DEFINITE REGULAR QUADRATIC FORMS OVER $\mathbb{F}_q[T]$

WAI KIU CHAN AND JOSHUA DANIELS

(Communicated by David E. Rohrlich)

ABSTRACT. Let q be a power of an odd prime, and $\mathbb{F}_q[T]$ be the ring of poly-
nomials over a finite field $\mathbb{F}_q$ of q elements. A quadratic form f over $\mathbb{F}_q[T]$ is
said to be regular if f globally represents all polynomials that are represented
by the genus of f. In this paper, we study definite regular quadratic forms over
$\mathbb{F}_q[T]$. It is shown that for a fixed q, there are only finitely many equivalence
classes of regular definite primitive quadratic forms over $\mathbb{F}_q[T]$, regardless of
the number of variables. Characterizations of those which are universal are
also given.

1. INTRODUCTION

Let $\mathfrak{o}$ be the ring of integers in a global field. Given a quadratic form f over $\mathfrak{o}$, it
is a fundamental question to determine the set of elements in $\mathfrak{o}$ that are represented
by f. A necessary condition for an element a of $\mathfrak{o}$ to be represented by f is that a is
represented by the genus of f, i.e. a is represented by f over all local completions
of $\mathfrak{o}$. It is known that in general this condition is not sufficient to guarantee a global
representation of a by f. When f represents all elements in $\mathfrak{o}$ that are represented
by its genus, we say that f is *regular*.

It was Dickson [5] who first studied regular quadratic forms over $\mathbb{Z}$. Later on,
Watson [17, 18] showed that there are only finitely many equivalence classes of
regular positive definite primitive ternary quadratic forms over $\mathbb{Z}$, and in [17] he
employed an arithmetic argument to obtain explicit upper bounds on the prime
power divisors of the discriminant of these regular forms. There has been consid-
erable recent interest in extending this arithmetic treatment to quadratic forms
satisfying other kinds of regularity conditions [1, 2, 3, 4]. See [2] for a summary of
the recent developments along this line of research.

Another example of $\mathfrak{o}$ of special interest is the ring of integers in a rational
function field with a finite constant field. Let q be a power of an odd prime and
$\mathbb{F}_q[T]$ be the polynomial ring over a finite field $\mathbb{F}_q$ of q elements. The goal of this
paper is to give a detailed investigation of regular quadratic forms over $\mathbb{F}_q[T]$. We
follow the arithmetic approach developed by Watson in [17]. As in the case of
quadratic forms over $\mathbb{Z}$, we restrict our attention to definite quadratic forms over
$\mathbb{F}_q[T]$, i.e. those quadratic forms which are anisotropic over $\mathbb{F}_q(T)_\infty$. Here ∞ is the
infinite place induced by the degree function. Henceforth, unless stated otherwise,

all quadratic forms over $\mathbb{F}_q[T]$ *considered in this paper are definite*; thus the number of variables of any quadratic form in the subsequent discussion is less than or equal to 4.

Some of the results presented in this paper mirror the existing finiteness theorems for regular quadratic forms over $\mathbb{Z}$. For example, we show that there are only finitely many equivalence classes of regular primitive binary and ternary quadratic forms over $\mathbb{F}_q[T]$ (Theorems 2.2 and 3.12). However, there are others for which their analogous statements for quadratic forms over $\mathbb{Z}$ are simply not true at all. For instance, we prove that all regular ternary quadratic forms over $\mathbb{F}_q[T]$ of square-free discriminant must have class number 1 (Corollary 3.9), and that there are only finitely many regular primitive quaternary quadratic forms over $\mathbb{F}_q[T]$ (Theorem 4.7). Combining the main theorems obtained in Sections 2 to 4, we have the following finiteness result on regular quadratic forms over $\mathbb{F}_q[T]$.

Theorem 1.1. *For a fixed finite field* $\mathbb{F}_q$, *there are only finitely many equivalence classes of regular quadratic forms over* $\mathbb{F}_q[T]$.

A lot of these regular quadratic forms have class number 1. Examples include binary regular quadratic forms (Theorem 2.2), ternary regular quadratic forms of square-free discriminants (Corollary 3.9) and universal quadratic forms (Theorem 4.2). It would be interesting to have explicit examples of regular quadratic forms whose class numbers are not 1.

Remark 1.2. It is known that there are regular quadratic forms over $\mathbb{Z}$ whose class numbers are not 1. These quadratic forms exist when the number of variables is at least 3. Examples of these forms in 3 or 4 variables can be found in [11] and [7] respectively. In fact, an infinite family of inequivalent regular quaternary quadratic forms over $\mathbb{Z}$ is exhibited in [7].

For our convenience, we denote $\mathbb{F}_q[T]$ by $\mathbf{A}$ and let $\mathbf{K}$ be the field of fractions of $\mathbf{A}$. A prime in $\mathbf{A}$ is a monic irreducible polynomial. The symbols $\mathfrak{p}$ and $\mathfrak{q}$ always represent finite places of $\mathbf{K}$, or the prime ideals that induce the places. The subsequent discussion will be conducted in the geometric language of quadratic spaces and lattices, and any unexplained notation and terminology can be found in [15]. The term *lattice* always means a finitely generated $\mathbf{A}$-module on a definite quadratic space over $\mathbf{K}$. It is obvious that regularity remains intact upon any scaling of the quadratic map on the lattice. Therefore, we further assume throughout the paper that every lattice L is *primitive*, i.e. $\mathfrak{s}(L) = \mathfrak{n}(L) = \mathbf{A}$.

In [6] and [9], it is shown that every lattice L has a reduced basis $\mathcal{B} = \{v_1, v_2, \ldots\}$ meaning that $\deg Q(v_i) \le \deg Q(v_j)$ and $\deg B(v_i, v_j) < \deg Q(v_i)$ for any $v_i, v_j \in \mathcal{B}$ with $i < j$. The i-th successive minimum of L, denoted $\mu_i(L)$, is defined to be $\deg Q(v_i)$. It is known that the increasing sequence $\mu_1(L), \mu_2(L), \ldots$ is independent of the reduced basis $\mathcal{B}$, and that the sum of all the successive minima of L is equal to $\deg(d(L))$ [9, Lemma 2]. For any $1 \le k \le \text{rank}(L)$, the sublattice spanned by the first k vectors in $\mathcal{B}$ is called a $k \times k$ section of L.

For any finite place $\mathfrak{p}$ of $\mathbf{K}$, let

$$\Lambda_{\mathfrak{p}}(L) = \{v \in L : Q(z) \equiv Q(v + z) \bmod \mathfrak{p} \, \forall z \in L\}.$$

By scaling the quadratic map on $\Lambda_{\mathfrak{p}}(L)$ suitably, we obtain a primitive lattice $\lambda_{\mathfrak{p}}(L)$. The proof of the following property of this $\lambda_{\mathfrak{p}}$-transformation can be found in [2, Section 2]. For its other properties, we refer the readers to [1, 2, 3, 4].

Lemma 1.3. *If $L_{\mathfrak{p}} = M_{\mathfrak{p}} \perp N_{\mathfrak{p}}$ where $M_{\mathfrak{p}}$ is unimodular and $\mathfrak{s}(N_{\mathfrak{p}}) \subseteq \mathfrak{p}^2$, then $\Lambda_{\mathfrak{p}}(L)_{\mathfrak{p}} = \mathfrak{p}M_{\mathfrak{p}} \perp N_{\mathfrak{p}}$ and $\Lambda_{\mathfrak{p}}(L)_{\mathfrak{q}} = L_{\mathfrak{q}}$ for all $\mathfrak{q} \neq \mathfrak{p}$. Furthermore, if L is regular, then $\lambda_{\mathfrak{p}}(L)$ is also regular.*

2. Regular binary lattices

We begin this section with the following approximation lemma. Its proof resembles that of the binary case of the approximation theorem in [12, Theorem 6.2.1]. We present it here for the convenience of the readers.

Lemma 2.1. *Let M be a binary lattice and Ω be a finite set of finite places for which $M_{\mathfrak{p}}$ is unimodular for all $\mathfrak{p} \notin \Omega$. Given any collection $\{v_{\mathfrak{p}} \in M_{\mathfrak{p}} : \mathfrak{p} \in \Omega\}$ and integer $s > 0$, there exists $v \in M$ such that $v \equiv v_{\mathfrak{p}} \mod \mathfrak{p}^s M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Omega$, and that $Q(v) \in \mathbf{A}_{\mathfrak{p}}^{\times}$ for all $\mathfrak{p} \notin \Omega$ with precisely one exception $\mathfrak{p} = \mathfrak{q}$ where $\mathrm{ord}_{\mathfrak{q}}(Q(v)) = 1$.*

Proof. Let V be the definite quadratic space underlying M. By scaling V suitably, we may assume that V represents 1. Therefore, we can identify V with the quadratic extension $\mathbf{E} = \mathbf{K}(\sqrt{-d(M)})$, and Q becomes the norm $\mathbb{N}$ from $\mathbf{E}$ to $\mathbf{K}$. Let $\mathfrak{O}$ be the maximal order in $\mathbf{E}$. Since $M_{\mathfrak{p}}$ represents a unit in $\mathbf{A}_{\mathfrak{p}}^{\times}$ for any $\mathfrak{p} \notin \Omega$, we may enlarge Ω, if necessary, so that $M_{\mathfrak{p}} = \mathfrak{O}_{\mathfrak{p}}$ for all $\mathfrak{p} \notin \Omega$. Using the weak approximation property for $\mathbf{E}$, we can find $w \in \mathbf{E}^{\times}$ which is sufficiently close to $v_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Omega$, and $w \in M_{\mathfrak{p}}$ for all $\mathfrak{p} \notin \Omega$. Decompose the principal ideal $(w) = w\mathfrak{O}$ as

$$(w) = \tilde{\mathfrak{m}}\tilde{\mathfrak{n}},$$

where the prime divisors of $\tilde{\mathfrak{n}}$ do not lie above any prime ideals in Ω. Since $w \in M_{\mathfrak{p}} = \mathfrak{O}_{\mathfrak{p}}$ for all $\mathfrak{p} \notin \Omega$, $\tilde{\mathfrak{n}}$ is an integral ideal. Let $\mathfrak{P}$ be the ideal

$$(\prod_{\mathfrak{p} \in \Omega} \mathfrak{p})^t$$

where t is a sufficiently large positive integer. By the Čebotarev density theorem (see [8] for a proof of the function field version), the ray class (mod $\mathfrak{P}$) represented by $\tilde{\mathfrak{n}}$ contains a prime ideal $\tilde{\mathfrak{q}}$ such that $\mathbb{N}(\tilde{\mathfrak{q}}) = \mathfrak{q}$ is a prime ideal in $\mathbf{A}$. Therefore, there exists $z \in \mathbf{E}$ such that $z \equiv 1 \mod \mathfrak{P}$ and $\tilde{\mathfrak{q}} = \tilde{\mathfrak{n}}z$. Letting $v = wz$, one can verify that v satisfies all the requirements. $\square$

Theorem 2.2. *A regular binary lattice must have class number 1. In particular, there are only finitely many isometry classes of regular primitive binary lattices.*

Proof. Let L be a regular binary lattice, and let Ω be a finite set of finite places $\mathfrak{p}$ for which $L_{\mathfrak{p}}$ is unimodular for all $\mathfrak{p} \notin \Omega$. Since L is assumed to be primitive, $L_{\mathfrak{p}}$ represents a unit $\epsilon_{\mathfrak{p}}$ for each $\mathfrak{p} \in \Omega$. Suppose that M is a lattice in $\mathrm{gen}(L)$. By the previous lemma, there exists $v \in M$ such that $Q(v) \in \epsilon_{\mathfrak{p}}\mathbf{A}_{\mathfrak{p}}^{\times 2}$ for all $\mathfrak{p} \in \Omega$, and that $Q(v) \in \mathbf{A}_{\mathfrak{p}}^{\times}$ for all $\mathfrak{p} \notin \Omega$ with one exception $\mathfrak{p} = \mathfrak{q}$ where $\mathrm{ord}_{\mathfrak{q}}(Q(v)) = 1$. Let π be the prime that generates $\mathfrak{q}$.

Since $Q(v)$ is represented by $M \in \mathrm{gen}(L)$ and L is regular, $Q(v)$ is also represented by L. By replacing L by a lattice in its class, we may assume that L also contains v. Let w be a basis vector of the orthogonal complement of v in L, and let N be the sublattice of L spanned by v and w. Since $Q(v)$ is a unit in $\mathbf{A}_{\mathfrak{p}}$ for any $\mathfrak{p} \neq \mathfrak{q}$, $N_{\mathfrak{p}} = L_{\mathfrak{p}}$ for those $\mathfrak{p}$. At $\mathfrak{q}$, $Q(v)$ is a uniformizer. This implies that $L_{\mathfrak{p}}$ must be isometric to $\langle 1, -1 \rangle$, and $N_{\mathfrak{q}} \cong \langle \pi, -\pi \rangle$. So, there are exactly two lattices in $\mathrm{gen}(L)$ which contain N, and they are obtained by adjoining $(v + w)/\pi$ and

$(v - w)/\pi$ respectively to N. In this case these two lattices must be M and L, and they are isometric via the symmetry τ_v. In particular, M and L are in the same class. □

3. Regular ternary lattices

In this section, L is a ternary lattice and V is the ambient quadratic space. By scaling the quadratic map by δ if necessary, we may assume that V_∞ is isometric to either $\langle 1, -\delta, T \rangle$ or $\langle 1, T, -\delta T \rangle$. By the local square theorem [9, Lemma 1] it follows that all monic even degree polynomials in $\mathbf{A}$ are squares in $\mathbf{K}_\infty$. So, V_∞ represents all monic polynomials and, in particular, all primes in $\mathbf{A}$.

3.1. **Lattices with special local structures.** For the sake of discussion, we say that a lattice L is *special* if it satisfies the following two conditions:

(1) $L_{\mathfrak{p}}$ has a unimodular component of rank 2 for every $\mathfrak{p}$,
(2) $\text{ord}_{\mathfrak{p}}(d(L)) \leq 1$ for every $\mathfrak{p}$ of degree ≤ 2.

For example, a lattice of square-free discriminant is special. It follows from the above definition that if L is special, then $L_{\mathfrak{p}}$ represents all units in $\mathbf{A}_{\mathfrak{p}}^\times$ for each finite place $\mathfrak{p}$, and hence $\text{gen}(L)$ represents 1.

Lemma 3.1. *There exists a prime g of degree 2 such that $\left(\frac{g}{T}\right) = -1$.*

Proof. Let $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^2 - \delta\beta^2 = \delta$, and let g be the polynomial $T^2 - 2\alpha T + \delta$. It is clear that $\left(\frac{g}{T}\right) = -1$. The roots of g are $\alpha \pm \beta\sqrt{\delta}$. Since δ is a non-square in $\mathbb{F}_q$, $\beta \neq 0$ and hence $\alpha \pm \beta\sqrt{\delta} \notin \mathbb{F}_q$. Therefore, g is irreducible over $\mathbb{F}_q$. □

Proposition 3.2. *Suppose that L is a regular special ternary lattice. Then*

$$(\mu_1(L), \mu_2(L), \mu_3(L)) = (0, 0, 1), (0, 0, 3) \text{ or } (0, 1, 1).$$

Consequently, $\deg(d(L)) \leq 3$ and there are only finitely many isometry classes of regular special ternary lattices.

Proof. Suppose that $V_\infty \cong \langle 1, -\delta, T \rangle$. In this case, L represents every element in $\mathbb{F}_q^\times$. Therefore, $\langle 1, -\delta \rangle$ is represented by L and $\mu_1(L) = \mu_2(L) = 0$. If T is represented by L, then $\mu_3(L) \leq 1$ because T is not represented by $\langle 1, -\delta \rangle$. Suppose that T is not represented by L. This could happen only when $L_{\mathfrak{p}} \cong \langle 1, -\delta, \delta T \rangle$, where $\mathfrak{p} = (T)$. Let g be the prime obtained in Lemma 3.1. It is clear that gT is represented by V_∞ and $L_{\mathfrak{q}}$ for all $\mathfrak{q} \neq (g)$. At $\mathfrak{q} = (g)$, δ becomes a square in $\mathbf{A}_{\mathfrak{q}}^\times$, and hence $\langle 1, -\delta \rangle$ is the hyperbolic plane. Therefore, $L_{\mathfrak{q}}$ represents gT as well. Consequently, L represents gT and $\mu_3(L) \leq 3$. Since V_∞ is anisotropic, $\mu_3(L)$ can only be 1 or 3 in this case.

If $V_\infty \cong \langle 1, T, -\delta T \rangle$, then L represents 1 and therefore $\mu_1(L) = 0$. Also, L represents either T or δT. If both T and δT are represented by L, then $\mu_2(L) = \mu_3(L) = 1$. So, we may assume that only one of T and δT is represented by L. Without loss of generality, let us assume that T, but not δT, is represented by L. Then L represents the binary lattice $\langle 1, T - \alpha^2 \rangle$ for some $\alpha \in \mathbb{F}_q$. Any monic linear polynomial represented by $\langle 1, T - \alpha^2 \rangle$ is of the form $T - \alpha^2 + \gamma^2$ for some $\gamma \in \mathbb{F}_q$. Therefore, the number of monic linear polynomials represented by $\langle 1, T - \alpha^2 \rangle$ is at most $\frac{q+1}{2}$. This means that there is a monic linear polynomial f which is not represented by $\langle 1, T - \alpha^2 \rangle$. Note that δf is also not represented by $\langle 1, T - \alpha^2 \rangle$. If

f is represented by L, then $\mu_3(L) = 1$. Otherwise, $L_{\mathfrak{q}} \cong \langle 1, -\delta, \delta f \rangle$ where $\mathfrak{q} = (f)$. But then δf is represented by L and hence $\mu_3(L) = 1$ again. $\qquad \square$

Lemma 3.3. *Suppose that $q = 3$. Let $\mathcal{L}$ be the lattice $\langle 1, 1, T(T-1)(T+1) \rangle$. Then $\mathcal{L}$ has class number 1 and hence it is regular.*

Proof. Let M be a lattice in $\mathrm{gen}(\mathcal{L})$. Then $(\mu_1(M), \mu_2(M), \mu_3(M))$ has only three possibilities: $(1, 1, 1), (0, 1, 2)$, and $(0, 0, 3)$. The first possibility is not admissible because V_∞ would have been isotropic. If the second possibility occurs, then

$$M \cong \langle \epsilon \rangle \perp \begin{bmatrix} f & \alpha \\ \alpha & g \end{bmatrix}$$

where $\epsilon \in \{1, \delta\}$, f is linear and g is of degree 2. Moreover, α must be 0 because f divides $d(M)$. Since V_∞ in this case is isometric to $\langle 1, 1, T \rangle$, the leading coefficient of f should be a square. Without loss of generality, we assume that f is monic, and hence $T(T-1)(T+1) = f(f-1)(f+1)$. If $\mathfrak{q}$ is the place generated by f, then $M_{\mathfrak{q}}$, which is isometric to $\mathcal{L}_{\mathfrak{q}} = \langle 1, 1, f(f-1)(f+1) \rangle$, represents $-f$ but not f. This is a contradiction.

Therefore, $\mu_1(M) = \mu_2(M) = 0$ and hence M represents $\langle 1, 1 \rangle$. This means that $M \cong \langle 1, 1, T(T-1)(T+1) \rangle \cong \mathcal{L}$, i.e. the class number of $\mathcal{L}$ is 1, which certainly implies that $\mathcal{L}$ is regular. $\qquad \square$

Lemma 3.4. *If L is special and $\deg(d(L)) = 3$, then L is regular if and only if $q = 3$ and $L \cong \mathcal{L}$. Here $\mathcal{L}$ is the lattice defined in Lemma 3.3.*

Proof. Suppose that L is regular. By Proposition 3.2, $(\mu_1(L), \mu_2(L), \mu_3(L)) = (0, 0, 3)$ and so L represents the binary lattice $\langle 1, -\delta \rangle$. Let ℓ be a linear prime in $\mathbf{A}$. If L represents ℓ, then $\mu_3(L)$ would have been equal to 1 because $\langle 1, -\delta \rangle$ does not represent ℓ. Therefore, L cannot represent ℓ. This implies that L_ℓ does not represent ℓ because L is regular. In particular, L_ℓ is not unimodular and thus $d(L)$ must be divisible by ℓ. As a result, $d(L)$ is divisible by all linear primes in $\mathbf{A}$. This is possible only when there are exactly 3 linear primes in $\mathbf{A}$; hence $q = 3$ and $L \cong \mathcal{L}$. $\qquad \square$

Theorem 3.5. *If L is a ternary lattice with $\deg(d(L)) \leq 2$, then the class number of L is 1 and hence L is regular.*

Proof. Since the quadratic space underlying L is definite, the degree of $d(L)$ cannot be zero. If $\deg(d(L)) = 1$, then $\mu_1(L) = \mu_2(L) = 0$ and $\mu_3(L) = 1$. This implies that $L \cong \langle 1, -\delta \rangle \perp \langle -\delta d(L) \rangle$. Therefore the class number of L is 1, and hence L is regular.

Suppose that $\deg(d(L)) = 2$. Since L is definite, $\mu_1(L) = 0$ and $\mu_2(L) = \mu_3(L) = 1$. Therefore $V_\infty \cong \langle 1, T, -\delta T \rangle$ and $L \cong \langle 1 \rangle \perp N$ where $\mu_1(N) = \mu_2(N) = 1$. For any $L' \in \mathrm{gen}(L)$, it is clear that $\mu_1(L') = 0$ and hence $L' \cong \langle 1 \rangle \perp N'$ for some binary lattice N' with $\mu_1(N') = \mu_2(N') = 1$. By [9, Theorem 2], $L \cong L'$ if and only if $N \cong N'$. Lemma 3.7 below shows that the class number of any binary lattice N with $\mu_1(N) = \mu_2(N) = 1$ is always 1. This shows that the class number of L is also 1 as asserted. $\qquad \square$

Remark 3.6. Note that L is not assumed to be special in the last theorem.

Lemma 3.7. *Let N be a binary lattice. If $\mu_1(N) = \mu_2(N) = 1$, then the class number of N is 1.*

Proof. Let p be the discriminant of N. Since N is definite, we may assume that the leading coefficient of p is $-\delta$. The class number and the proper class number of N are denoted by $h(N)$ and $h^+(N)$ respectively. With respect to a suitable basis of N,

$$(\ddagger) \qquad N \cong \begin{bmatrix} T+a & c \\ c & -\delta T + b \end{bmatrix},$$

where $a, b, c \in \mathbb{F}_q$.

Suppose that p is square-free. Then N is a maximal lattice. Since the degree of p is 2, the field $\mathbf{E} = \mathbf{K}(\sqrt{-p})$ is an imaginary quadratic extension of $\mathbf{K}$ [16, pp. 248-249]. Moreover, if $U(\mathbf{E})$ denotes the group of units in the ring of integers in $\mathbf{E}$, then $[U(\mathbf{E}) : \mathbb{F}_q^\times] = 1$ by [16, Proposition 14.2]. So, by [13, Theorem 6],

$$h^+(N) = \begin{cases} h(\mathbf{E}) & \text{if } p \text{ is irreducible;} \\ \frac{h(\mathbf{E})}{2} & \text{otherwise,} \end{cases}$$

where $h(\mathbf{E})$ is the ideal class number of $\mathbf{E}$. Note that the quantity Q appearing in [13, Theorem 6] is the index $[U(\mathbf{E}) : \mathbb{F}_q^\times]$ because the group of units in $\mathbb{F}_q[T]$ is just $\mathbb{F}_q^\times$. Since the genus of $\mathbf{E}$ is 0 (by, for example, the Riemann-Hurwitz Theorem [16, Theorem 7.16]), the divisor class number of $\mathbf{E}$ is 1 and $h(\mathbf{E}) = 2$ [16, Proposition 14.7]. In particular both $h^+(N)$ and $h(N)$ are 1 when p is reducible.

Suppose that p is irreducible. Then $h^+(N) = 2$ by the above calculation. We shall show that N does not have any improper automorph, and hence $h(N) \neq h^+(N)$. In particular, $h(N)$ must be 1. It is clear that in $(\ddagger)$ c cannot be 0. Suppose that $\begin{bmatrix} \alpha & \gamma \\ \beta & \eta \end{bmatrix}$ is an improper automorph of N, i.e. $\alpha\eta - \beta\gamma = -1$ and

$$\begin{bmatrix} \alpha & \gamma \\ \beta & \eta \end{bmatrix}^t \begin{bmatrix} T+a & c \\ c & -\delta T + b \end{bmatrix} \begin{bmatrix} \alpha & \gamma \\ \beta & \eta \end{bmatrix} = \begin{bmatrix} T+a & c \\ c & -\delta T + b \end{bmatrix}.$$

This leads to the following 6 equations:

$$(\text{I}) \begin{cases} \alpha^2 - \beta^2\delta &= 1 \\ \gamma^2 - \eta^2\delta &= -\delta \\ \alpha\gamma - \eta\beta\delta &= 0 \end{cases} \qquad (\text{II}) \begin{cases} \alpha^2 a + 2c\beta\alpha + \beta^2 b &= a \\ \alpha\gamma a + c\beta\gamma + \alpha c\eta + \eta\beta b &= c \\ \gamma^2 a + 2\eta c\gamma + \eta^2 b &= b. \end{cases}$$

If $\beta = 0$, then $\gamma = 0$ and $\alpha = \eta = \pm 1$. Therefore, $\beta \neq 0$ and $\gamma \neq 0$ as well. Using the first equations in (I) and (II) we obtain

$$\alpha^2[(\delta a + b)^2 - 4c^2\delta] = (\delta a + b)^2.$$

However, $(\delta a + b)^2 - 4c^2\delta$ is the discriminant of the irreducible polynomial p. Hence $\alpha = 0 = \delta a + b$. From the third equation in (II) it follows that $\eta = 0$, whence $-\delta = \gamma^2$. But then $p = (\gamma(T+a) - c)(\gamma(T+a) + c)$, which is impossible.

Now suppose that p is of the form $-\delta\ell^2$ where ℓ is a prime of degree 1. In this case, $0 = (b - \delta a)^2 + 4\delta(ab - c^2) = (b + \delta a)^2 - 4\delta c^2$. This is impossible unless $c = 0$ and $b = -\delta a$; hence $T + a = \ell$ and $N \cong \langle \ell, -\delta\ell \rangle$. Therefore, $h(N) = 1$. $\qquad\square$

Remark 3.8. The above lemma would have been false had we only assumed that $\deg(d(N)) = 2$. For example, if $N \cong \langle 1, p \rangle$ where p is irreducible of degree 2, then $N' = \langle \delta, \delta p \rangle$ is in $\text{gen}(N)$. Obviously, N and N' are not isometric.

All the results obtained thus far imply the following corollary, which is interesting by its own.

Corollary 3.9. *Every regular special ternary lattice has class number* 1. *In particular every regular lattice of square-free discriminant has class number* 1.

Remark 3.10. The above corollary does not hold for ternary $\mathbb{Z}$-lattices. The regular $\mathbb{Z}$-lattice

$$\begin{bmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 6 \end{bmatrix},$$

which corresponds to the entry [1 1 3 0 1 0] in [11, Table 1], is special because its discriminant is 22, which is square-free. But its class number is greater than 1.

3.2. **Main result.** By applying the $\lambda_{\mathfrak{p}}$-transformation (see Lemma 1.3) to a ternary lattice L successively we arrive at a lattice $\lambda^{(\mathfrak{p})}(L)$ whose discriminant is not divisible by $\mathfrak{p}^2$, and at any $\mathfrak{q} \neq \mathfrak{p}$, $L_{\mathfrak{q}} \cong \lambda^{(\mathfrak{p})}(L)_q^{\epsilon}$ for some $\epsilon \in \mathbf{A}_{\mathfrak{q}}^{\times}$. By applying $\lambda^{(\mathfrak{p})}$ to L at every finite place $\mathfrak{p}$, we obtain a lattice $\lambda(L)$ whose discriminant is square-free. If L is regular, then $\lambda^{(\mathfrak{p})}(L)$ and $\lambda(L)$ are also regular.

Proposition 3.11. *Let L be a regular ternary lattice. The degree of every prime divisor of $d(L)$ is bounded by a constant which is independent of L.*

Proof. If π is a prime which divides $d(\lambda(L))$, then $\deg(\pi) \leq 2$ by Proposition 3.2. So we are interested in those prime divisors of $d(L)$ that do not divide $d(\lambda(L))$. Let π be such a prime and $\mathfrak{p}$ be the place generated by π. We may further assume that $\mathrm{ord}_{\mathfrak{q}}(d(L)) \leq 1$ for all $\mathfrak{q} \neq \mathfrak{p}$. Let Ω be the set $\{f \text{ prime} : f \mid d(L), f \neq \pi\}$. Proposition 3.2 implies that the degree of any prime in Ω is at most 2.

Under the conditions we imposed on L, $L_{\mathfrak{p}}$ has two possible structures:

$$(*) \qquad \begin{cases} M_{\mathfrak{p}} \perp N_{\mathfrak{p}}, \text{ where } M_{\mathfrak{p}} \text{ is binary unimodular and } \mathfrak{s}(N_{\mathfrak{p}}) \subseteq \mathfrak{p}^2; \\ \langle a \rangle \perp N_{\mathfrak{p}}, \text{ where } a \in \mathbf{A}_{\mathfrak{p}}^{\times} \text{ and } \mathfrak{s}(N_{\mathfrak{p}}) \subseteq \mathfrak{p}^2. \end{cases}$$

In the first case, L is a special lattice; hence $\deg(\pi) \leq 2$.

For the second case, we may assume that $\deg(\pi) > 1$ and $\pi \notin \Omega$. If L represents all elements in $\mathbb{F}_q^{\times}$, then L represents $\langle 1, -\delta \rangle$, which is not possible. This leaves us two scenarios:

(i) L represents all elements within a single square class in $\mathbb{F}_q^{\times}$;

(ii) L does not represent any element in $\mathbb{F}_q^{\times}$.

In (i), L represents an $\epsilon \in \{1, \delta\}$. Let g_1 and g_2 be two primes of degree 3. In particular, g_1 and g_2 are not in Ω. If $\left(\frac{g_i}{\pi}\right) = \left(\frac{\epsilon}{\pi}\right)$ for some i, then g_i is represented by L for this i. Otherwise, $g_1 g_2$ is a square in $\mathbf{A}_{\mathfrak{p}}^{\times}$. We claim that $\epsilon g_1 g_2$ is represented by L. It suffices to check the representability at ∞. If $\epsilon = 1$, then it is clear that $g_1 g_2$ is represented by V_{∞} since V_{∞} represents all even degree monic polynomials. When $\epsilon = \delta$, then V_{∞} must be isometric to $\langle 1, -\delta, T \rangle$. In this case, V_{∞} represents all even degree polynomials. In conclusion, L contains two linearly independent vectors v and w with $\deg(Q(v)) = 0$ and $\deg(Q(w)) \leq 6$. The degree of the discriminant of the binary sublattice spanned by v and w is then ≤ 6. The structure of $L_{\mathfrak{p}}$ implies that π^2 must divide that discriminant. Therefore, $2 \deg(\pi) \leq 6$ and $\deg(\pi) \leq 3$.

In (ii), $L_{\mathfrak{p}}$ cannot represent 1, and hence a is a non-square in $\mathbf{A}_{\mathfrak{p}}^{\times}$. Suppose that δ remains a non-square unit in $\mathbf{A}_{\mathfrak{p}}$. This implies that δ is not represented by V_{∞} and so $V_{\infty} \cong \langle 1, T, -\delta T \rangle$. Let p_1 and p_2 be two primes of degree 3. For $i = 1$ or 2, either p_i or δp_i is represented by L. Therefore, $2 \deg(\pi) \leq \deg(p_1) + \deg(p_2)$ and $\deg(\pi) \leq 3$.

Now, suppose that δ becomes a square in $\mathbf{A}_{\mathfrak{p}}^{\times}$ (in particular, $\deg(\pi)$ is even). Let $g \in \mathbf{A}$ be one of the smallest (in terms of degree) non-square units in $\mathbf{A}_{\mathfrak{p}}^{\times}$. Since every element in $\mathbb{F}_q^{\times}$ is a square in $\mathbf{A}_{\mathfrak{p}}^{\times}$, the leading coefficient of g can be assumed to be 1. Then g must be a prime and $\deg(g) < \deg(\pi)$. We claim that $g \in \Omega$. Assume to the contrary that g is outside Ω. Let $d = \deg(g)$ and $\ell = \deg(\pi)$. The number of nonzero multiples of g in $\mathbf{A}^{(\ell)} = \{h \in \mathbf{A} : \deg(h) \leq \ell - 1\}$ is $q^{\ell-d} - 1$. Since $q^{\ell-d} - 1 < \frac{q^{\ell}-1}{2}$, there exists a non-residue modulo $\mathfrak{p}$ in $\mathbf{A}^{(\ell)}$ which is not a multiple of g. This implies that there exists a prime $f \in \mathbf{A}^{(\ell)}$, not equal to g, which is a non-residue modulo $\mathfrak{p}$. Both g and f are represented by L, and f is not a square multiple of g. Therefore, $2\ell \leq \deg(fg) \leq d + \ell - 1 < 2\ell$, which is a contradiction.

Now we know that $g \in \Omega$. Let $\mathfrak{q} = (g)$ and f_1, f_2, f_3, f_4 be four primes outside Ω such that f_1 and f_2 are in different square classes modulo $\mathfrak{q}$, and so are f_3 and f_4. Observe that for $i = 1, 2$, exactly one of f_i and gf_i is represented by $L_{\mathfrak{p}}$. Also, at least one of gf_1 and gf_2 is represented by $L_{\mathfrak{q}}$.

If f_1 or f_2 is represented by $L_{\mathfrak{p}}$, then f_1 or f_2 is represented by L. Otherwise, gf_1 and gf_2 are represented by $L_{\mathfrak{p}}$, and this implies that either gf_1 or gf_2 is represented by L. We can repeat the same argument for f_3 and f_4. Then $2 \deg(\pi) \leq 2 \max_i \{\deg(f_i)\} + 2 \deg(g)$ and we are done. $\qquad\square$

Theorem 3.12. *There are only finitely many isometry classes of definite regular primitive ternary lattices.*

Proof. Let S be the set of all finite places $\mathfrak{p}$ for which $\mathrm{ord}_{\mathfrak{p}}(d(L)) > 0$ for some ternary regular lattice L. It follows from the previous proposition that S is a finite set independent of L. Select two disjoint sets of places $\mathcal{P}_1, \mathcal{P}_2$ with the following property:

> if an $\epsilon_{\mathfrak{p}} \in \mathbf{A}_{\mathfrak{p}}^{\times}$ is given at each $\mathfrak{p} \in S$, there exist $g_1 \in \mathcal{P}_1$ and $g_2 \in \mathcal{P}_2$ such that $g_i \equiv \epsilon_{\mathfrak{p}} \bmod \mathfrak{p}$ for $i = 1, 2$ and for all $\mathfrak{p} \in S$.

Note that $\mathcal{P}_1$ and $\mathcal{P}_2$ can be chosen to be finite and independent of all regular ternary lattices.

If L is a regular ternary lattice, it represents at least one prime from $\mathcal{P}_1$ and another prime in $\mathcal{P}_2$. Therefore, $\mu_1(L) + \mu_2(L) \leq 2m$ where $m = \max\{\deg(g) : g \in \mathcal{P}_1 \cup \mathcal{P}_2\}$. Consequently, up to isometry, there are only finitely many possible 2×2 sections of L, and their discriminants have degrees $\leq 2m$. Let B be a binary lattice with $\deg(d(B)) \leq 2m$, and $f_B \in \mathbf{A}$ which is represented by B. Dirichlet's theorem [16, Theorem 4.7] shows that there exists a prime h_B, not dividing $f_B d(B)$, such that if $\mathfrak{q} = (h_B)$, then $B_{\mathfrak{q}}$ is anisotropic. This h_B depends only on B. Now, it follows from the strong form of Dirichlet's theorem [16, Theorem 4.8] that there is a prime $\ell_B \notin S$ such that $\ell_B h_B f_B$ is represented by B_{∞} and $B_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$. However, $\ell_B h_B f_B$ is not represented by $B_{\mathfrak{q}}$. If B is a 2×2 section of a regular ternary lattice L, then $\ell_B h_B f_B$ is represented by L but not by B. Therefore, $\mu_3(L) \leq \max_B\{m, \deg(\ell_B h_B f_B)\}$. $\qquad\square$

4. Quaternary regular lattices

A lattice is called universal if it represents every polynomial in $\mathbf{A}$. It is not hard to see that the rank of a universal lattice must be 4. It is conjectured in [10] that

a lattice is universal if and only if it represents $1, \delta, T$ and δT. This conjecture is confirmed affirmatively in [14]. We offer another proof in the following.

Theorem 4.1. *A lattice L is universal if and only if it represents $1, \delta, T$ and δT.*

Proof. The "only if" part is obvious. Suppose that L represents $1, \delta, T$ and δT. It is clear that L is quaternary, and it represents the binary lattice $\langle 1, -\delta \rangle$. Moreover, $\mu_3(L)$ and $\mu_4(L)$ must be 1. Therefore, L is of the form $\langle 1, -\delta \rangle \perp N$ where N is a binary lattice with $\mu_1(N) = \mu_2(N) = 1$. In particular, $\deg(d(L)) = 2$, and for any $M \in \text{gen}(L)$, $\mu_1(M) = \mu_2(M) = 0$ and $\mu_3(M) = \mu_4(M) = 1$. As a result, the class number of L is the same as that of N, which is 1 by Lemma 3.7. So, L is regular and thus universal because $Q(\text{gen}(L)) = \mathbf{A}$. $\qquad\square$

Corollary 4.2. *Every universal lattice has class number 1.*

Proof. This is clear from the proof of the last theorem. $\qquad\square$

We give yet another characterization of universal lattices which could be useful in practice.

Corollary 4.3. *A lattice L is universal if and only if L is quaternary and the degree of $d(L)$ is exactly 2. Consequently, there are only finitely many isometry classes of universal lattices.*

Proof. The "only if" part of the first statement is clear. Now, suppose that L is a quaternary lattice with $\deg(d(L)) = 2$. Then $\mu_1(L) = \mu_2(L) = 0$ and $\mu_3(L) = \mu_4(L) = 1$. Therefore,

$$L \cong \langle 1, -\delta \rangle \perp \begin{bmatrix} T + a & c \\ c & -\delta T + b \end{bmatrix},$$

where $a, b, c \in \mathbb{F}_q$. Since $\langle 1, -\delta \rangle$ represents all elements in $\mathbb{F}_q$, L represents $1, \delta, T$ and δT, which means that L is universal by Theorem 4.1. $\qquad\square$

We now turn our attention to regular quaternary lattices.

Lemma 4.4. *Let L be a regular quaternary lattice. Suppose that $\mathfrak{p}$ is a finite place for which the unimodular Jordan component of $L_\mathfrak{p}$ is not isotropic. Then there exists a regular lattice L' such that either the unimodular Jordan component of $L'_\mathfrak{p}$ is isotropic or $L'_\mathfrak{p}$ is the unique anisotropic $\mathbf{A}_\mathfrak{p}$-maximal lattice, and for each $\mathfrak{q} \neq \mathfrak{p}$ $L'_\mathfrak{q}$ is isometric to $L^\epsilon_\mathfrak{q}$ for some $\epsilon \in \mathbf{A}^\times_\mathfrak{q}$.*

Proof. It suffices to prove that we can obtain L' from L by means of a finite number of $\lambda_\mathfrak{p}$-transformations. Suppose that $L_\mathfrak{p} = J_0 \perp J_1$ where J_0 is unimodular and $\mathfrak{s}(J_1) \subseteq \mathfrak{p}$. We may assume that J_0 is anisotropic. Let $\pi \in \mathbf{A}$ be the monic generator of $\mathfrak{p}$. Then

$$\lambda_p(L)_\mathfrak{p} \cong \begin{cases} J_0 \perp J_1^{1/\pi^2} & \text{if } \mathfrak{s}(J_1) \subseteq \mathfrak{p}^2, \\ J_1^{1/\pi} \perp J_0^\pi & \text{if } \mathfrak{s}(J_1) = \mathfrak{p}. \end{cases}$$

By applying the $\lambda_\mathfrak{p}$-transformation successively, we obtain a lattice L' with the desired properties. $\qquad\square$

Corollary 4.5. *Let L be a quaternary regular lattice. There exists a universal lattice $\tilde{L}$ with $d(\tilde{L}) \mid d(L)$.*

Proof. Let P be the set of finite places $\mathfrak{p}$ for which the unimodular Jordan component of $L_{\mathfrak{p}}$ is not isotropic. It is clear that P is a finite set. Now apply Lemma 4.4 at every place in P, and let $\tilde{L}$ be the resulting lattice. Since $\tilde{L}$ is regular and $\tilde{L}_{\mathfrak{p}}$ is universal for every place $\mathfrak{p}$ (including the infinite place), $\tilde{L}$ is a universal lattice. $\square$

Proposition 4.6. *If π is a prime which divides the discriminant of a regular quaternary lattice, then $\deg(\pi) \leq 2$.*

Proof. Let L be a regular quaternary lattice, and let $\tilde{L}$ be the universal lattice obtained from Corollary 4.5. If $\pi \mid d(\tilde{L})$, then $\deg(\pi) \leq 2$. Let π be a prime which divides $d(L)$ but not $d(\tilde{L})$, and $\mathfrak{p}$ be the place generated by π. Then $L_{\mathfrak{p}}$ is of the form

$$L_{\mathfrak{p}} = M_{\mathfrak{p}} \perp N_{\mathfrak{p}}$$

where $M_{\mathfrak{p}}$ is unimodular of rank ≤ 2, and $\mathfrak{s}(N_{\mathfrak{p}}) \subseteq \mathfrak{p}^2$. We may assume that $\deg(\pi) := \ell > 2$ and $L_{\mathfrak{q}}$ is universal for all $\mathfrak{q} \neq \mathfrak{p}$.

If $M_{\mathfrak{p}}$ is binary, then L represents all nonzero polynomials in $\mathbf{A}$ of degree $\leq \ell - 1$. Since ℓ is assumed to be at least 3, therefore L represents $1, \delta, T$ and δT. But then L is universal and $\ell \leq 2$, which is a contradiction.

Suppose that the rank of $M_{\mathfrak{p}}$ is 1. Consider the set

$$S = \{f \in \mathbf{A} : f \neq 0, \deg(f) \leq \ell - 1, f \longrightarrow L_{\mathfrak{p}}\}.$$

It is clear that $|S| = (q^{\ell} - 1)/2$. Let J be the sublattice spanned by all $v \in L$ with $Q(v) \in S$. If $\operatorname{rank}(J) = k \geq 2$, then $2(k-1)\ell \leq \deg(d(J)) \leq k(\ell - 1)$, which is not possible for any $\ell \geq 3$. Therefore, $k = 1$ and every element in S is a square multiple of a particular element g in S. If $\deg(g) = d$, the number of nonzero square multiples of g in S is at most $(q^{\frac{\ell - d + 1}{2}} - 1)/2$, which is less than $|S|$. This is a contradiction and hence $\ell \leq 2$. $\square$

Theorem 4.7. *There are only finitely many isometry classes of regular primitive quaternary lattices.*

Proof. Following the argument in the proof of Theorem 3.12, one can show that the first three successive minima of a regular quaternary lattice L are bounded by an absolute constant. Therefore, up to isometry there are only finitely many possible 3×3 sections of L, and the discriminants of all these 3×3 sections have degrees less than some constant γ. Let M be a ternary lattice with $\deg(d(M)) < \gamma$, and let Ω_M be the set of finite places $\mathfrak{p}$ for which $M_{\mathfrak{p}}$ is not unimodular. For each $\mathfrak{p} \in \Omega_M$, let $f_{\mathfrak{p}} \in \mathbf{A}$ be the prime generating $\mathfrak{p}$ and let $\mathfrak{s}(M_{\mathfrak{p}}) = \mathfrak{p}^{n_{\mathfrak{p}}}$. Set

$$F = \prod_{\mathfrak{p} \in \Omega_M} f_{\mathfrak{p}}^{n_{\mathfrak{p}}},$$

and for each $\mathfrak{p} \in \Omega_M$ select $\eta_{\mathfrak{p}} \in \mathbf{A}_{\mathfrak{p}}^{\times}$ such that $\eta_{\mathfrak{p}} F \longrightarrow M_{\mathfrak{p}}$. Since M_{∞} is an anisotropic ternary space over $\mathbf{K}_{\infty}$, it does not represent a polynomial of the form ϵT^s where $\epsilon \in \mathbb{F}_q^{\times}$ and $s \in \{0, 1\}$. By the strong form of Dirichlet's Theorem [16, Theorem 4.8], there exists a prime $g \in \mathbf{A}$ such that

$$\deg(F) + \deg(g) \equiv s \bmod 2$$

and

$$g \equiv \epsilon \eta_{\mathfrak{p}} \bmod \mathfrak{p} \text{ for all } \mathfrak{p} \in \Omega_M.$$

If M is a 3×3 section of a regular quaternary lattice L, then $\epsilon g F$ is not represented by M_∞. But $\epsilon g F$ is represented by L. The degree of $\epsilon g F$ depends only on M. If we let D be the maximum of all these degrees, then D is independent of L and $\mu_4(L) \leq D$. $\qquad \square$

As is pointed out in the introduction, the $\mathbb{Z}$-analog of the above theorem is not true. Indeed there are infinitely many isometry classes of positive definite regular primitive quaternary $\mathbb{Z}$-lattices, see for example [7].

References

[1] W. K. Chan and A. G. Earnest, *Discriminant bounds for spinor regular ternary quadratic lattices*, J. London Math. Soc. (2) **69** (2004), 545-561. MR2048511 (2005b:11042)

[2] W. K. Chan, A. G. Earnest and B.-K. Oh, *Regularity properties of positive definite integral quadratic forms*, Contemporary Math. Amer. Math. Soc., **344** (2004), 59-71. MR2058667 (2005c:11043)

[3] W. K. Chan and B.-K. Oh, *Finiteness theorems for positive definite n-regular quadratic forms*, Trans. Amer. Math. Soc., **355** (2003), 2385-2396. MR1973994 (2004i:11032)

[4] W. K. Chan and B.-K. Oh, *Positive ternary quadratic forms with finitely many exceptions*, Proc. Amer. Math. Soc., **132** (2004), 1567-1573. MR2051115 (2005a:11044)

[5] L. E. Dickson, *Ternary quadratic forms and congruences*, Ann. of Math. **28** (1927), 333-341. MR1502786

[6] D. Z. Djoković, *Hermitian matrices over polynomial rings*, J. Algebra **43** (1976), 359-374. MR0437565 (55:10489)

[7] A. G. Earnest, *An application of character sum inequalities to quadratic forms*, Number Theory, Canadian Math. Soc. Conference Proceedings **15** (1995), 155-158. MR1353928 (96j:11044)

[8] M. Fried and M. Jarden, *Field Arithmetic*, Springer Verlag, New York, 1986. MR0868860 (89b:12010)

[9] L. Gerstein, *Definite quadratic forms over $\mathbb{F}_q[x]$*, J. Algebra, **268** (2003), 252-263. MR2005286 (2004f:11032)

[10] L. Gerstein, *On representation by quadratic $\mathbb{F}_q[x]$-lattices*, Contemporary Math. Amer. Math. Soc., **344** (2004), 129-134. MR2058672

[11] W. Jagy, I. Kaplansky and A. Schiemann, *There are 913 regular ternary forms*, Mathematika, **44** (1997), 332-341. MR1600553 (99a:11046)

[12] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge University Press, Cambridge, 1999. MR1245266 (95c:11044)

[13] U. Korte, *Class numbers of definite binary quadratic lattices over algebraic function fields*, J. Number Theory **19** (1984), 33-39. MR0751162 (85m:11023)

[14] M. H. Kim, Y. Wang and F. Xu, *Universal quadratic forms over $\mathbb{F}_q[x]$*, preprint.

[15] O. T. O'Meara, *Introduction to quadratic forms*, Springer Verlag, New York, 1963. MR0152507 (27:2485)

[16] M. Rosen, *Number theory in function fields*, Springer Verlag, New York, 2001. MR1876657 (2003d:11171)

[17] G. L. Watson, *Some problems in the theory of numbers*, Ph.D. thesis, University College, London (1953).

[18] G. L. Watson, *The representation of integers by positive ternary quadratic forms*, Mathematika **1** (1954), 104-110. MR0067162 (16:680c)

Department of Mathematics, Wesleyan University, Middletown, Connecticut 06459
E-mail address: wkchan@wesleyan.edu

Department of Mathematics, Wesleyan University, Middletown, Connecticut 06459
E-mail address: jdaniels@wesleyan.edu
Current address: 2920 Deakin Street #1, Berkeley, California 94705