2^\times.$$

Proof: This follows immediately from Lemma 3.1 and Lemma 3.2. □

This classification is the same as the classification used (but not explicitly stated) in [4, Appendix B]. Note that Yang's matrix T differs by a factor 2 from the matrix B we use. In particular, the invariant β used in [4, Proposition B.4] satisfies $\beta \geq -1$ rather than $\beta \geq 0$.

4 The Gross–Keating invariants for $\ell = 2$

In this section we compute the Gross–Keating invariants of ternary quadratic forms (L, Q) over $\mathbb{Z}_2$ in terms of the normal form of Proposition 3.3. The computation of the a_i can be found in Proposition 4.1 (non-diagonalizable case) and Proposition 4.2 (diagonalizable case). The computation of ε can be found in Proposition 4.9. This section is based on [4, Appendix B].

We start by considering quadratic forms which are not diagonalizable. Recall from Proposition 3.3 that if Q is not diagonalizable then there exists a basis $\boldsymbol{\psi}$ of L with respect to which we have

$$Q(x) = \epsilon_1 2^{\mu_1}x_1^2 + 2^{\mu_2}(ux_2^2 + x_2x_3 + ux_3^2), \qquad \text{with} \qquad u \in \{0,1\}, \quad \epsilon_1 \in \mathbb{Z}_2^\times. \tag{8}$$

We do not suppose that $\mu_1 \leq \mu_2$.

Proposition 4.1 *Suppose that Q is given by (8). Then*

$$(a_1, a_2, a_3) = \begin{cases} (\mu_1, \mu_2, \mu_2), & \textit{if } \mu_1 \leq \mu_2, \\ (\mu_2, \mu_2, \mu_1), & \textit{if } \mu_1 > \mu_2. \end{cases}$$

Proof: Lemma 1.3.(b) implies that $a_1 = \min(\mu_1, \mu_2)$. We distinguish two cases.

Suppose that $\mu_1 \leq \mu_2$. Then $a_1 = \mu_1$ and $\mathrm{ord}(\Delta) = \mu_1 + 2\mu_2 \geq a_1 + a_2 + a_3$ (Lemma 1.3.(a)). Therefore $a_2 \leq (a_2 + a_3)/2 \leq \mu_2$. The existence of a basis $\boldsymbol{\psi}$ as in (8) implies that $(\mu_1, \mu_2, \mu_2) \in S(\boldsymbol{\psi})$. We conclude that $a_2 = a_3 = \mu_2$.

Suppose that $\mu_1 > \mu_2$. In this case we have that $a_1 = \mu_2$. Recall that we defined ρ as the minimum of the valuation of the determinant of the 2×2-minors of B. One computes that

$\rho = \min(2\mu_2, 1+\mu_1+\mu_2) = 2\mu_2$, since we assumed that $\mu_1 \geq \mu_2+1$. Lemma 1.3.(c) implies that $\rho \geq a_1+a_2$, hence $a_2 \leq \mu_2$. The existence of a basis $\boldsymbol{\psi}$ as in (8) implies that $(\mu_2,\mu_2,\mu_1)\in S(\boldsymbol{\psi})$. We conclude that $(a_1,a_2,a_3) = (\mu_2,\mu_2,\mu_1)$. $\square$

We now consider diagonalizable quadratic forms Q. Contrary to the situation for $\ell \neq 2$, a basis $\boldsymbol{\psi}$ which diagonalizes Q is not optimal (Definition 1.2).

Proposition 4.2 *Suppose that Q is diagonalizable. Let $\boldsymbol{\psi}$ be a basis of L such that*

$$Q(x) = b_1x_1^2 + b_2x_2^2 + b_3x_3^2, \qquad \text{with } b_i = \epsilon_i 2^{\mu_i}, \quad \epsilon_i \in \mathbb{Z}_2^\times \quad \text{and} \quad \mu_1 \leq \mu_2 \leq \mu_3. \tag{9}$$

(a) Suppose that $\mu_1 \not\equiv \mu_2 \bmod 2$. Then $(a_1,a_2,a_3) = (\mu_1,\mu_2,\mu_3+2)$.

(b) Suppose that $\mu_1 \equiv \mu_2 \bmod 2$.

- *(i) If $\epsilon_1+\epsilon_2 \equiv 2 \bmod 4$ or $\mu_3 \leq \mu_2+1$, then $(a_1,a_2,a_3) = (\mu_1,\mu_2+1,\mu_3+1)$.*
- *(ii) Otherwise, $(a_1,a_2,a_3) = (\mu_1,\mu_2+2,\mu_3)$.*

The proof of this proposition is divided in several lemmas. We use the notation of Proposition 4.2. In particular, $\boldsymbol{\psi}$ is a basis of L with respect to which Q is as in (9). Let $\boldsymbol{\varphi}$ be an optimal basis, i.e. suppose that the inequalities (2) hold. We write $C = (c_{ij})$ for the change of basis matrix expressing $\boldsymbol{\varphi}$ in terms of $\boldsymbol{\psi}$. We write the quadratic form Q in terms of the basis $\boldsymbol{\varphi}$ as $Q(x) = \sum_{i\leq j} d_{ij}x_ix_j$. In other words, the d_{ij} are the coefficients of the matrix obtained by dividing the diagonal elements of C^tBC by two. One computes that

$$d_{ii} = c_{1i}^2b_1 + c_{2i}^2b_2 + c_{3i}^2b_3. \tag{10}$$

Lemma 4.3 *Suppose that Q is diagonal and $\mu_1 \not\equiv \mu_2 \bmod 2$. Then $(a_1,a_2,a_3) = (\mu_1,\mu_2,\mu_3+2)$.*

Proof: We have already seen that $a_1 = \mu_1$. Therefore it follows from the definition of the a_i that $a_2 \geq \mu_2$. We claim that $a_2 = \mu_2$. Suppose that $a_2 > \mu_2$.

Write $\mu_2 = \mu_1+2\gamma+1$. The inequalities (2) imply that $\mathrm{ord}(d_{22}) \geq a_2 \geq \mu_2+1$ and $\mathrm{ord}(d_{33}) \geq a_3 \geq a_2 \geq \mu_2+1$. Since $\mu_1 \not\equiv \mu_2 \bmod 2$, it follows from (10) that $\mathrm{ord}(c_{12}) \geq \gamma+1$ and $\mathrm{ord}(c_{13}) \geq \gamma+1$.

We first suppose that $\mu_3 > \mu_2$. Then $\mathrm{ord}(c_{22}) \geq 1$ and $\mathrm{ord}(c_{33}) \geq 1$. But this implies that $\det(C) \equiv 0 \bmod 2$. This gives a contradiction.

If $\mu_2 = \mu_3$, we proceed similarly. In this case $c_{22} \equiv c_{32} \bmod 2$ and $c_{23} \equiv c_{33} \bmod 2$. This implies again that $\det(C) \equiv 0 \bmod 2$. We conclude that $a_2 = \mu_2$.

Since $\mathrm{ord}(\Delta) = \mathrm{ord}(\det(B)) + 2 = \mu_1+\mu_2+\mu_3+2$, it follows from Lemma 1.3.(a) that $a_3 \leq \mu_3+2$. To show that $a_3 = \mu_3+2$ it suffices to find a basis $\boldsymbol{\varphi}$ such that $(\mu_1,\mu_2,\mu_3+2)\in S(\boldsymbol{\varphi})$. We now construct such a basis.

Our assumptions imply that μ_3 is congruent to μ_1 or μ_2 (modulo 2). We suppose that $\mu_3 \equiv \mu_1 \bmod 2$. (The case $\mu_3 \equiv \mu_2 \bmod 2$ is similar.) Write $\mu_2 = \mu_1+2\gamma+1$ and $\mu_3 = \mu_1+2\lambda$. We distinguish two cases:

- $\epsilon_1+\epsilon_3 \equiv 0 \bmod 4$,
- $\epsilon_1+\epsilon_3 \equiv 2 \bmod 4$.

In the first case define

$$C = \begin{pmatrix} 1 & 0 & 2^\lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + b_2x_2^2 + 2^{\lambda+1}b_1x_1x_3 + (b_3+2^{2\lambda}b_1)x_3^2$.

In the second case we define

$$C = \begin{pmatrix} 1 & 0 & 2^{\lambda} \\ 0 & 1 & 2^{\lambda-\gamma} \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2+b_2x_2^2+2^{\lambda+1}b_1x_1x_3+(b_3+2^{2\lambda}b_1+2^{2(\lambda-\gamma)}b_2)x_3^2+2^{\lambda-\gamma+1}b_2x_2x_3$. It is easy to check that the basis $\boldsymbol{\varphi}$ corresponding to C satisfies (2) for $a_1 = \mu_1$, $a_2 = \mu_2$ and $a_3 = \mu_3 + 2$. This proves the lemma. □

The proof of Lemmas 4.4, 4.5 and 4.6 follows the same pattern as the proof of Lemma 4.3.

Lemma 4.4 *Suppose that Q is diagonalizable, $\mu_1 \equiv \mu_2 \bmod 2$ and $\mu_3 \leq \mu_2+1$. Then $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$.*

Proof: Since $a_1 = \mu_1$ and $\mathrm{ord}(\Delta) = \mu_1 + \mu_2 + \mu_3 + 2$ it follows from Lemma 1.3 that $a_1 + 2a_2 \leq a_1 + a_2 + a_3 \leq \mu_1 + \mu_2 + \mu_3 + 2 \leq \mu_1 + 2\mu_2 + 3$. This implies that $a_2 \leq \mu_2 + 1$.

We now construct a basis $\boldsymbol{\varphi}$ such that $(\mu_1, \mu_2 + 1, \mu_3 + 1) \in S(\boldsymbol{\varphi})$. The lemma follows from this. Let C be the corresponding change of basis matrix. Write $\mu_2 = \mu_1 + 2\gamma$.

If $\mu_2 = \mu_3$ define

$$C = \begin{pmatrix} 1 & 2^{\gamma} & 2^{\gamma} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2)x_2^2 + 2^{\gamma+1}b_1(x_1x_2 + x_1x_3) + (b_3 + 2^{2\gamma}b_1)x_3^2 + 2^{1+2\gamma}b_1x_2x_3$.

If $\mu_3 = \mu_2 + 1$ and $\epsilon_1 + \epsilon_2 \equiv 2 \bmod 4$ define

$$C = \begin{pmatrix} 1 & 2^{\gamma} & 2^{\gamma} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (b_2 + 2^{2\gamma}b_1)x_2^2 + 2^{\gamma+1}b_1(x_1x_2 + x_1x_3) + (b_3 + 2^{2\gamma}b_1 + b_2)x_3^2 + (2^{2\gamma+1}b_1 + 2b_2)x_2x_3$.

If $\mu_3 = \mu_2 + 1$ and $\epsilon_1 + \epsilon_2 \equiv 0 \bmod 4$ define

$$C = \begin{pmatrix} 1 & 2^{\gamma} & 2^{\gamma} \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2 + b_3)x_2^2 + 2^{\gamma+1}b_1(x_1x_2 + x_1x_3) + (4b_3 + 2^{2\gamma}b_1 + b_2)x_3^2 + (2^{2\gamma+1}b_1 + 2b_2 + 4b_3)x_2x_3$.

In each of these cases one checks that $(\mu_1, \mu_2 + 1, \mu_3 + 1) \in S(\boldsymbol{\varphi})$. □

Lemma 4.5 *Suppose that Q is diagonal, $\mu_1 \equiv \mu_2 \bmod 2$ and $\epsilon_1+\epsilon_2 \equiv 2 \bmod 4$. Then $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$.*

Proof: By Lemma 4.4 we may assume that $\mu_3 \geq \mu_2 + 2$. We claim that $a_2 \leq \mu_2 + 1$. Suppose that $a_2 \geq \mu_2 + 2$. As before, we suppose that $\boldsymbol{\varphi}$ is an optimal basis. As before, we write $C = (c_{ij})$ for the change of basis matrix and $D = C^tBC = (d_{ij})$ for the matrix corresponding to the new basis. Write $\mu_2 = \mu_1 + 2\gamma$.

The assumption $a_2 \geq \mu_2+2$ implies that $\mathrm{ord}(d_{22}) \geq a_2 \geq \mu_2+2$ and $\mathrm{ord}(d_{33}) \geq a_3 \geq a_2 \geq \mu_2+2$. It follows from (10) that $\mathrm{ord}(c_{12}) \geq \gamma$ and $\mathrm{ord}(c_{13}) \geq \gamma$. Suppose that $\mathrm{ord}(c_{12}) = \gamma$. Then $\mathrm{ord}(c_{22}) = 1$ and $d_{22} \equiv 2^{\mu_2}(\epsilon_1+\epsilon_2) \not\equiv 0 \bmod 2^{\mu_2+2}$. This gives a contradiction. Similarly, we obtain a contradiction if $\mathrm{ord}(c_{13}) = \gamma$. Therefore $\mathrm{ord}(c_{1j}) > \gamma$ for $j = 2, 3$ and $d_{22} \equiv c_{22}^2b_2 \bmod 2^{\mu_2+2}$.

Since $\mathrm{ord}(d_{22}) \geq \mu_2 + 2$ and $\mathrm{ord}(b_2) = \mu_2$, we conclude that $\mathrm{ord}(c_{22}) > 0$. Similarly, $d_{33} \equiv c_{23}^2 b_2 \bmod 2^{\mu_2+2}$; this implies that $\mathrm{ord}(c_{23}) > 0$. But then $\det(C) \equiv 0 \bmod 2$. This gives a contradiction. We conclude that $a_2 \leq \mu_2 + 1$.

To prove the lemma, we construct a basis $\boldsymbol{\varphi}$ such that $(\mu_1, \mu_2{+}1, \mu_3{+}1) \in S(\boldsymbol{\varphi})$. We distinguish two subcases:

- $\mu_3 \equiv \mu_1 \bmod 2$,
- $\mu_3 \not\equiv \mu_1 \bmod 2$.

Suppose that $\mu_3 \equiv \mu_1 \bmod 2$. Write $\mu_2 = \mu_1 + 2\gamma$ and $\mu_3 = \mu_1 + 2\lambda$. Let $\boldsymbol{\varphi}$ be the basis of L corresponding to the change of basis matrix

$$C = \begin{pmatrix} 1 & 2^\gamma & 2^\lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2)x_2^2 + 2^{\gamma+1}b_1x_1x_2 + 2^{\lambda+1}b_1x_1x_3 + (b_3 + 2^{2\lambda}b_1)x_3^2 + 2^{\gamma+\lambda+1}b_1x_2x_3$.

Suppose that $\mu_3 \not\equiv \mu_1 \bmod 2$. Write $\mu_2 = \mu_1 + 2\gamma$ and $\mu_3 = \mu_1 + 2\lambda + 1$. Let $\boldsymbol{\varphi}$ be the basis of L corresponding to the change of basis matrix

$$C = \begin{pmatrix} 1 & 2^\gamma & 2^\lambda \\ 0 & 1 & 2^{\lambda-\gamma} \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2)x_2^2 + 2^{\gamma+1}b_1x_1x_2 + 2^{\lambda+1}b_1x_1x_3 + (b_3 + 2^{2\lambda}b_1 + 2^{2(\lambda-\gamma)}b_2)x_3^2 + (2^{\gamma+\lambda+1}b_1 + 2^{\lambda-\gamma+1}b_2)x_2x_3$.

In each of these cases one checks that $(\mu_1, \mu_2 + 1, \mu_3 + 1) \in S(\boldsymbol{\varphi})$. □

Lemma 4.6 *Suppose that Q is diagonal, $\mu_1 \equiv \mu_2 \bmod 2$, $\mu_3 \geq \mu_2 + 2$ and $\epsilon_1 + \epsilon_2 \equiv 0 \bmod 4$. Then $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 2, \mu_3)$.*

Proof: Write $\mu_2 = \mu_1 + 2\gamma$. We already know that $a_1 = \mu_1$. We claim that $a_2 \leq \mu_2 + 2$. Suppose $a_2 \geq \mu_2 + 3$. The same reasoning as in the beginning of the proof of Lemma 4.4 shows that we may assume that $\mu_3 \geq \mu_2 + 4$. If $c_{22} \equiv c_{23} \equiv 0 \bmod 2$, we conclude as in the proof of Lemma 4.5 that $\det(C) \equiv 0 \bmod 2$. This gives a contradiction, hence either c_{22} or c_{23} is a unit.

Suppose that c_{22} is a unit. (The argument in the case that c_{23} is a unit is similar, and we omit it.) Then $\mathrm{ord}(c_{12}) = \gamma$. One computes that

$$d_{12} \equiv 2c_{12}c_{11}b_1 + 2c_{21}c_{22}b_2 \bmod 2^{\mu_2+3}. \tag{11}$$

It follows from (2) that $2\mathrm{ord}(d_{12}) \geq a_1 + a_2 \geq \mu_1 + \mu_2 + 3 = 2\mu_1 + 2\gamma + 3$. Hence

$$\mathrm{ord}(d_{12}) \geq \mu_1 + \gamma + 2. \tag{12}$$

Recall that Lemma 1.3.(b) implies that $\mathrm{ord}(d_{11}) = a_1$.

First suppose that $\mu_1 < \mu_2$, that is $\gamma \neq 0$. Since d_{11} has valuation a_1, c_{11} is a unit. It follows from (11) that $\mathrm{ord}(d_{12}) = \mu_1 + \gamma + 1$. This contradicts (12).

Now suppose that $\mu_1 = \mu_2$. Since $d_{11} \equiv c_{12}^2 b_1 + c_{21}^2 b_2 \bmod 2^{\mu_1+1}$. Since d_{11} has valuation $a_1 = \mu_1$, it follows that either

(i) $c_{12} \equiv 1 \bmod 2$ and $c_{21} \equiv 0 \bmod 2$, or

(ii) $c_{12} \equiv 0 \bmod 2$ and $c_{21} \equiv 1 \bmod 2$.

Since $\mathrm{ord}(d_{12}) \geq \mu_1 + 2$, it follows from (11) that (i) holds and that $c_{11} \equiv 0 \bmod 2$. One computes that

$$d_{23} \equiv 2c_{12}c_{13}b_1 + 2c_{22}c_{23}b_2 \equiv 2c_{13}b_1 + 2c_{23}b_2 \pmod{2^{\mu_1+2}},$$

since c_{12} and c_{22} are units. It follows that $c_{13} \equiv c_{23} \bmod 2$. But this implies that $\det(C) \equiv 0 \bmod 2$. (In case $\epsilon_1 + \epsilon_2 \equiv 4 \bmod 8$ one could alternatively argue as in the proof of Lemma 4.5.)

Let $\boldsymbol{\varphi}$ be the basis of L corresponding to the change of basis matrix

$$C = \begin{pmatrix} 1 & 2^\gamma & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $b_{22}(\boldsymbol{\varphi}) \equiv 0 \bmod 2^{\mu_2+2}$. With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2)x_2^2 + 2^{\gamma+1}b_1x_1x_2 + b_3x_3^2$. Therefore $(\mu_1, \mu_2 + 1, \mu_3) \in S(\boldsymbol{\varphi})$. This proves the lemma. $\square$

The following proposition is an immediate consequence of the computation of the invariants a_i. It illustrates that the a_i satisfy similar properties for $\ell = 2$ and $\ell \neq 2$, which is not so clear from the definition.

Proposition 4.7 *Let Q be a ternary quadratic form over $\mathbb{Z}_\ell$ for $\ell \geq 2$. Then*

$$\mathrm{ord}(\Delta) = a_1 + a_2 + a_3.$$

Proof: For $\ell \neq 2$ this is Proposition 2.6.(b). For $\ell = 2$ the theorem follows from the Propositions 4.1 and 4.2. $\square$

In the rest of this section we define the Gross–Keating invariant ε for $\ell = 2$ and show that it is well defined (compare to Lemma 2.8).

Definition 4.8 Suppose that $a_1 \equiv a_2 \bmod 2$ and $a_3 > a_2$. Let $\boldsymbol{\varphi}$ be an optimal basis. We define $\varepsilon = \varepsilon(\boldsymbol{\varphi})$ by $\varepsilon = 1$ if the subspace of $L \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ spanned by φ_1 and φ_2 is isotropic, and $\varepsilon = -1$, otherwise.

Proposition 4.9 *Suppose that $a_1 \equiv a_2 \bmod 2$ and $a_3 > a_2$.*

(a) The invariant ε does not depend on the choice of the basis.

(b) (i) If Q is not diagonalizable we may write $Q(x) = \epsilon_1 2^{\mu_1}x_1^2 + 2^{\mu_2}(ux_2^2 + x_2x_3 + ux_3^2)$ with $u \in \{0, 1\}$ and $\mu_1 > \mu_2$. In this case

$$\varepsilon = (-1)^u.$$

(ii) If Q is diagonalizable we may write $Q(x) = \epsilon_1 2^{\mu_1}x_1^2 + \epsilon_2 2^{\mu_2}x_2^2 + \epsilon_3 2^{\mu_3}x_3^2$ with $\epsilon_1 + \epsilon_2 \equiv 0 \bmod 4$, $\mu_1 \equiv \mu_2 \bmod 2$ and $\mu_3 \geq \mu_2 + 2$. We have that

$$\varepsilon = (-1)^{(\epsilon_1+\epsilon_2)/4}.$$

Proof: The fact that one of the two cases of (b) holds follows immediately from Propositions 4.1 and 4.2.

Suppose that Q is not diagonalizable. Write $Q(x) = \epsilon_1 2^{\mu_1}x_1^2 + 2^{\mu_2}(ux_2^2 + x_2x_3 + ux_3^2)$, as in the statement of the proposition, and let $\boldsymbol{\psi}$ be the corresponding basis. Write Q_2 for the restriction of Q to the sublattice spanned by the basis vectors ψ_2, ψ_3. Lemma 3.2 implies that Q_2 is isotropic if and only $u = 0$. This implies that $\varepsilon(\boldsymbol{\psi}) = (-1)^u$.

We now show that ε is well defined in this case. It suffices to show that $\varepsilon(\boldsymbol{\varphi}) = \varepsilon(\boldsymbol{\psi})$ for optimal bases $\boldsymbol{\varphi}$ and $\boldsymbol{\psi}$ with respect to which Q is in a normal form as in Proposition 3.3. By assumption, Q is not diagonalizable. (In fact, it follows from Proposition 4.2 that no quadratic form $Q(x) = \epsilon_1 2^{\mu_1} x_1^2 + 2^{\mu_2}(ux_2^2 + x_2x_3 + ux_3^2)$ with $u \in \{0, 1\}$ and $\mu_1 > \mu_2$ is diagonalizable. Hence we could have dropped this assumption from the statement of the proposition.) Write $Q'(x) = \epsilon_1' 2^{\mu_1} x_1^2 + 2^{\mu_2}(u'x_2^2 + x_2x_3 + u'x_3^2)$ for Q expressed with respect to the basis $\boldsymbol{\varphi}$. Since $\Delta(Q) = \Delta(Q')$ we have that $\epsilon_1(4u^2 - 1) = \epsilon_1'(4(u')^2 - 1)$, therefore $u = u'$ implies that $\epsilon_1 = \epsilon_1'$. Hence, to show that $\varepsilon(\boldsymbol{\varphi}) = \varepsilon(\boldsymbol{\psi})$, it suffices to show that $u = u'$. We assume that $u = 1$ and $u' = 0$, and derive a contradiction.

The basis vector φ_2 is isotropic. Write $\varphi_2 = c_1\psi_1 + c_2\psi_2 + c_3\psi_3$. The fact that $Q(\varphi_2) = 0$ implies that $\mu_1 \equiv \mu_2 \bmod 2$. Moreover, it follows that $\mathrm{ord}(c_j) \geq (\mu_1 - \mu_2)/2 > 0$ for $j = 2, 3$. Since φ_2 is primitive, it follows that $c_1 \equiv 1 \bmod 2$. An easy computation shows that $\mathrm{ord}\,(\varphi_2, \psi_i) > \mu_2$ for $i = 1, 2, 3$. In particular $\mathrm{ord}\,(\varphi_2, \varphi_3) > \mu_2$. But this contradicts the assumption that $\mathrm{ord}\,(\varphi_2, \varphi_3) = \mu_2$.

Next we assume that Q is diagonalizable, and let $Q(x)$ be as in the statement of (b.ii). Write $\boldsymbol{\psi}$ for the corresponding basis of L. Let Q_2 be the restriction of Q to the subspace spanned by ψ_1, ψ_2. Then Q_2 is isotropic if and only if $-\det(Q)$ is a square ([3, Theorem IV.6]). It is easy to see that this happens if and only if $\epsilon_1 + \epsilon_2 \equiv 0 \bmod 8$.

We now show that ε is independent of the choice of the optimal basis in this case. Let $\boldsymbol{\varphi}$ be an optimal basis. Let $C = (c_{ij})$ be the corresponding change of basis matrix expressing $\boldsymbol{\varphi}$ in terms of $\boldsymbol{\psi}$. Write $\mu_1 = \mu_2 + 2\gamma$.

We suppose that $\mu_2 > \mu_1$, that is $\gamma > 0$. (The case $\mu_1 = \mu_2$ is analogous and left to the reader.) We use the notation of the proof of Lemma 4.6. In particular, we write $Q(x) = \sum_{i \leq j} d_{ij} x_i x_j$ for the representation of Q in terms of the basis $\boldsymbol{\varphi}$.

We showed in the proof of Lemma 4.6 that either c_{22} or c_{23} is a unit. Suppose that $c_{22} \equiv 0 \bmod 2$ and $c_{23} \equiv 1 \bmod 2$. It follows that $\mathrm{ord}(d_{33}) \geq a_3 = \mu_3 \geq \mu_2 + 3$. Therefore (10) implies that $\mathrm{ord}(c_{13}) = \gamma$. We showed in the proof of Lemma 4.6 that c_{11} is a unit. Since $d_{13} \equiv 2c_{11}c_{13}b_1 + 2c_{21}c_{23}b_2 \bmod 2^{\mu_3+1}$, we conclude that $2\mathrm{ord}(d_{13}) = 2 + 2\gamma + 2\mu_1 = \mu_1 + \mu_2 + 2$. (Here we use that $\gamma > 0$.) But this contradicts $2\mathrm{ord}(d_{13}) \geq a_1 + a_3 = \mu_1 + \mu_3 \geq \mu_1 + \mu_2 + 3$. We conclude that c_{22} is a unit. Recall from the proof of Lemma 4.6 that this implies that $c_{12} \equiv 1 \bmod 2$ and $c_{21} \equiv 0 \bmod 2$. Therefore the determinant of the submatrix

$$\tilde{C} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

of C is a unit. We may define

$$D = \begin{pmatrix} \tilde{C}^{-1} & 0 \\ 0 & 1 \end{pmatrix}.$$

With respect to the basis corresponding to CD, the quadratic form Q becomes $Q(x) = (b_1 + \delta_1^2 b_3)x_1^2 + (b_2 + \delta_2^2 b_3)x_2^2 + 2\delta_1 b_3 x_1 x_2 + x_3(\text{other terms})$, for certain $\delta_1, \delta_2 \in \mathbb{Z}_2$. Since $\mathrm{ord}(b_3) \geq \mathrm{ord}(b_2) + 3$ this implies that the subspace spanned by φ_1 and φ_2 is isotropic if and only if the space spanned by ψ_1 and ψ_2 is isotropic. □

5 Anisotropic quadratic forms

The goal is to classify all anisotropic ternary quadratic forms over $\mathbb{Z}_2$, starting from the normal form of Proposition 3.3. We will see that for anisotropic forms we may choose an optimal basis $\boldsymbol{\varphi}$ so that $\mathrm{ord}(Q(\varphi_i)) = a_i$, similar to what we had for $\ell \neq 2$ (Corollary 5.8).

Proposition 5.1 *Let Q be a ternary quadratic form over $\mathbb{Q}_\ell$. Write $Q(x) = b_1x_1^2 + b_2x_2^2 + b_3x_3^2$. We denote by $\det(Q) = b_1b_2b_3$ the determinant of Q. Then Q is isotropic if and only if*

$$(-1, -\det(Q)) = \prod_{i<j} (b_i, b_j).$$

Here $(\cdot,\cdot)$ denotes the Hilbert symbol.

Proof: This is [3, Theorem IV.6.ii]. $\square$

Proposition 5.2 *Let Q be a ternary quadratic form over $\mathbb{Z}_2$ which is not diagonalizable. Let $\boldsymbol{\psi}$ be an optimal basis such that $Q(x) = \epsilon_1 2^{\mu_1} x_1^2 + 2^{\mu_2}(ux_2^2 + x_2x_3 + ux_3^2)$ with $u \in \{0,1\}$. Then Q is isotropic if and only if $u = 0$ or $\mu_1 \equiv \mu_2 \bmod 2$.*

Proof: If $u = 0$ then Q is obviously isotropic. Therefore suppose that $u = 1$. To decide whether Q is isotropic, we may consider Q as quadratic form over $\mathbb{Q}_2$. We have $Q(x) \sim_{\mathbb{Q}_2} \epsilon_1 2^{\mu_1} x_1^2 + 2^{\mu_2}(x_2^2 + 3x_3^2)$. The proposition follows from Proposition 5.1 by direct verification using the formula for the Hilbert symbol [3, Theorem III.1]. $\square$

Lemma 5.3 *Let Q be a ternary quadratic form over $\mathbb{Z}_\ell$. We do not assume that $\ell = 2$. Suppose that $a_1 \equiv a_2 \equiv a_3 \bmod 2$. Then Q is isotropic.*

Proof: If Q is not diagonalizable then the lemma follows from Proposition 5.2, since $(a_1, a_2, a_3) \in \{(\mu_1, \mu_2, \mu_2), (\mu_2, \mu_2, \mu_1)\}$.

Suppose that Q is diagonalizable. Write $Q(x) = \epsilon_1 \ell^{\mu_1} x_1^2 + \epsilon_2 \ell^{\mu_2} x_2^2 + \epsilon_3 \ell^{\mu_3} x_3^2$. If $\ell \neq 2$ we have that $\mu_i = a_i$ hence $\mu_1 \equiv \mu_2 \equiv \mu_3 \bmod 2$. To show that Q is isotropic, it suffices to consider Q over $\mathbb{Q}_\ell$. After multiplying the basis vectors by a suitable constant, we may assume that $\mu_1 = \mu_2 = \mu_3 = 0$. The lemma now follows immediately from Proposition 5.1, since the Hilbert symbol is trivial on units for $\ell \neq 2$.

Suppose that $\ell = 2$ and Q is diagonalizable. Proposition 4.2 implies that $\mu_1 \equiv \mu_2 \equiv \mu_3 \bmod 2$ and $\epsilon_1 + \epsilon_2 \equiv 0 \bmod 4$. As for $\ell \neq 2$, it is no restriction to suppose that $Q(x) = \epsilon_1 x_2^2 + \epsilon_2 x_2^2 + \epsilon_3 x_3^2$. One computes that this quadratic form is anisotropic if and only if $\epsilon_1 \equiv \epsilon_2 \equiv \epsilon_3 \bmod 4$. Hence in our case Q is isotropic. $\square$

For future reference we record from the proof of Lemma 5.3 when a diagonal ternary form over $\mathbb{Z}_2$ is anisotropic.

Lemma 5.4 *Let $Q(x) = \epsilon_1 2^{\mu_1} x_1^2 + \epsilon_2 2^{\mu_2} x_2^2 + \epsilon_3 2^{\mu_3} x_3^2$ be a diagonal, ternary quadratic form over $\mathbb{Z}_2$. Suppose that $\mu_1 \equiv \mu_2 \equiv \mu_3 \bmod 2$. Then Q is anisotropic if and only if $\epsilon_1 \equiv \epsilon_2 \equiv \epsilon_3 \bmod 4$.*

Lemma 5.5 *Let $Q(x) = \epsilon_1 2^{\mu_1} x_1^2 + \epsilon_2 2^{\mu_2} x_2^2 + \epsilon_3 2^{\mu_3} x_3^2$ be a diagonal, ternary quadratic form over $\mathbb{Z}_2$. Suppose that $\mu_1 \equiv \mu_2 \bmod 2$ and $\mu_3 \not\equiv \mu_1 \bmod 2$.*

(a) Suppose that $\epsilon_1 \equiv \epsilon_2 \equiv \epsilon_3 \bmod 4$. Then Q is anisotropic if and only if $\epsilon_2 \equiv \pm\epsilon_1 \bmod 8$.

(b) Suppose that the ϵ_i are not all equivalent modulo 4. Then Q is anisotropic if and only if $\epsilon_2 \equiv \pm 3\epsilon_1 \bmod 8$.

Proof: The proof is similar to the proof of Lemma 5.3 and is left to the reader. $\square$

Notation 5.6 Let Q be a ternary quadratic form with Gross–Keating invariants (a_1, a_2, a_3). For every $1 \leq i < j \leq 3$ we define

$$\delta_{ij} = \lceil \frac{a_i + a_j}{2} \rceil,$$

where $\lceil a \rceil$ is the smallest integer greater than or equal to a.

Theorem 5.7 *Let $Q(x) = \epsilon_1 2^{\mu_1} x_1^2 + \epsilon_2 2^{\mu_2} x_2^2 + \epsilon_3 2^{\mu_3} x_3^2$ be a diagonal anisotropic quadratic form over $\mathbb{Z}_2$ with $\mu_1 \leq \mu_2 \leq \mu_3$. Then one of the following cases occurs.*

(a) *Suppose* $\mu_1 \equiv \mu_3 \not\equiv \mu_2 \bmod 2$ *and* $\epsilon_1 \equiv 3\epsilon_3 \bmod 8$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2, \mu_3 + 2)$ *and* $a_1 \not\equiv a_2 \bmod 2$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}\epsilon_1 x_1^2 + 2^{a_2}\epsilon_2 x_2^2 + 2^{\delta_{13}}\epsilon_1 x_1 x_3 + 2^{a_3}\epsilon_1 x_3^2.$$

(b) *Suppose* $\mu_1 \equiv \mu_3 \not\equiv \mu_2 \bmod 2$ *and* $\epsilon_1 \equiv \epsilon_3 \bmod 4$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2, \mu_3 + 2)$ *and* $a_1 \not\equiv a_2 \bmod 2$. *Moreover,* $\epsilon_2 \equiv \epsilon_1 \bmod 4$ *if* $\epsilon_3 \equiv \epsilon_1 \bmod 8$ *and* $\epsilon_2 \equiv -\epsilon_1 \bmod 4$ *if* $\epsilon_3 \equiv 5\epsilon_1 \bmod 8$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}\epsilon_1 x_1^2 + 2^{a_2}\epsilon_2 x_2^2 + 2^{\delta_{13}}\epsilon_1 x_1 x_3 + 2^{\delta_{23}}\epsilon_2 x_2 x_3 + 2^{a_3}\epsilon_1 u x_3^2.$$

Here $u = (\epsilon_1 + \epsilon_2)/2$ *if* $\epsilon_2 \equiv \epsilon_1 \bmod 4$ *and* $u = (3\epsilon_1 + \epsilon_2)/2$ *if* $\epsilon_2 \equiv -\epsilon_1 \bmod 4$.

(c) *Suppose* $\mu_1 \not\equiv \mu_2 \equiv \mu_3 \bmod 2$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2, \mu_3 + 2)$ *and* $a_2 \not\equiv a_1 \bmod 2$. *The quadratic form with respect to an optimal basis is as in (a) and (b) with the role of* x_1 *and* x_2 *reversed.*

(d) *Suppose* $\mu_1 \equiv \mu_2 \bmod 2$ *and* $\mu_2 = \mu_3$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_1 \not\equiv a_2 \bmod 2$. *Moreover,* $\epsilon_1 \equiv \epsilon_2 \equiv \epsilon_3 \bmod 4$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}\epsilon_1 x_1^2 + 2^{a_2}u_2 x_2^2 + 2^{\delta_{13}}\epsilon_1(x_1x_2 + x_1x_3) + 2^{\delta_{23}}\epsilon_1 x_2 x_3 + 2^{a_3}u_3 x_3^2.$$

Here $u_i = (\epsilon_1 + \epsilon_i)/2$ *for* $i = 2, 3$.

(e) *Suppose* $\mu_1 \equiv \mu_2 \bmod 2$, $\mu_3 = \mu_2 + 1$ *and* $\epsilon_1 \equiv \epsilon_2 \bmod 4$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_2 \not\equiv a_1 \bmod 2$. *Moreover,* $\epsilon_2 \equiv \epsilon_1 \bmod 8$ *if* $\epsilon_3 \equiv \epsilon_1 \bmod 4$ *and* $\epsilon_2 \equiv 5\epsilon_1 \bmod 8$ *if* $\epsilon_3 \equiv -\epsilon_1 \bmod 4$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}\epsilon_1 x_1^2 + 2^{a_2}u_2 x_2^2 + 2^{\delta_{13}}\epsilon_1(x_1x_2 + x_1x_3) + 2^{\delta_{23}}u_2 x_2 x_3 + 2^{a_3}u_3 x_3^2.$$

Here $u_2 = (\epsilon_1 + \epsilon_2)/2$ *and* $u_3 = (\epsilon_1 + \epsilon_3)/2$ *(resp.* $(3\epsilon_1 + \epsilon_3)/2$*) depending on whether* $\epsilon_3 \equiv \epsilon_1 \bmod 4$ *or not.*

(f) *Suppose* $\mu_1 \equiv \mu_2 \bmod 2$, $\mu_3 = \mu_2 + 1$ *and* $\epsilon_1 \equiv -\epsilon_2 \bmod 4$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_1 \equiv a_2 \bmod 2$. *Moreover,* $\epsilon_2 \equiv 3\epsilon_1 \bmod 8$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}\epsilon_1 x_1^2 + 2^{a_2}u_2 x_2^2 + 2^{\delta_{13}}\epsilon_1(x_1x_2 + x_1x_3) + 2^{\delta_{23}}u_{23} x_2 x_3 + 2^{a_3}u_3 x_3^2.$$

Here $u_2 = (\epsilon_1 + \epsilon_2 + 2\epsilon_3)/2$, $u_{23} = (\epsilon_1 + \epsilon_2 + 4\epsilon_3)/2$ *and* $u_3 = \epsilon_1 + 2\epsilon_3$.

(g) *Suppose* $\mu_1 \equiv \mu_2 \equiv \mu_3 \bmod 2$ *and* $\epsilon_1 \equiv \epsilon_2 \bmod 4$ *and* $\mu_3 \geq \mu_2 + 2$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_2 \not\equiv a_1 \bmod 2$. *Moreover,* $\epsilon_3 \equiv \epsilon_1 \bmod 4$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}\epsilon_1 x_1^2 + 2^{a_2}u_2 x_2^2 + 2^{\delta_{12}}\epsilon_1 x_1 x_2 + 2^{\delta_{13}}\epsilon_1 x_1 x_3 + 2^{\delta_{23}}\epsilon_1 x_2 x_3 + 2^{a_3}u_3 x_3^2.$$

Here $u_i = (\epsilon_1 + \epsilon_i)/2$ *for* $i = 2, 3$.

(h) *Suppose* $\mu_1 \equiv \mu_2 \not\equiv \mu_3 \bmod 2$ *and* $\epsilon_1 \equiv \epsilon_2 \bmod 4$ *and* $\mu_3 \geq \mu_2 + 2$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_2 \not\equiv a_1 \bmod 2$. *One of the following two cases holds:*

$$\begin{cases} \epsilon_2 \equiv \epsilon_1 \bmod 8 \text{ and } \epsilon_3 \equiv \epsilon_1 \bmod 4, \\ \epsilon_2 \equiv 5\epsilon_1 \bmod 8 \text{ and } \epsilon_3 \equiv -\epsilon_1 \bmod 4. \end{cases}$$

There exists an optimal basis with respect to which

$$Q(x) = 2^{a_1}\epsilon_1 x_1^2 + 2^{a_2}u_2 x_2^2 + 2^{\delta_{12}}\epsilon_1 x_1 x_2 + 2^{\delta_{13}}\epsilon_1 x_1 x_3 + 2^{\delta_{23}}u_2 x_2 x_3 + 2^{a_3}u_3 x_3^2.$$

Here $u_2 = (\epsilon_1 + \epsilon_2)/2$ *and* $u_3 = (\epsilon_1 + \epsilon_3)/2$ *(resp.* $u_3 = (3\epsilon_1 + \epsilon_3)/2$*) depending on whether* $\epsilon_1 \equiv \epsilon_3 \bmod 4$ *or not.*

(i) *Suppose* $\mu_1 \equiv \mu_2 \not\equiv \mu_3 \bmod 2$, $\mu_3 \geq \mu_2 + 2$ *and* $\epsilon_2 \equiv 3\epsilon_1 \bmod 8$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 2, \mu_3)$ *and* $a_1 \equiv a_2 \bmod 2$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}\epsilon_1 x_1^2 + 2^{a_2}u_2 x_2^2 + 2^{\delta_{12}}\epsilon_1 x_1 x_2 + 2^{a_3}\epsilon_3 x_3^2.$$

Here $u_2 = (\epsilon_1 + \epsilon_2)/2$.

Proof: This follows from the results of Section 4 together with the Lemmas 5.4, 5.5. □

Corollary 5.8 *Suppose that* Q *is anisotropic. Then there exists a basis* $\boldsymbol{\varphi}$ *satisfying (2) such that*

$$\mathrm{ord}(b_{ii}(\boldsymbol{\varphi})) = a_i$$

for $i = 1, 2, 3$.

Proof: This follows immediately from Theorem 5.7 (diagonal case) and Proposition 5.2 (non-diagonal case). □

In Section 6, we give a more conceptual proof of Corollary 5.8. The following lemma gives a list of the small cases.

Lemma 5.9 *Let* Q *be an anisotropic ternary quadratic form over* $\mathbb{Z}_2$ *and suppose that* $a_3 \leq 1$. *Then one of the following possibilities occurs.*

(a) *We have* $(a_1, a_2, a_3) = (0, 0, 1)$. *In this case* Q *is not diagonalizable; it is of the form*

$$Q(x) = x_1^2 + x_1 x_2 + x_2^2 + \epsilon_3 2 x_3^2.$$

(b) *We have* $(a_1, a_2, a_3) = (0, 1, 1)$ *and* Q *is not diagonalizable. Then* Q *is of the form*

$$Q(x) = \epsilon_1 x_1^2 + 2(x_2^2 + x_2 x_3 + x_3^2).$$

(c) *We have* $(a_1, a_2, a_3) = (0, 1, 1)$ *and* Q *is diagonalizable. Then* Q *is as in Theorem 5.7.(d) with* $a_1 = \delta_{13} = 0$ *and* $a_2 = a_3 = \delta_{23} = 1$.

6 Alternative version of the Gross–Keating invariants for anisotropic forms

We fix an arbitrary prime number ℓ and a free quadratic module (L, Q) over $\mathbb{Z}_\ell$ of rank n. We assume that (L, Q) is anisotropic, i.e. that $Q(\psi) = 0$ implies $\psi = 0$. Under this assumption, there is an alternative definition of the Gross–Keating invariants and a very useful characterization of optimal bases.

We define a function $v : L \to \mathbb{Z} \cup \{\infty\}$ by the rule

$$v(\psi) := \mathrm{ord}_\ell Q(\psi).$$

For $\psi \in L$ and $x \in \mathbb{Z}_p$ we have

$$v(x\psi) = 2\mathrm{ord}_\ell(x) + v(\psi). \tag{13}$$

Lemma 6.1 *The function* v *satisfies the triangle inequality*

$$v(\psi + \psi') \geq \min\left(v(\psi), v(\psi')\right). \tag{14}$$

Moreover, if the inequality in (14) *is strict we have* $v(\psi) = v(\psi')$.

Proof: If ψ and ψ' are linearly dependent the claim is obvious. We may hence assume that they are linearly independent. For $x, y \in \mathbb{Z}_\ell$ we write

$$Q(x\psi + y\psi') = ax^2 + y^2b + cxy.$$

Suppose that $v(\psi + \psi') < v(\psi), v(\psi')$. Then $\mathrm{ord}_\ell(a + b + c) < \mathrm{ord}_\ell(a)$, $\mathrm{ord}_\ell(b)$. The usual triangle inequality for ord_ℓ implies

$$\mathrm{ord}_\ell(c) = \mathrm{ord}_\ell(a + b + c) < \mathrm{ord}_\ell(a),\, \mathrm{ord}_\ell(b).$$

Using Newton approximation, it is now easy to show there exists $x \in \mathbb{Z}_\ell^\times$ such that $Q(x\psi + \psi') = 0$. This contradicts the assumption that (L, Q) is anisotropic and proves (14). The second assertion of the lemma follows from (14), applied to a suitable combination of the vectors $\pm\psi$, $\pm\psi'$ and $\psi + \psi'$. $\square$

Remark 6.2 If $n \leq 3$, one gets an alternative proof of Lemma 6.1 by noting that (L, Q) is represented by the quaternion division algebra D over $\mathbb{Q}_\ell$, equipped with its norm form. The function v is then the restriction of the standard valuation of D.

Let $\boldsymbol{\psi} = (\psi_i)$ be a basis of L. For $i = 1, \ldots, n$, let $L_{i-1} \subset L$ be the subspace (of rank $i - 1$) spanned by $\psi_1, \ldots, \psi_{i-1}$. We define a function $\tilde{v}_i : L/L_{i-1} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by the rule

$$\tilde{v}_i(\psi + L_{i-1}) := \max\left(v(\psi') \,|\, \psi' \in \psi + L_{i-1}\right).$$

Note that $\tilde{v}_i(\psi) = \infty$ if and only of $\psi \in L_{i-1}$.

Definition 6.3 A basis $\boldsymbol{\psi} = (\psi_i)$ of L is called *ideal*, if

$$v(\psi_i) = \tilde{v}_i(\psi_i + L_{i-1}) = \min_{\psi \in L}\left(\tilde{v}_i(\psi + L_{i-1})\right)$$

holds for $i = 1, \ldots, n$.

It is clear that there exists an ideal basis of L. The next lemma gives a useful characterization of an ideal basis.

Lemma 6.4 *A basis $\boldsymbol{\psi} = (\psi_i)$ of L is ideal if and only if*

$$v(\psi_i) \leq v(\psi_j) \quad \text{for } i \leq j, \tag{15}$$

and for all $(x_i) \in \mathbb{Z}_\ell^n$ we have

$$v(\sum_i x_i\psi_i) = \min_i v(x_i\psi_i). \tag{16}$$

Proof: Let $\boldsymbol{\psi} = (\psi_i)$ be a basis of L. If (15) and (16) hold, then one easily checks from Definition 6.3 that $\boldsymbol{\psi}$ is ideal.

Conversely, suppose that $\boldsymbol{\psi}$ is ideal. The inequality (15) follows directly from Definition 6.3. It remains to prove (16). Fix $(x_i) \in \mathbb{Z}_\ell^n$ and k with $1 \leq k \leq n$. Set $\varphi_k := \sum_{i<k} x_i\psi_i$. We claim that

$$v(\varphi_k + x_k\psi_k) = \min\left(v(\varphi_k),\, v(x_k\psi_k)\right). \tag{17}$$

From this claim, (16) follows by induction.

For $k = 1$, the claim is obvious. To prove it for $k > 1$ we may assume that it holds for $k' = k - 1$. Also, by the triangle inequality (14), the left hand side of (17) is greater than or equal to the right hand side. Suppose that the left hand side is strictly greater than the right hand side. Then we have $v(\varphi_k) = v(x_k\psi_k)$. Using (13), (15) and the claim for $k' = k-1$, we find that $\mathrm{ord}_\ell(x_k) \leq \mathrm{ord}_\ell(x_i)$ for all $i \leq k$. After dividing by x_k, we may therefore assume that $x_k = 1$. However, by the definition of an ideal basis we have

$$v(\varphi_k) \;=\; v(\psi_k) \geq v(\varphi_k + \psi_k).$$

This contradicts our assumption and proves the claim. □

Let us fix an ideal basis $\boldsymbol{\psi} = (\psi_1, \ldots, \psi_n)$ of L, and set

$$a_i := v(\psi_i), \quad i = 1, \ldots, n.$$

We want to show that the a_i are the Gross–Keating invariants of (L, Q). We first check that (a_i) lies in the set S (Section 1). For this we write the quadratic form Q as follows:

$$Q(\sum_i x_i\psi_i) = \sum_{i\leq j} b_{ij}x_ix_j.$$

We set $a_{ij} := \mathrm{ord}_\ell(b_{ij})$. Note that $a_i = a_{ii}$.

Proposition 6.5 *For $1 \leq i \leq j \leq n$ we have*

$$a_{ij} \geq \frac{a_i + a_j}{2}.$$

Proof: The case $i = j$ being trivial, we may assume that $i < j$. Our proof is by contradiction. First we assume that $2a_{ij} + 1 < a_i + a_j$. We set $c := \max(a_{ij} - a_i + 1, 0)$ and look at the right hand side of

$$Q(\ell^c\psi_i + \psi_j) = b_{ii}\ell^{2c} + b_{jj} + b_{ij}\ell^c.$$

The three terms of this sum have ℓ-valuation $a_i + 2c$, a_j and $a_{ij} + c$, respectively. By our choice of c we have

$$a_{ij} + c < \min(a_i + 2c,\, a_j).$$

It follows that

$$v(\ell^c\psi_i + \psi_j) = a_{ij} + c < \min(v(\ell^c\psi_i),\, v(\psi_j)).$$

This contradicts the triangle inequality and excludes the case $2a_{ij} + 1 < a_i + a_j$.

It remains to exclude the case $2a_{ij} + 1 = a_i + a_j$. Since $a_i \leq a_j$ we have $c := a_{ij} - a_i \geq 0$. Let $x \in \mathbb{Z}_\ell^\times$ be a ℓ-adic unit. Then

$$Q(\ell^c x\psi_i + \psi_j) = b_{ii}\ell^{2c}x^2 + b_{jj} + b_{ij}\ell^c x. \tag{18}$$

By our choice of c we have

$$a_i + 2c = a_j - 1 = a_{ij} + c.$$

We see that on the right hand side of (18), the first and the last term have the minimal valuation $a_j - 1$, while the middle term has valuation a_j. Therefore, for an appropriate choice of x, we get

$$v(\ell^c x\psi_i + \psi_j) \geq a_j > \min(v(\ell^c x\psi_i), v(\psi_j)).$$

But this contradicts Lemma 6.4, (16). The proposition follows. □

Proposition 6.6 *An ideal basis is also optimal (Definition 1.2). In other words: if $\boldsymbol{\psi} = (\psi_i)$ is an ideal basis of L, then (a_i) (where $a_i := v(\psi_i)$) are the Gross–Keating invariants of (L, Q).*

Proof: The previous proposition says that (a_i) is an element of S. It remains to show that (a_i) is a maximal element, with respect to the lexicographical ordering.

Let $\boldsymbol{\psi}' = (\psi'_i)$ be an arbitrary basis of L, and let (a'_i) be an element of $S(\boldsymbol{\psi}')$ (Section 1). We will show that $a'_k \leq a_k$ for $k = 1, \ldots, n$, which proves the proposition. Write

$$\psi'_i = \sum_j x_{ij}\psi_j, \qquad \text{with} \qquad (x_{ij}) \in \mathrm{GL}_n(\mathbb{Z}_\ell).$$

The condition $(a'_i) \in S(\boldsymbol{\psi}')$ together with Lemma 6.4 shows that

$$a'_i \leq v(\psi'_i) = \min_j (a_j + 2\mathrm{ord}_\ell(x_{ij})). \tag{19}$$

Using that (x_{ij}) is invertible, one shows that there exists at least one pair of indices (ij) with $k \leq i$ and $j \leq k$ such that x_{ij} is a unit. Applying (19) and (15) we get

$$a'_k \leq a'_i \leq a_j \leq a_k.$$

This is what we had to prove. □

Corollary 6.7 *Let $\boldsymbol{\psi} = (\psi_i)$ be an ideal basis of L. Fix an index k and write $\psi_k = p\psi'_k$, with $\psi'_k \in L \otimes \mathbb{Q}_\ell$. Let L' be the module generated by L and by ψ'_k. Then the Gross–Keating invariants of L' are $(a_1, \ldots, a_k - 2, \ldots, a_n)$ (in some order).*

Proof: Let $\boldsymbol{\psi}' := (\psi_1, \ldots, \psi'_k, \ldots, \psi_n)$. For $(x_i) \in \mathbb{Z}_\ell^n$, Lemma 6.4 shows that

$$\begin{aligned} v(x_k\psi'_k + \sum_{i\neq k} x_i\psi_i) \;&=\; v(x_k\psi_k + \sum_{i\neq k} px_i\psi_i) - 2 \\ &= \min\,(v(x_k\psi_k),\, v(px_i\psi_i),\, i \neq k) - 2 \\ &= \min\,(v(x_k\psi'_k),\, v(x_i\psi_i),\, i \neq k). \end{aligned}$$

Again by Lemma 6.4 we conclude that $\boldsymbol{\psi}'$ (in some order) is an ideal basis of L'. The corollary follows now from the previous proposition. □

Remark 6.8 Corollary 6.7 is wrong without the assumption that (L, Q) is anisotropic. Consider, for instance, the (isotropic) quadratic form $Q(x) = x_1^2 - x_2^2 + 4x_3^2$ over $\mathbb{Z}_2$. Dividing the last vector of the standard basis by 2 we obtain the quadratic form $Q'(x) = x_1^2 - x_2^2 + x_3^2$. According to Proposition 4.2(b), the Gross–Keating invariants of Q are $(0, 2, 2)$, while the invariants of Q' are $(0, 1, 1)$.

Lemma 6.9 *Let $M \subset L$ be a sublattice, i.e. a sub-$\mathbb{Z}_\ell$-module of rank n. Let $b_1, \ldots, b_n$ be the Gross-Keating invariants of $(M, Q|_M)$. Then $b_i \geq a_i$.*

Proof: We choose ideal bases $(\psi_1, \ldots, \psi_n)$ for L and $(\varphi_1, \ldots, \varphi_n)$ for M. Then $a_i = v(\psi_i)$ and $b_i = v(\varphi_i)$. Let us fix an index $i \in \{1, \ldots, n\}$ and show $b_i \geq a_i$. For an element $\psi = \sum_j x_j\psi_j$ of L, we set $\psi' := \sum_{j<i} x_j\psi_j$ and $\psi'' := \sum_{j\geq i} x_j\psi_j$. Then $\psi = \psi' + \psi''$ and $v(\psi'') \geq a_i$. Since the vectors $\varphi'_1, \ldots, \varphi'_i$ lie in a subspace of rank $i-1$, there exist $x_1, \ldots, x_i \in \mathbb{Z}_\ell$, not all zero, such that $\sum_{j\leq i} x_j\varphi'_j = 0$. Then

$$\sum_{j\leq i} x_j\varphi_j \;=\; \sum_{j\leq i} x_j\varphi''_j.$$

Applying Lemma 6.4 (16) to the left hand side and the triangle inequality (14) to the right hand side, we conclude that

$$\min_{j\leq i}\,(b_j + 2\mathrm{ord}_\ell(x_j)) \;\geq\; \min_{j\leq i}\,(v(\varphi''_j) + \mathrm{ord}_\ell(x_j)) \;\geq\; \min_{j\leq i}\,(a_i + 2\mathrm{ord}_\ell(x_j)).$$

For the index j for which $\mathrm{ord}_\ell(x_j)$ takes its minimal value we get $a_i \leq b_j \leq b_i$. This proves the lemma. □

References

[1] J. W. S. Cassels. *Rational quadratic forms.* Cambridge University Press, 1978.

[2] B. H. Gross and K. Keating. On the intersection of modular correspondences. *Invent. Math.* 112, 225–245, 1993.

[3] J-P. Serre. *Cours d'arithmétique.* Presses Universitaires de France, 1970.

[4] T. Yang. Local densities of 2-adic quadratic forms. *J. Number Theory* 108, 287–345, 2004.

[5] T. Yang. Isotropic or anisotropic. Letter to M. Rapoport.

Mathematisches Insitut
Heinrich-Heine-Universität
40225 Düsseldorf
bouw@math.uni-duesseldorf.de