MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

A NORMAL FORM FOR DEFINITE QUADRATIC FORMS OVER $\mathbb{F}_q[t]$

MARKUS KIRSCHMER

Abstract. An efficient algorithm to compute automorphism groups and isometries of definite $\mathbb{F}_q[t]$-lattices for odd q is presented. The algorithm requires several square root computations in $\mathbb{F}_{q^2}$ but no enumeration of orbits having more than eight elements.

1. Introduction

In [7], H. Minkowski introduced his notion of reduced definite quadratic forms over the integers. He forces the basis vectors of the corresponding $\mathbb{Z}$-lattice to be "as short as possible". It is known that every definite $\mathbb{Z}$-lattice of rank at most four has some basis such that the basis vectors achieve Minkowski's successive minima of the lattice.

Definite $\mathbb{Z}$-lattices can have arbitrary rank and the Gram matrix of Minkowski reduced bases is in general not unique. Therefore W. Plesken and B. Souvignier proposed a sophisticated backtrack search to compute isometries of two definite $\mathbb{Z}$-lattices (see [8]).

Over the polynomial ring $\mathbb{F}_q[t]$ where q denotes some power of an odd prime, the situation is much better. Let $\mathbb{F}_q(t)$ be the field of fractions of $\mathbb{F}_q[t]$ and let $\mathbb{F}_q(t)_{(1/t)}$ be the completion of $\mathbb{F}_q(t)$ at the "infinite" place $(1/t)$. A quadratic form Q on some finite dimensional $\mathbb{F}_q(t)$-space V is called *definite* if the extended form $Q_{(1/t)}\colon V\otimes\mathbb{F}_q(t)_{(1/t)} \to \mathbb{F}_q(t)_{(1/t)}$ is anisotropic. Each completion of $\mathbb{F}_q(t)$ is a local field and the residue class fields are a finite extensions of $\mathbb{F}_q$. Hence it follows from the Hasse-Minkowski principle that the rank of any anisotropic quadratic form over $\mathbb{F}_q(t)$ is at most four.

Let Q be a definite quadratic form on a finite dimensional $\mathbb{F}_q(t)$-space V. In [2] D. Djoković defined the notion of reduced bases of a $\mathbb{F}_q[t]$-lattice L in a quadratic $\mathbb{F}_q(t)$-space (V, Q). L. Gerstein showed in [3] that the vectors of a reduced basis also achieve the successive minima of L (see Definition 2.3) and the number of reduced bases is finite.

Therefore the construction of isometries and the computation of automorphism groups of lattices is a finite problem. However, there are lattices of rank 4 which have up to $|\mathrm{GL}_2(\mathbb{F}_q)|^2$ reduced bases but only two automorphisms. So orbit enumeration is not feasible.

Received by the editor March 28, 2011.
2000 *Mathematics Subject Classification.* 11E12.

©XXXX American Mathematical Society

Thus the goal of the paper is to define a distinguished Gram matrix (called *normal Gram matrix* in the sequel) for each isometry class of lattices in V. It will depend on some user choices (like to fix a nonsquare in $\mathbb{F}_q^*$) and it is clearly not the only way of defining distinguished Gram matrices. However, the normal Gram matrices presented in this paper can be computed from any reduced Gram matrix quite efficiently and they allow an easy construction of isometries and automorphism groups of lattices in V. The algorithms are already available in MAGMA version 2.17 ([1]) as DominantDiagonalForm, IsIsometric and AutomorphismGroup. These algorithms are also used in the computation of representatives of ideal classes of Eichler orders in definite quaternion algebras over $\mathbb{F}_q(t)$ (see [4] for details).

The paper is organized as follows. Section 2 recalls Gerstein's reduction theory for definite quadratic forms over $\mathbb{F}_q(t)$ and states the main result of the article. Section 3 might be of independent interest. It discusses the orbits (of some subgroups) of $\mathrm{GO}_2^-(\mathbb{F}_q)$ on $\mathbb{F}_q^{2\times 1}$ and $\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$ on $\mathbb{F}_q^{2\times 2}$. Here $\mathrm{GO}_2^-(\mathbb{F}_q)$ denotes the orthogonal group of some anisotropic binary quadratic form over $\mathbb{F}_q$. In particular, systems of representatives and their stabilizers are worked out. Section 4 defines the normal Gram matrix and Section 5 gives algorithms that can be used to obtain the normal Gram matrix of a given lattice in some definite $\mathbb{F}_q(t)$-space. The last section gives alternative representatives of the actions of $\mathrm{GO}_2^-(\mathbb{F}_q)$ and $\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$ in the case that -1 is a square in $\mathbb{F}_q^*$ which require less choices to be made.

2. Preliminaries

Since q is assumed to be odd, the concept of quadratic and bilinear forms are essentially equivalent. To be able to work with Gram matrices, bilinear forms will be preferred in this paper.

As above let V be a finite dimensional $\mathbb{F}_q(t)$-space equipped with a definite bilinear form f (i.e. the corresponding quadratic form $Q_f \colon V \to \mathbb{F}_q(t),\ v \mapsto f(v,v)$ is definite). A lattice L in V is a free $\mathbb{F}_q[t]$-submodule of V of full rank. The lattice L is *integral* if $f(x,y) \in \mathbb{F}_q[t]$ for all $x, y \in L$. If $B = (B_1, \ldots, B_n)$ is some $\mathbb{F}_q[t]$-basis of L then $\mathcal{G}(B) = (f(B_i, B_j))_{i,j} \in \mathbb{F}_q(t)^{n\times n}$ is the *Gram matrix* of B. Given a matrix $T = (T_{i,j}) \in \mathrm{GL}_n(\mathbb{F}_q[t])$, then $T \cdot B$ denotes the basis $(\sum_i T_{1,i}B_i, \ldots, \sum_i T_{n,i}B_i)$ of L. Then $\mathcal{G}(T \cdot B) = T\mathcal{G}(B)T^{\mathrm{tr}}$ where T^{tr} denotes the transpose of T.

Two lattices L, L' are called *isometric* if there exists some *isometry* φ in

$$O(V) = \{\psi \in \mathrm{End}_{\mathbb{F}_q(t)}(V) \mid Q_f(\psi(v)) = Q_f(v) \text{ for all } v \in V\}$$

such that $\varphi(L) = L'$. The group $O(L) := \{\varphi \in O(V) \mid \varphi(L) = L\}$ of isometries from L to L itself is called the *automorphism group* of L.

The lattices L and L' are isometric if and only if there exists bases B, B' of L, L' such that $\mathcal{G}(B) = \mathcal{G}(B')$. Further, if B and B' are bases of two isometric lattices then the monic greatest common divisor of the denominators of the entries of $\mathcal{G}(B)$ and $\mathcal{G}(B')$ must be equal. Hence for the computation of isometries and automorphism groups, one can always assume that the lattices one has to deal with are integral (if not, simply rescale the bilinear form f). Thus all lattices in this paper are assumed to be integral.

Given $d_i \in \mathrm{GL}_{n_i}(\mathbb{F}_q)$ for $1 \le i \le r$ then $\mathrm{Diag}(d_1, \ldots, d_r)$ denotes the block diagonal matrix with blocks d_1 up to d_r on the diagonal and 0 blocks elsewhere.

Similarly, given subgroups H_i of $\mathrm{GL}_{n_i}(\mathbb{F}_q)$ for $1 \le i \le r$ then $\mathrm{Diag}(H_1, \ldots, H_r)$ denotes the matrix group $\{\mathrm{Diag}(h_1, \ldots, h_r) \mid h_i \in H_i\}$.

The algorithms for computing isometries and automorphism groups are based on the following reduction theory developed by D. Djoković and L. Gerstein in [2, 3].

Definition 2.1. A symmetric matrix $A = (A_{i,j}) \in \mathbb{F}_q[t]^{n\times n}$ is said to have *dominant diagonal* if

- $\deg A_{i,i} > \deg A_{i,j}$ whenever $i \neq j$
- $\deg A_{i,i} \le \deg A_{i+1,i+1}$ for all $1 \le i < n$.

Given a lattice L in V, there exists an algorithm (see [2, 3]) that constructs a basis B of L such that its Gram matrix $\mathcal{G}(B)$ has dominant diagonal. Such a basis B will be called *reduced* (with respect to the form f). Moreover, Gerstein showed that

Theorem 2.2 (Gerstein [3])**.** *Let V be a n-dimensional $\mathbb{F}_q(t)$-space equipped with a definite bilinear form f. Suppose $B = (B_1, \ldots, B_n)$ is a reduced basis of an integral lattice L in V and let $\mathcal{G}(B) = (A_{i,j})$ denote its Gram matrix. Further let $\{\deg A_{i,i} \mid 1 \le i \le n\} = \{m_1, \ldots, m_r\}$ with $m_1 < m_2 < \cdots < m_r$. Then*

(1) *If $v \in L$ and $1 \le \ell \le n$ such that $(B_1, \ldots, B_{\ell-1}, v)$ is linearly independent then $\deg f(v,v) \ge \deg A_{\ell,\ell}$. In particular,*
$$\min\{\deg f(v,v) \mid v \in L,\ v \neq 0\} = m_1 = \deg A_{1,1}\ .$$
(2) *$n_i := |\{j \in \{1, \ldots, n\} \mid \deg A_{j,j} = m_i\}| \le 2$ for all i.*
(3) *The set of all reduced bases of L is given by*
$$\{\mathrm{Diag}(d_1, \ldots, d_r) \cdot B \mid d_i \in \mathrm{GL}_{n_i}(\mathbb{F}_q)\}\ .$$

Definition 2.3. The numbers $m_1, m_2, \ldots, m_r$ in Theorem 2.2 are called the *successive minima* of L.

Theorem 2.2 shows that testing whether two lattices L, L' in V are isometric is essentially a finite problem. If B is a reduced basis of L then an enumeration of the orbit $\{T\mathcal{G}(B)T^{\mathrm{tr}} \mid T \in \mathrm{Diag}(\mathrm{GL}_{n_1}(\mathbb{F}_q), \ldots, \mathrm{GL}_{n_r}(\mathbb{F}_q))\}$ will eventually find a suitable transformation as well as the stabilizer $\mathrm{Stab}_{O(V)}(L) = O(L)$ of L. But such an approach would be quite inefficient since for example if $n_1 = n_2 = 2$ then there exist lattices L such that $O(L) \cong C_2$. In this case the above orbit has the size $\frac{1}{2}|\mathrm{GL}_2(\mathbb{F}_q)|^2$ and therefore cannot be enumerated if q is large.

Thus a distinguished Gram matrix of L will be developed in the sequel (see Definition 4.3). It will be called the *normal Gram matrix* of L. It will depend on a few user choices like fixing some nonsquare $\varepsilon \in \mathbb{F}_q^*$ for example (see Section 3 for details). But besides these choices, it will be a separating invariant of the isometry class of L. I.e. two lattices L, L' are isometric if and only if they have the same normal Gram matrix. Moreover, the normal Gram matrix of a lattice L can be computed efficiently from any given reduced basis of L without enumerating orbits having more than 8 elements. However the algorithm requires the computation of several square roots in $\mathbb{F}_{q^2}$. More precisely it is shown that

Theorem 2.4. *Let V be a n-dimensional vector space over $\mathbb{F}_q(t)$ equipped with a definite bilinear form f and let L be an integral lattice in V. Given the Gram matrix $\mathcal{G}(B)$ of some reduced basis of L, there exists an algorithm which computes the base change from B to some basis B' of L such that $\mathcal{G}(B')$ is the normal Gram*

matrix of L as well as $O(L)$ as a matrix group with respect to B' using no more than s_n square root computations and $O(d)$ elementary operations where d is the largest successive minimum of L and

$$s_n = \begin{cases} 2 & \text{if } n = 1 \\ 8 & \text{if } n = 2 \\ 10 & \text{if } n = 3 \\ 25 & \text{if } n = 4 \end{cases}.$$

Elementary operations mean comparison, addition, multiplication or division of elements in $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$. For example given two polynomials $f, g \in \mathbb{F}_q[t]$ of degree d and $a \in \mathbb{F}_q$ it already takes $O(d)$ elementary operations to evaluate $f + ag$.

Remark 2.5. Finally note that before one can apply the algorithm claimed in Theorem 2.4, one has to obtain some reduced basis B of L first. Section 1 of [3] gives an algorithm that given any basis C of L and $\mathcal{G}(C)$ computes some $T \in \mathrm{GL}_n(\mathbb{F}_q[t])$ such that $T \cdot C$ is a reduced basis of L. In the worst case, the algorithm requires $O(c^2)$ elementary operations where c denotes the largest degree of any entry in $\mathcal{G}(C)$. Hence Theorem 2.4 shows that computing the initial reduced basis is usually the hard part.

3. Distinguished representatives of orbits

Already the classification of the regular quadratic or bilinear forms over $\mathbb{F}_q$ requires that one distinguishes some nonsquare in $\mathbb{F}_q^*$. Similarly, the classification of the definite quadratic or bilinear forms over $\mathbb{F}_q[t]$ will depend on the following three (rather unmotivated) choices:

(1) Some generator α of the multiplicative group $\mathbb{F}_{q^2}^*$.
(2) Some nonsquare $\varepsilon \in \mathbb{F}_q^*$.
(3) A total order $<$ on the set of elements of $\mathbb{F}_{q^2}$.

Remark 3.1.

(1) Let $\mathrm{Nr}\colon \mathbb{F}_{q^2} \to \mathbb{F}_q, x \mapsto x^{q+1}$ be the usual norm of the field extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. Then $\mathrm{Nr}(\alpha)$ can be chosen as a nonsquare $\varepsilon \in \mathbb{F}_q^*$.
(2) Let p be the characteristic of $\mathbb{F}_q$. If the Conway polynomial $c(x) \in \mathbb{F}_p[x]$ for $\mathbb{F}_{q^2}$ is known (see [6]), then the above choices can be made in a unique and consistent way. The residue class $\overline{x} := x + c(x)\mathbb{F}_q[x]$ of x is a canonical primitive element. The elements of $\mathbb{F}_p$ can be ordered as $0 < 1 < \cdots < p-1$ and this order is extended to $\mathbb{F}_p[x]$ using the lexicographic order. This yields a total order $<$ on $\mathbb{F}_{q^2} = \mathbb{F}_p[x]/c(x)\mathbb{F}_q[x]$.

Once α, ε and $<$ are chosen, let $\mathfrak{i} \in \mathbb{F}_{q^2}$ such that $\mathfrak{i}^2 = \varepsilon^{-1}$ and $\mathfrak{i} < -\mathfrak{i}$. Then $(1, \mathfrak{i})$ is a $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$ and the corresponding regular representation is

$$\mathfrak{R}\colon \mathbb{F}_{q^2} \to \mathbb{F}_q^{2\times 2},\ x + y\mathfrak{i} \mapsto \begin{pmatrix} x & y/\varepsilon \\ y & x \end{pmatrix}.$$

The element $\beta := \alpha^{q-1}$ generates the norm one subgroup of $\mathbb{F}_{q^2}^*$ and its regular representation $\mathfrak{R}(\beta)$ will be denoted by s in the sequel.

The bilinear form on $\mathbb{F}_q^2$ given by the Gram matrix $F_\varepsilon := \mathrm{Diag}(1, -\varepsilon)$ is up to isometry the unique anisotropic binary form over $\mathbb{F}_q$ (see for example [5, (12.1)]).

Its (special) orthogonal group is given by

$$\mathrm{SO}_2^-(\mathbb{F}_q) := \left\{X \in \mathrm{SL}_2(\mathbb{F}_q) \mid XF_\varepsilon X^{\mathrm{tr}} = F_\varepsilon\right\} = \langle s\rangle$$
$$\mathrm{GO}_2^-(\mathbb{F}_q) := \left\{X \in \mathrm{GL}_2(\mathbb{F}_q) \mid XF_\varepsilon X^{\mathrm{tr}} = F_\varepsilon\right\} = \langle s,\ \mathrm{Diag}(1,-1)\rangle\ .$$

Finally let $\mathbb{F}_{q,<}^* := \{x \in \mathbb{F}_q^* \mid x < -x\}$.

3.1. **The action of $\mathrm{GO}_2^-(\mathbb{F}_q)$ on $\mathbb{F}_q^{2\times 1}$.**

The group $\mathrm{GO}_2^-(\mathbb{F}_q)$ acts on $\mathbb{F}_q^{2\times 1}$ by left multiplication. From

$$\mathrm{SO}_2^-(\mathbb{F}_q) = \{\mathfrak{R}(u) \mid u \in \mathbb{F}_{q^2} \text{ and } \mathrm{Nr}(u) = 1\}$$

it follows that for all $a, b \in \mathbb{F}_q$ and $u \in \mathbb{F}_{q^2}$ with $\mathrm{Nr}(u) = 1$ one has

$$\mathfrak{R}(u) \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \tag{3.1}$$

where $x + \mathfrak{i}y = u \cdot (a + \mathfrak{i}b)$. In particular, $\mathrm{Nr}(a + \mathfrak{i}b) = \mathrm{Nr}(x + \mathfrak{i}y)$. Thus the norm is an invariant of the $\mathrm{SO}_2^-(\mathbb{F}_q)$-orbits. More precisely

Proposition 3.2. *$\mathbb{F}_q^{2\times 1}$ decomposes into q orbits under $\mathrm{SO}_2^-(\mathbb{F}_q)$. These are represented by*

$$\left\{\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \in \mathbb{F}_q^{2\times 1} \mid a + \mathfrak{i}b \in T\right\}$$

where $T = \{0\} \cup \{c\alpha^m \mid c \in \mathbb{F}_{q,<}^* \text{ and } m \in \{0,1\}\}$.

Proof. All elements in T have different norms. Hence the proposed representatives must lie in different $\mathrm{SO}_2^-(\mathbb{F}_q)$-orbits. The following algorithm shows that each $\mathrm{SO}_2^-(\mathbb{F}_q)$-orbit contains at least one of the claimed representatives. □

The computation of a group element $g \in \mathrm{SO}_2^-(\mathbb{F}_q)$ sending some given $v \in \mathbb{F}_q^{2\times 1}$ to one of the representatives from Proposition 3.2 is straight forward.

Algorithm 3.3.

Input: *Some $v \in \mathbb{F}_q^{2\times 1}$.*

Output: *Some $g \in \mathrm{SO}_2^-(\mathbb{F}_q)$ such that gv is one of the representatives from Proposition 3.2.*

1 **if** $v = 0$ **then return** I_2.

2 *Write $v_1^2 - v_2^2/\varepsilon = c^2\mathrm{Nr}(\alpha)^m$ with $m \in \{0,1\}$ and $c \in \mathbb{F}_{q,<}^*$.*

3 **return** $\mathfrak{R}(c\alpha^m/(v_1 + \mathfrak{i}v_2))$.

Proof. The element $c\alpha^m/(v_1 + \mathfrak{i}v_2)$ has norm 1. Hence it is contained in $\langle\beta\rangle$ and its regular representation acts like explained in equation 3.1. □

Note that to get c and m in line 2 above, the algorithm has to compute two square roots in the worst case.

Remark 3.4. Let $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ be some nonzero representative from Proposition 3.2. Then $a + \mathfrak{i}b = c\alpha^m$ for some $c \in \mathbb{F}_q^*$ and $m \in \{0,1\}$. Moreover $D := \mathrm{Diag}(1,-1)$ satisfies $D \cdot \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} a \\ -b \end{smallmatrix}\right)$ i.e. the action of D on $\mathbb{F}_q^2$ corresponds to the Frobenius map on $\mathbb{F}_{q^2}$. Hence the identity $(\beta^m \cdot (c\alpha^m))^q = c((\alpha\beta)^q)^m = c(\alpha^q)^{qm} = c\alpha^m$ shows that

$$\mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \langle Ds^m\rangle \cong C_2\ .$$

So Proposition 3.2 also describes a system of representatives of the $\mathrm{GO}_2^-(\mathbb{F}_q)$-orbits.

3.2. **The action of $\mathrm{GO}_2^-(\mathbb{F}_q)$ on $\mathbb{F}_q^{2\times 2}$.**

The group $\mathrm{GO}_2^-(\mathbb{F}_q)$ acts on $\mathbb{F}_q^{2\times 2}$ by $\mathrm{GO}_2^-(\mathbb{F}_q)\times\mathbb{F}_q^{2\times 2}\to\mathbb{F}_q^{2\times 2}$, $(g,M)\mapsto gMg^{\mathrm{tr}}$. Just as before, it is more convenient to enumerate the $\mathrm{SO}_2^-(\mathbb{F}_q)$-orbits first.

Since $\mathrm{SO}_2^-(\mathbb{F}_q)=\langle s\rangle$ is cyclic and s acts linearly on $\mathbb{F}_q^{2\times 2}$, it is natural to decompose the space $\mathbb{F}_q^{2\times 2}$ into s-invariant subspaces. The eigenspaces of the $\mathbb{F}_{q^2}$-linear endomorphism $\mathbb{F}_{q^2}^{2\times 2}\to\mathbb{F}_{q^2}^{2\times 2}$, $M\mapsto sMs^{\mathrm{tr}}$ are

$$\left\langle F_\varepsilon,\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right\rangle_{\mathbb{F}_{q^2}},\quad \left\langle\begin{pmatrix}1&\mathrm{i}^{-1}\\ \mathrm{i}^{-1}&\varepsilon\end{pmatrix}\right\rangle_{\mathbb{F}_{q^2}},\quad \left\langle\begin{pmatrix}1&-\mathrm{i}^{-1}\\ -\mathrm{i}^{-1}&\varepsilon\end{pmatrix}\right\rangle_{\mathbb{F}_{q^2}}$$

with corresponding eigenvalues 1, β^2 and $\beta^{2q}=\beta^{-2}$ respectively. Hence the map

$$\begin{aligned}\varphi\colon \mathbb{F}_q^2\times\mathbb{F}_{q^2}&\to\mathbb{F}_q^{2\times 2},\\ (a,b,\lambda)&\mapsto aF_\varepsilon+\begin{pmatrix}0&-b\\b&0\end{pmatrix}+\frac{\lambda}{2}\begin{pmatrix}1&\mathrm{i}^{-1}\\ \mathrm{i}^{-1}&\varepsilon\end{pmatrix}+\frac{\lambda^q}{2}\begin{pmatrix}1&-\mathrm{i}^{-1}\\ -\mathrm{i}^{-1}&\varepsilon\end{pmatrix}\end{aligned}$$

is an isomorphism of $\mathbb{F}_q$-spaces. Its inverse is given by

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\mapsto\left(\frac{a}{2}-\frac{d}{2\varepsilon},\ \frac{c-b}{2},\ \frac{a}{2}+\frac{d}{2\varepsilon}+\mathrm{i}\frac{b+c}{2}\right)$$

and φ satisfies $s\varphi(a,b,\lambda)s^{\mathrm{tr}}=\varphi(a,b,\beta^2\lambda)$ for all $a,b\in\mathbb{F}_q$ and $\lambda\in\mathbb{F}_{q^2}$. Thus φ allows an easy description of the $\mathrm{SO}_2^-(\mathbb{F}_q)$-orbits of $\mathbb{F}_q^{2\times 2}$.

Proposition 3.5. *There are $q^2(2q-1)$ orbits of $\mathbb{F}_q^{2\times 2}$ under $\mathrm{SO}_2^-(\mathbb{F}_q)$. They are represented by*

representative	*stabilizer*	*orbit length*	*#orbits*
$\varphi(a,b,0)$	$\mathrm{SO}_2^-(\mathbb{F}_q)$	1	q^2
$\varphi(a,b,c\alpha^m\beta^n)$	$\langle -I_2\rangle$	$\frac{q+1}{2}$	$2q^2(q-1)$

where $a,b\in\mathbb{F}_q$, $c\in\mathbb{F}_{q,<}^*$ and $m,n\in\{0,1\}$.

Proof. The elements $\{c\alpha^m \mid c\in\mathbb{F}_{q,<}^*$ and $m\in\{0,1\}\}$ have different norms. Further, β generates the norm 1 subgroup of $\mathbb{F}_{q^2}^*$ and $\langle\beta\rangle/\langle\beta^2\rangle\cong C_2$. Hence the elements $\{0\}\cup\{c\alpha^m\beta^n \mid c\in\mathbb{F}_{q,<}^*$ and $n,m\in\{0,1\}\}$ lie in different orbits under $\langle\beta^2\rangle$. Thus the proposed representatives lie in different $\mathrm{SO}_2^-(\mathbb{F}_q)$-orbits. The following algorithm shows that each orbit has at least one representative of the above form. □

To find the matrix $g\in\mathrm{SO}_2^-(\mathbb{F}_q)$ such that gMg^{tr} is one of the representatives from Proposition 3.5 one can use the following algorithm.

Algorithm 3.6.

Input: *Some matrix $M\in\mathbb{F}_q^{2\times 2}$.*

Output: *Some $g\in\mathrm{SO}_2^-(\mathbb{F}_q)$ such that gMg^{tr} is one of the representatives from Proposition 3.5.*

1 *Let $(a,b,\lambda)=\varphi^{-1}(M)$.*
2 **if** $\lambda=0$ **then return** I_2.
3 *Write $\mathrm{Nr}(\lambda)=\mathrm{Nr}(\alpha)^m c^2$ with $m\in\{0,1\}$ and $c\in\mathbb{F}_{q,<}^*$.*
4 *Write $\lambda/(c\alpha^m)=\beta^n u^2$ with $n\in\{0,1\}$ and $u\in\mathbb{F}_{q^2}^*$ such that $\mathrm{Nr}(u)=1$.*
5 **return** *the regular representation $\mathfrak{R}(u^{-1})$ of u^{-1}.*

Proof. If $\lambda = 0$ then there is nothing to show. Suppose $\lambda \neq 0$. Then $\mathrm{Nr}(\alpha)$ is not a square. Hence c and m exist and $\lambda/(c\alpha^m)$ has norm 1. Thus $\lambda/(c\alpha^m) \in \langle\beta\rangle$ and therefore u and n exist. Then $\mathfrak{R}(u^{-1})M\mathfrak{R}(u^{-1})^{\mathrm{tr}} = \varphi(a, b, u^{-2}\lambda) = \varphi(a, b, c\alpha^m\beta^n)$. □

Again, to get c and m in line 3 at most two square root computations are needed. The same holds for u and n in line 4. So in total the algorithm might compute up to four square roots.

The matrix $D := \mathrm{Diag}(1, -1)$ satisfies $D\varphi(a, b, \lambda)D^{\mathrm{tr}} = \varphi(a, -b, \lambda^q)$. Hence one immediately obtains the following corollary.

Corollary 3.7. *There are q^3 orbits of $\mathbb{F}_q^{2\times 2}$ under $\mathrm{GO}_2^-(\mathbb{F}_q)$. They are represented by*

representative	*stabilizer*	*orbit length*	*#orbits*
$\varphi(a, 0, 0)$	$\mathrm{GO}_2^-(\mathbb{F}_q)$	1	q
$\varphi(a, b', 0)$	$\mathrm{SO}_2^-(\mathbb{F}_q)$	2	$q\frac{q-1}{2}$
$\varphi(a, 0, c\beta^n)$	$\langle -I_2, s^nD\rangle$	$\frac{q+1}{2}$	$q(q-1)$
$\varphi(a, b', c\beta^n)$	$\langle -I_2\rangle$	$q+1$	$q\frac{(q-1)^2}{2}$
$\varphi(a, b, c\alpha)$	$\langle -I_2\rangle$	$q+1$	$q^2\frac{q-1}{2}$

where $n \in \{0, 1\}$, $a, b \in \mathbb{F}_q$ and $b', c \in \mathbb{F}_{q,<}^*$.

Remark 3.8. Suppose $M \in \mathbb{F}_q^{2\times 2}$ is one of the representatives of the $\mathrm{SO}_2^-(\mathbb{F}_q)$-orbits as given in Proposition 3.5 and let $D = \mathrm{Diag}(1, -1)$. Then precisely one matrix in $\{M, DMD, sDMDs^{\mathrm{tr}}\}$ is a representative of a $\mathrm{GO}_2^-(\mathbb{F}_q)$-orbit as defined in Corollary 3.7. Hence given any $M' \in \mathbb{F}_q^{2\times 2}$, only one call to Algorithm 3.6 is required to find the representative from Corollary 3.7 of the $\mathrm{GO}_2^-(\mathbb{F}_q)$-orbit of M'.

3.3. The action of $\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$ on $\mathbb{F}_q^{2\times 2}$.

The group $\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$ acts on $\mathbb{F}_q^{2\times 2}$ by

$$(\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)) \times \mathbb{F}_q^{2\times 2} \to \mathbb{F}_q^{2\times 2},\ ((g, h), M) \mapsto gMh^{\mathrm{tr}}\,.$$

Proposition 3.9. *Let $D = \mathrm{Diag}(1, -1)$ and $x, y \in \mathbb{F}_q$ such that $\alpha = x + y\mathfrak{i}$. Then the orbits of the action $\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$ on $\mathbb{F}_q^{2\times 2}$ are represented by*

type	*representative*	*stabilizer*	$\lvert orbit\rvert$	*#orbits*
1	$\varphi(0, 0, 0)$	$\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$	1	1
2	$\varphi(a, 0, 0)$	$\langle (s, s),\ (D, D)\rangle$	$2(q+1)$	$\frac{q-1}{2}$
3	$\varphi(ax, ay, 0)$	$\langle (s, s),\ (D, sD)\rangle$	$2(q+1)$	$\frac{q-1}{2}$
4	$\varphi(a, 0, a\beta^n)$	$\langle T, (I_2, s^nD), (s^nD, I_2)\rangle$	$\frac{(q+1)^2}{2}$	$q-1$
5	$\varphi(ax, ay, a\alpha\beta^n)$	$\langle T, (I_2, s^nD), (Ds^{1-n}, I_2)\rangle$	$\frac{(q+1)^2}{2}$	$q-1$
6	$\varphi(a, 0, c\beta^n)$	$\langle T,\ (s^nD, s^nD)\rangle$	$(q+1)^2$	$\frac{(q-1)(q-3)}{4}$
7	$\varphi(ax, ay, c\alpha\beta^n)$	$\langle T, (Ds^{1-n}, s^nD)\rangle$	$(q+1)^2$	$\frac{(q-1)(q-3)}{4}$
8	$\varphi(a, 0, \tilde{c}\alpha)$	$\langle T\rangle$	$2(q+1)^2$	$\frac{(q-1)^2}{4}$

where $n \in \{0, 1\}$, $a, c, \tilde{c} \in \mathbb{F}_{q,<}^*$ such that $a < c$ and $T = (-I_2, -I_2)$.

Proof. Let $M \in \mathbb{F}_q^{2\times 2}$. Then $M = \varphi(a, b, c + d\mathfrak{i})$ for some $a, b, c, d \in \mathbb{F}_q$. One checks that $MD = \varphi(c, d, a + b\mathfrak{i})$ and $sM = \varphi(u, v, \beta(c + d\mathfrak{i}))$ where $u + v\mathfrak{i} = \beta(a + b\mathfrak{i})$. With the description of the action of $\{(g, g) \mid g \in \mathrm{GO}_2^-(\mathbb{F}_q)\}$ on $\mathbb{F}_q^{2\times 2}$ from Corollary 3.7 this shows that $N(M) := \{\mathrm{Nr}(a + b\mathfrak{i}),\ \mathrm{Nr}(c + d\mathfrak{i})\}$ is an invariant of the orbit of M.

Suppose first $0 \in N(M)$. After replacing M by MD if necessary, one may suppose that $c = d = 0$. Applying Algorithm 3.3 to $\binom{a}{b}$ yields some $g \in \mathrm{SO}_2^-(\mathbb{F}_q)$ such that $g\binom{a}{b}$ is one of the representatives from Proposition 3.2. Then gM is one of the representatives of type 1, 2 or 3 from above.
If $N(M) = \{r\}$ for some $r \neq 0$, then Algorithm 3.3 yields some $g \in \mathrm{SO}_2^-(\mathbb{F}_q)$ such that $g\binom{a}{b}$ is one of the representatives from Proposition 3.2. Then $gM = \varphi(a', 0, *)$ or $\varphi(a'x, a'y, *)$ with $a' \in \mathbb{F}_{q,<0}^*$ depending on whether r is a square or not. By Proposition 3.5, there exists some $h \in \mathrm{SO}_2^-(\mathbb{F}_q)$ such that $hgMh^{\mathrm{tr}}$ is a representative of type 4 or 5, again depending on whether r is a square or not.
Suppose now $N(M)$ contains both, a square and a nonsquare. After replacing M by MD one may assume that $\mathrm{Nr}(a+\mathfrak{i}b) = a^2 - b^2/\varepsilon = {a'}^2$ for some $a' \in \mathbb{F}_{q,<}^*$. Again applying Algorithm 3.3 to $\binom{a}{b}$ yields some $g \in \mathrm{SO}_2^-(\mathbb{F}_q)$ such that $gM = \varphi(a', 0, *)$. By Corollary 3.7, there exists some $h \in \mathrm{GO}_2^-(\mathbb{F}_q)$ such that $hgMh^{\mathrm{tr}}$ is of type 8. This leaves the cases where $a^2 - b^2/\varepsilon = {a'}^2\alpha^m$ and $c^2 - d^2/\varepsilon = {c'}^2\alpha^m$ with $m \in \{0, 1\}$ and $a', c' \in \mathbb{F}_{q,<}^*$ such that $a' \neq c'$. After replacing M by MD one may assume that $a' < c'$. Again, if $m = 0$ then Algorithm 3.3 and Corollary 3.7 yield some $g \in \mathrm{SO}_2^-(\mathbb{F}_q)$, $h \in \mathrm{GO}_2^-(\mathbb{F}_q)$ such that $hgMh^{\mathrm{tr}}$ is of type 6. Similarly, if $m = 1$ then $hgMh^{\mathrm{tr}}$ is of type 7 for some $g, h \in \mathrm{SO}_2^-(\mathbb{F}_q)$. Thus each orbit contains at least one element from the list above.
One verifies that the stabilizers of the representatives contain at least the elements given in the table above. Hence the orbits are at most as long as claimed. Now the lengths of the claimed orbits do sum up to q^4. Thus each representative lies in its own orbit and the stabilizers are correct. □

Remark 3.10. Let $0 \neq M \in \mathbb{F}_q^{2\times 2}$. Computing some $g, h \in \mathrm{GO}_2^-(\mathbb{F}_q)$ such that gMh^{tr} is one of the representatives from Proposition 3.9 can be done using no more than 10 square root computations (and a fixed number of elementary operations). If gMh^{tr} is of type 2 or 3 (see Proposition 3.9), then 2 square root computations suffice.

Proof. Suppose the notation of the proof of Proposition 3.9. If $0 \in N(M)$ then only one call to Algorithm 3.3 is needed which takes no more than 2 square root computations. If $N(M) = \{r\}$ then Algorithms 3.3 and 3.6 are called once. This takes at most $6 = 2 + 4$ square root computations. Suppose now $N(M)$ contains two different units. Then one has to test whether $\mathrm{Nr}(a + \mathfrak{i}b)$ and $\mathrm{Nr}(c + \mathfrak{i}d)$ are squares. This takes at most two square root computations. Then one also has to compute a' and maybe c', which may take another two computations (note that the value of the exponent m is already known by now). Finally, the calls to Algorithms 3.3 and 3.6 require another 6 square root computations. So in total, no more than 10 square root computations are needed. □

Remark 3.11. Let $G = \mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$, $D = \mathrm{Diag}(1, -1)$ and $x, y \in \mathbb{F}_q$ such that $x + \mathfrak{i}y = \alpha$. Suppose

$$H_2 = \mathrm{Stab}_G(\varphi(1, 0, 0)) = \{(g, g) \mid g \in \mathrm{GO}_2^-(\mathbb{F}_q)\}$$
$$H_3 = \mathrm{Stab}_G(\varphi(x, y, 0)) = \langle (s, s),\ (D, sD) \rangle$$

denote the stabilizers of the representatives of type 2 and 3 from Proposition 3.9 respectively. Then $\mathfrak{R}(\alpha)\varphi(1, 0, 0) = \varphi(x, y, 0)$. In particular, $h = (\mathfrak{R}(\alpha), I_2) \in G$ satisfies $hH_2h^{-1} = H_3$. Thus the H_3-orbits of $\mathbb{F}_q^{2\times 2}$ are represented by $\mathfrak{R}(\alpha)M$

where M runs through the system of representatives of the $\mathrm{GO}_2^-(\mathbb{F}_q)$-orbits given in Proposition 3.7.

4. The normal Gram matrix

Definition 4.1. For $k \in \mathbb{Z}_{\geq 0}$ and $f \in \mathbb{F}_q[t]$ let $f^{(k)}$ denote the coefficient of t^k in f. Similarly, if $M \in \mathbb{F}_q[t]^{m\times n}$ let $M^{(k)} = (M_{i,j}^{(k)})_{i,j} \in \mathbb{F}_q^{m\times n}$. I.e. $M = \sum_{k\geq 0} M^{(k)} t^k$.

Remark 4.2. Suppose the notation of Theorem 2.2 and set $j_i = 1 + \sum_{k<i} n_k$ for $1 \leq i \leq k$. Then there exists a reduced basis C of L such that the leading coefficients of the diagonal entries of $\mathcal{G}(C) = (G_{i,j})$ satisfy

- $G_{j_i,j_i}^{(m_i)} \in \{1, \varepsilon\}$ whenever $n_i = 1$.
- $(G_{j_i,j_i}^{(m_i)}, G_{j_i+1,j_i+1}^{(m_i)}) = (1, -\varepsilon)$ whenever $n_i = 2$.

Further, the reduced bases of L which satisfy these conditions form an orbit under

$$\mathrm{Diag}(H_1, \ldots, H_r) \text{ where } H_i = \begin{cases} \{\pm 1\} & \text{if } n_i = 1 \\ \mathrm{GO}_2^-(\mathbb{F}_q) & \text{if } n_i = 2 \end{cases}.$$

Proof. The first statement is obvious if $n_i = 1$. If $n_i = 2$ it follows from Theorem 2.2(1) and the fact that F_ε represents the unique isometry class of anisotropic binary quadratic forms over $\mathbb{F}_q$. The second statement follows from Theorem 2.2(3) and the definition of $\mathrm{GO}_2^-(\mathbb{F}_q)$. □

The total order $<$ on $\mathbb{F}_q$ extends in the natural way to $\mathbb{F}_q[t]$ and from there to $\mathbb{F}_q[t]^{1\times n}$ via the lexicographical order. Since $\mathbb{F}_q[t]^{m\times n}$ can be identified with $\mathbb{F}_q[t]^{1\times nm}$ by concatenating rows, this gives rise to a total order on $\mathbb{F}_q[t]^{m\times n}$. This order will also be denoted by $<$ in the sequel.

If S is a subset of $\mathbb{F}_q^{m\times n}$ then $\min S$ will denote the minimum of the set S with respect to the order $<$.

The normal Gram matrices can now be defined explicitly.

Definition 4.3. Let L be an integral lattice in a definite bilinear $\mathbb{F}_q(t)$-space (V, f) of dimension n. Further let $m_1, \ldots, m_r$ be the successive minima of L.

Suppose first $n \in \{2, r\}$. Let $\mathcal{B}$ denote the set of all reduced bases of L that satisfy the conditions of Remark 4.2.

(1) If $n = r$ then $\min\{\mathcal{G}(B) \mid B \in \mathcal{B}\}$ is the *normal Gram matrix* of L.
(2) Suppose $n = 2$ and $r = 1$. In this case pick some $B \in \mathcal{B}$. If $\mathcal{G}(B) \in F_\varepsilon \cdot \mathbb{F}_q[t]$ then $\mathcal{G}(B)$ is the normal Gram matrix of L.
Otherwise let $d = \max\{k \geq 0 \mid \mathcal{G}(B)^{(k)} \notin F_\varepsilon \cdot \mathbb{F}_q\}$ and let M be the representative from Corollary 3.7 of the $\mathrm{GO}_2^-(\mathbb{F}_q)$-orbit of $\mathcal{G}(B)^{(d)}$. Then the normal Gram matrix of L is $\min\{\mathcal{G}(\tilde{B}) \mid \tilde{B} \in \mathcal{B} \text{ and } \mathcal{G}(\tilde{B})^{(d)} = M\}$.

Suppose $n \notin \{2, r\}$. Let $L_i = \langle\{v \in L \mid \deg f(v, v) = m_i\}\rangle$ for $1 \leq i \leq r$. Further let C_i be a basis of L_i such that $\mathcal{G}(C_i)$ is the normal Gram matrix of L_i as defined above and let H_i be the matrix representation of $O(L_i)$ with respect to C_i. The concatenation of $C_1, \ldots, C_r$ yields a basis $B = (B_1, \ldots, B_n)$ of L. Finally let $\mathcal{B} = \{\mathrm{Diag}(h_1, \ldots, h_r) \cdot B \mid h_i \in H_i\}$.

(3) Suppose that for all $1 \leq i \leq r$: $H_i \neq \mathrm{GO}_2^-(\mathbb{F}_q)$ or L_i is perpendicular to every other L_k. Then $\min\{\mathcal{G}(\tilde{B}) \mid \tilde{B} \in \mathcal{B}\}$ is the normal Gram matrix of L.

(4) Suppose (3) does not apply and also suppose that $H_i = \mathrm{GO}_2^-(\mathbb{F}_q)$ for only one $1 \le i \le r$. Let $j \in \{1, \dots, n-1\}$ such that $B_j, B_{j+1} \in L_i$.
For $M \in \mathbb{F}_q^{n\times n}$ let $\psi(M) \in \mathbb{F}_q^{2\times(n-r)}$ denote the matrix obtained from M by removing the columns numbered j or $j+1$ and removing the rows not numbered j or $j+1$. Further let $d = \max\{k \ge 0 \mid \psi(\mathcal{G}(B)^{(k)}) \ne 0\}$ and let $\mathcal{B}'$ denote the set of all $B' \in \mathcal{B}$ such that the first nonzero column of $\psi(\mathcal{G}(B')^{(d)})$ is a representative of Proposition 3.2. Then the normal Gram matrix of L is then given by $\{\mathcal{G}(B') \mid B' \in \mathcal{B}'\}$.

(5) Suppose $H_1 = H_2 = \mathrm{GO}_2^-(\mathbb{F}_q)$ and suppose that L_1 is not perpendicular to L_2. For $M \in \mathbb{F}_q^{4\times4}$ let $\phi(M) \in \mathbb{F}_q^{2\times2}$ denote the upper right 2×2 submatrix of M. Let $d = \max\{k \ge 0 \mid \phi(\mathcal{G}(B)^{(k)}) \ne 0\}$ and

$$\mathcal{B}' = \{B' \in \mathcal{B} \mid \phi(\mathcal{G}(B')^{(d)}) \text{ is a representative of Proposition 3.9}\}.$$

Further let $B' \in \mathcal{B}'$ and let H' denote the stabilizer of $\phi(\mathcal{G}(B')^{(d)})$ in $\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$.

(a) If $|H'| \le 8$ or if $\phi(\mathcal{G}(B')^{(k)})$ is H'-invariant for all $0 \le k < d$ then $\min\{\mathcal{G}(\tilde{B}) \mid \tilde{B} \in \mathcal{B}'\}$ is the normal Gram matrix of L.

(b) Otherwise let $d' = \max\{k \ge 0 \mid \phi(\mathcal{G}(B')^{(k)})$ is not H'-invariant$\}$ and let $\mathcal{B}''$ denote the subset of all bases $B'' \in \mathcal{B}'$ such that $\phi(\mathcal{G}(B'')^{(d')})$ is a representative of some H'-orbit as in Corollary 3.7 or Remark 3.11 (depending on whether $H' = \{(g,g) \mid g \in \mathrm{GO}_2^-(\mathbb{F}_q)\}$ or not). Then $\min\{\mathcal{G}(B'') \mid \tilde{B} \in \mathcal{B}''\}$ is the normal Gram matrix of L.

Remark 4.4. Let L, L' be integral lattices in a finite dimensional definite bilinear $\mathbb{F}_q(t)$-space. Then

(1) The normal Gram matrix of L is well defined.
(2) The lattices L and L' are isometric if and only if they have the same normal Gram matrix.

Proof. Suppose the notation of Definition 4.3. The five cases in Definition 4.3 are mutually exclusive and do not depend on any choices made. In Definition 4.3(2), the bases in $\mathcal{B}$ form an orbit under $\mathrm{GO}_2^-(\mathbb{F}_q)$ and F_ε is $\mathrm{GO}_2^-(\mathbb{F}_q)$-invariant. Hence in this case, the normal Gram matrix of L does not depend on the choice of B. If $n \notin \{2, r\}$ the orbit $\mathcal{B}$ consists of all possible choices for B. So in case (3) the normal Gram matrix of L does not depend on B. For the same reason, the values of j and d in case (4) do not depend on B. So case (4) is well defined. Using similar arguments one sees that case (5) neither depends on B nor B'. This proves the first part of the remark.
The if part of the second statement is obvious. Suppose $\tau\colon L' \to L$ is an isometry. Then let B and B' be bases of L and L' such that $\mathcal{G}(B)$ and $\mathcal{G}(B')$ are the normal Gram matrices of L and L' respectively. Then $\mathcal{G}(\tau(B')) = \mathcal{G}(B')$ is a normal Gram matrix of L. By (1) it must be equal to $\mathcal{G}(B)$. □

5. Algorithms

First, an algorithm to compute some basis satisfying the conditions in Remark 4.2 is presented.

The quadratic form corresponding to the Gram matrix F_ε is (up to isometry) the unique anisotropic binary quadratic form over $\mathbb{F}_q$. Hence given $a, b \in \mathbb{F}_q^*$ such that $\mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q,\ (x,y) \mapsto x^2a + y^2b$ is anisotropic, there exists some $T \in \mathrm{GL}_2(\mathbb{F}_q)$

such that $T\mathrm{Diag}(a,b)T^{\mathrm{tr}} = F_\varepsilon$. Algorithms for finding such a base change T are well known but usually require (at least in some cases) finding suitable random elements. If $q-1 \notin 4\mathbb{Z}$ a generator α of $\mathbb{F}_{q^2}^*$ will be required anyway later on. The following deterministic algorithm makes use of this fact.

Algorithm 5.1.

Input: *$a, b \in \mathbb{F}_q^*$ such that $(x,y) \mapsto x^2a + y^2b$ is anisotropic.*

Output: *A matrix $T \in \mathrm{GL}_2(\mathbb{F}_q)$ such that $T\mathrm{Diag}(a,b)T^{\mathrm{tr}} = F_\varepsilon$.*

1 *Write $ac^2 = \varepsilon^k$ with $c \in \mathbb{F}_q^*$ and $k \in \{0,1\}$.*
2 *Let $d \in \mathbb{F}_q^*$ be a square root of $-\varepsilon^{1-k}/b$.*
3 **if** $k = 0$ **then return** $T := \mathrm{Diag}(c,d)$.
4 **if** $q-1 \in 4\mathbb{Z}$ **then**
5 | **return** $T := \left(\begin{smallmatrix} 0 & dj \\ cj & 0 \end{smallmatrix}\right)$ *where $j \in \mathbb{F}_q^*$ denotes a square root of -1.*
6 **else**
7 | *Let $u \in \mathbb{F}_q^*$ be a square root of $-\mathrm{Nr}(\alpha)$.*
8 | **return** $T := \frac{1}{u}\left(\begin{smallmatrix} yc/\varepsilon & xd \\ xc & yd \end{smallmatrix}\right)$ *where $x, y \in \mathbb{F}_q$ such that $\alpha = x + \mathrm{i}y$.*

Proof. The form $(x,y) \mapsto x^2a + y^2b$ is anisotropic. Thus a is a square if and only if $-1/b$ is a nonsquare. Hence d does exist. If $q-1 \in 4\mathbb{Z}$ then -1 is a square in $\mathbb{F}_q$ otherwise $-\mathrm{Nr}(\alpha)$ is a product of two nonsquares i.e. a square. So the matrix T exists in all cases. One checks that T does the trick. □

Again, getting c and k in the first line requires up to 4 square root computations. The second line and maybe one of the lines 5 or 7 each compute another square root. So in total, the algorithm above requires up to 4 square root computations and a fixed number of elementary operations.

Algorithm 5.2.

Input: *The Gram matrix $\mathcal{G}(B)$ of some reduced basis B of integral lattice L in a definite bilinear $\mathbb{F}_q$-space of dimension n.*

Output: *Some $T \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $T \cdot B$ satisfies the conditions of Remark 4.2.*

1 *From $\mathcal{G}(B)$ read off the successive minima $m_1, \ldots, m_r$ of L as well as $n_i = |\{1 \le k \le n \mid \deg \mathcal{G}(B)_{k,k} = m_i\}|$ for $1 \le i \le r$.*
2 **for** $1 \le i \le r$ **do**
3 | $j \leftarrow 1 + \sum_{k<i} n_k$
4 | **if** $n_i = 2$ **then**
5 | | *let $T_i \in \mathrm{GL}_2(\mathbb{F}_q)$ such that $T_i\mathrm{Diag}(\mathcal{G}(B)_{j,j}^{(m_i)}, \mathcal{G}(B)_{j+1,j+1}^{(m_i)}){T_i}^{\mathrm{tr}} = F_\varepsilon$.*
6 | **else** *let $T_i \in \mathbb{F}_q^*$ such that $T_i^2\mathcal{G}(B)_{j,j}^{(m_i)} = \varepsilon^k$ with $k \in \{0,1\}$.*
7 **return** $\mathrm{Diag}(T_1, \ldots, T_r)$.

If $n_i = 2$, line 5 can be done by calling Algorithm 5.1 which requires at most $4 = 2n_i$ square root computations. Otherwise line 6 requires at most 2 square root computations. So in total, $2\sum_i n_i = 2n$ square root computations suffice.

Remark 5.3. Let L be an integral lattice in a n-dimensional definite bilinear $\mathbb{F}_q(t)$-space such that L has n successive minima. Further let d be the largest successive minimum of L.

Given the Gram matrix $\mathcal{G}(B)$ of some reduced basis B of L, Algorithm 5.2 computes some $T \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $T \cdot B$ satisfies the conditions of Remark 4.2 using no more than $2n$ square root computations and $O(1)$ elementary operations. Let $H = \{\mathrm{Diag}(a_1, \ldots, a_n) \mid a_i \in \{-1, 1\}\}$ and $S = \{hT\mathcal{G}(B)(hT)^{\mathrm{tr}} \mid h \in H\}$. Then $\min S$ is the normal Gram matrix of L by Definition 4.3(1). The set S contains at most $2^{n-1} \leq 8$ matrices since $-\mathrm{id}_L \in O(L)$. Thus S can be enumerated using $O(d)$ elementary operations. This yields $O(L) = \mathrm{Stab}_H(\min(S))$ and some $T' \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\min S = T'\mathcal{G}(B)T'^{\mathrm{tr}}$. Hence Theorem 2.4 holds for lattices of rank n with n successive minima.

5.1. **The binary case.** The following pseudo code shows how to compute the normal Gram matrix and the automorphism group of a lattice of rank 2.

Algorithm 5.4.

Input: *The Gram matrix $\mathcal{G}(B)$ of some reduced basis B of an integral lattice L in a definite bilinear $\mathbb{F}_q(t)$-space of dimension 2.*

Output: *Some $T \in \mathrm{GL}_2(\mathbb{F}_q[t])$ such that $\mathcal{G}(T \cdot B)$ is the normal Gram matrix of L and $O(L)$ as a matrix group relative to the basis $T \cdot B$.*

1 *Using Algorithm 5.2, compute $T \in \mathrm{GL}_2(\mathbb{F}_q)$ such that $T \cdot B$ satisfies the conditions of Remark 4.2 and initialize $G \leftarrow T\mathcal{G}(B)T^{\mathrm{tr}}$.*
2 **if** $\deg G_{1,1} = \deg G_{2,2}$ **then**
3 **if** $G \in F_\varepsilon \cdot \mathbb{F}_q[t]$ **then return** *T and* $\mathrm{GO}_2^-(\mathbb{F}_q)$.
4 $d \leftarrow \max\{k \geq 0 \mid G^{(k)} \notin F_\varepsilon \cdot \mathbb{F}_q\}$
5 *Compute $h \in \mathrm{GO}_2^-(\mathbb{F}_q)$ such that $M := hG^{(d)}h^{\mathrm{tr}}$ is a representative from Corollary 3.7 (see Remark 3.8).*
6 $T \leftarrow hT$, $G \leftarrow hGh^{\mathrm{tr}}$ *and* $H \leftarrow \mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}(M)$.
7 **else** $H \leftarrow \langle -I_2, \mathrm{Diag}(1, -1)\rangle$
8 **if** *there exists some $h \in H$ such that $h \notin \{\pm I_2\}$* **then**
9 **if** $hGh^{\mathrm{tr}} \neq G$ **then** $H \leftarrow \langle -I_2\rangle$
10 **if** $hGh^{\mathrm{tr}} < G$ **then** $T \leftarrow hT$
11 **return** *T and H.*

Proof. The matrix G in step 1 equals $\mathcal{G}(T \cdot B)$. Hence, if $G \in F_\varepsilon \cdot \mathbb{F}_q[t]$ then G is the normal Gram matrix of L and $O(L) \cong \mathrm{GO}_2^-(\mathbb{F}_q)$. Suppose $G \notin F_\varepsilon \cdot \mathbb{F}_q[t]$. If L has one successive minimum, the matrix M in line 5 is symmetric. Thus the stabilizer H in line 6 has at most 4 elements and it contains $-I_2$ (see Corollary 3.7). The same holds for the group H in line 7. So lines 8-10 do compute $\min\{h\mathcal{G}(T \cdot B)h^{\mathrm{tr}} \mid h \in H\}$ which is the normal Gram matrix of L according to Definition 4.3. Further these lines find the stabilizer of this minimum in H which is $O(L)$. Hence the algorithm gives correct output. □

Corollary 5.5. *Let B be a basis of a lattice L in a definite bilinear $\mathbb{F}_q(t)$-space of dimension 2 such that $\mathcal{G}(B)$ is the normal Gram matrix of L. Then the matrix representation of $O(L)$ with respect to the basis B is either $\mathrm{GO}_2^-(\mathbb{F}_q)$, $\{\pm I_2\}$ or $\langle -I_2, s^n\mathrm{Diag}(1, -1)\rangle \cong C_2 \times C_2$ with $n \in \{0, 1\}$.*

Proof of Theorem 2.4 for $n = 2$. Algorithm 5.2 in line 1 requires $O(1)$ elementary operations and at most 4 square root computations. The computation of G in line 1 requires $O(d)$ elementary operations where d is the largest successive minimum

of L. Lines 2-4 can be done in one step by testing whether $G^{(k)}\mathrm{Diag}(1,-\varepsilon^{-1})$ is a scalar matrix in $\mathbb{F}_q^{2\times 2}$ for all $0 \le k < d$. This requires $O(d)$ elementary operations. The computation of h in line 5 requires at most 4 square root computations and $O(1)$ elementary operations by Remark 3.8. The remaining steps only need $O(d)$ elementary operations. □

5.2. **The ternary case.** Given a ternary lattice L with only two successive minima, the following algorithm can be used to compute the normal Gram matrix of L. For simplicity, it is assumed that the first two diagonal entries of a reduced Gram matrix of L have the same degree.

Algorithm 5.6.

Input: *The Gram matrix $\mathcal{G}(B)$ of some reduced basis $B = (B_1, B_2, B_3)$ of an integral lattice L in a definite bilinear $\mathbb{F}_q(t)$-space with $\deg \mathcal{G}(B)_{1,1} = \deg \mathcal{G}(B)_{2,2}$.*

Output: *Some $T \in \mathrm{GL}_3(\mathbb{F}_q[t])$ such that $\mathcal{G}(T \cdot B)$ is the normal Gram matrix of L and $O(L)$ as a matrix group relative to the basis $T \cdot B$.*

1 *Compute some $T_1 \in \mathrm{GL}_2(\mathbb{F}_q)$ such that $G' := \mathcal{G}(T_1 \cdot (B_1, B_2))$ is the normal Gram matrix of $\langle B_1, B_2\rangle$ and let $H = \mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}(G')$ (see Algorithm 5.4).*

2 *Compute $\lambda \in \mathbb{F}_q^*$ such that $\mathcal{G}(\lambda B_3)$ is the normal Gram matrix of $\langle B_3\rangle$.*

3 $T \leftarrow \mathrm{Diag}(T_1, \lambda)$ *and* $G \leftarrow T\mathcal{G}(B)T^{\mathrm{tr}}$.

4 **if** $G_{1,3} = G_{2,3} = 0$ **then return** T *and* $\mathrm{Diag}(H, \{\pm 1\})$.

5 **if** $H = \mathrm{GO}_2^-(\mathbb{F}_q)$ **then**

6 $\quad d \leftarrow \max\{\deg G_{1,3}, \deg G_{2,3}\}$.

7 $\quad$ *Using Algorithm 3.3, compute $g \in \mathrm{SO}_2^-(\mathbb{F}_q)$ such that $v := g \cdot \begin{pmatrix} G_{1,3} \\ G_{2,3} \end{pmatrix}^{(d)}$ is one of the representatives of Proposition 3.2.*

8 $\quad T \leftarrow \mathrm{Diag}(g, 1)T$, $G \leftarrow T\mathcal{G}(B)T^{\mathrm{tr}}$ *and* $H \leftarrow \mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}(v)$.

9 *Compute $h \in H' := \mathrm{Diag}(H, \{\pm 1\})$ such that $hGh^{\mathrm{tr}} = \min\{h'Gh'^{\mathrm{tr}} \mid h' \in H'\}$.*

10 **return** hT *and* $\mathrm{Stab}_{H'}(hGh^{\mathrm{tr}})$.

Proof. Let $S = \mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}(G')$. Then $\{\mathrm{Diag}(hT_1, \pm\lambda)\cdot B \mid h \in S\}$ is the set $\mathcal{B}$ from Definition 4.3. Hence if $\langle B_3\rangle$ is perpendicular to $\langle B_1, B_2\rangle$ then $\mathcal{G}(\mathrm{Diag}(T_1, \lambda)\cdot B)$ is the normal Gram matrix of L and its stabilizer in $\mathrm{GL}_3(\mathbb{F}_q)$ is $\mathrm{Diag}(S, \{\pm 1\})$. So in this case the algorithm gives correct output. Suppose now that the two sublattices are not perpendicular. If $S = \mathrm{GO}_2^-(\mathbb{F}_q)$ then the set $\mathcal{B}'$ from Definition 4.3(4) is given by $\{\mathrm{Diag}(hgT_1, \pm\lambda)\cdot B \mid h \in \mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}(v)\}$. Thus line 9 enumerates $\{\mathcal{G}(B') \mid B' \in \mathcal{B}'\}$ if $S = \mathrm{GO}_2^-(\mathbb{F}_q)$ and $\{\mathcal{G}(B') \mid B' \in \mathcal{B}\}$ otherwise. The minimum of the enumerated set is the normal Gram matrix of L by Definition 4.3. □

Proof of Theorem 2.4 for $n = 3$. By Remark 5.3, only the case that L has two successive minima remains. Then, without loss of generality, the previous algorithm can be applied to L.
First, the number of square root computations will be counted. The second line of Algorithm 5.6 computes at most two square roots and the same holds for line 7 (see Theorem 2.4 and Algorithm 3.3). Now Algorithm 5.4 in line 1 computes at most 8 square roots unless $\mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}(G') = \mathrm{GO}_2^-(\mathbb{F}_q)$, in that case 4 square roots suffice. So whether $\mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}(G') = \mathrm{GO}_2^-(\mathbb{F}_q)$ or not, no more than 10 square

root computations will be necessary.
Let d be the largest successive minimum of L. Then the first two lines also require $O(d)$ elementary operations (see Theorem 2.4). The base changes in lines 3 and 8 also require $O(d)$ elementary operations (note that $\mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}(v)$ is known from Remark 3.4). Finally $H' < \mathrm{GL}_3(\mathbb{F}_q)$ in line 9 has at most 8 elements (see Corollary 5.5 and Remark 3.4). Thus the final orbit enumeration requires $O(d)$ elementary operations. □

5.3. **The quaternary case.** The following pseudo code shows how to compute the normal Gram matrix and the automorphism group of a lattice of rank 4.

Algorithm 5.7.

Input: *The Gram matrix $\mathcal{G}(B)$ of some reduced basis B of an integral lattice L in a definite bilinear $\mathbb{F}_q(t)$-space of dimension 4.*

Output: *Some $T \in \mathrm{GL}_4(\mathbb{F}_q[t])$ such that $\mathcal{G}(T \cdot B)$ is the normal Gram matrix of L and $O(L)$ as a matrix group relative to the basis $T \cdot B$.*

Notation: *Let $L_1, \dots, L_r, H_1, \dots, H_r, \mathcal{B}$ and ψ be as in Definition 4.3.*

1 *Compute some $T \in \mathrm{GL}_4(\mathbb{F}_q)$ such that $T \cdot B \in \mathcal{B}$.*
2 $G \leftarrow T\mathcal{G}(B)T^{\mathrm{tr}}$ *and* $H \leftarrow \mathrm{Diag}(H_1, \dots, H_r)$.
3 **if** $H_1 = H_2 = \mathrm{GO}_2^-(\mathbb{F}_q)$ *and L_1 is not perpendicular to L_2* **then**
4 *Let M be the upper right 2×2 submatrix of G.*
5 *Compute $(g, h) \in \hat{G} := \mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$ such that $M' := gM^{(d)}h^{\mathrm{tr}}$ is a representative from Proposition 3.9 where $d = \max\{k \geq 0 \mid M^{(k)} \neq 0\}$.*
6 $T \leftarrow \mathrm{Diag}(g, h)T$, $G \leftarrow T\mathcal{G}(B)T^{\mathrm{tr}}$, $M \leftarrow gMh^{\mathrm{tr}}$ *and* $H' \leftarrow \mathrm{Stab}_{\hat{G}}(M')$.
7 **if** $|H'| > 8$ *and $M^{(k)}$ is not H'-invariant for all $k \geq 0$* **then**
8 *Let $d' = \max\{k \geq 0 \mid M^{(k)}$ is not H'-invariant$\}$.*
9 *Using Algorithm 3.6, compute $(g, h) \in H'$ such that $M'' := gM^{(d')}h^{\mathrm{tr}}$ is a representative from Corollary 3.7 or Remark 3.11.*
10 $T \leftarrow \mathrm{Diag}(g, h)T$, $G \leftarrow T\mathcal{G}(B)T^{\mathrm{tr}}$ *and* $H' \leftarrow \mathrm{Stab}_{H'}(M'')$.
11 $H \leftarrow \{\mathrm{Diag}(g, h) \mid (g, h) \in H'\}$.
12 **else if** *there exist $i \neq \ell$ such that $H_i = \mathrm{GO}_2^-(\mathbb{F}_q)$ and $L_i \not\perp L_\ell$* **then**
13 *Let $j = \min\{1 \leq k \leq 3 \mid B_k \in L_i\}$ and $d = \max\{k \geq 0 \mid \psi(G^{(k)}) \neq 0\}$.*
14 *Let $h_1, \dots, h_c$ be a transversal of $\langle \mathrm{Diag}(-I_{j-1}, I_2, -I_{3-j})\rangle$ in $\mathrm{Diag}(H_1, \dots, H_{i-1}, \{I_2\}, H_{i+1}, \dots, H_r)$.*
15 **for** $1 \leq k \leq c$ **do**
16 *Using Algorithm 3.3, compute $g \in \mathrm{SO}_2^-(\mathbb{F}_q)$ such that the first nonzero row v_k of $g\psi(G^{(d)}{h_k}^{\mathrm{tr}})$ is a representative from Proposition 3.2.*
17 $T'_k \leftarrow \mathrm{Diag}(I_{j-1}, g, I_{3-j})h_k$ *and* $H'_k \leftarrow \mathrm{Diag}(\{I_{j-1}\}, \mathrm{Stab}_{H_i}(v_k), \{I_{3-j}\})$.
18 *Find $T_k \in \mathrm{GL}_4(\mathbb{F}_q)$ such that $T_k G {T_k}^{\mathrm{tr}} = \min\{g'T'_kG(g'T'_k)^{\mathrm{tr}} \mid g' \in H'_k\}$.*
19 $S_k \leftarrow \mathrm{Stab}_{H'_k}(T_k G {T_k}^{\mathrm{tr}})$.
20 **if** $c = 2$ *and* $T_2 G {T_2}^{\mathrm{tr}} = T_1 G {T_1}^{\mathrm{tr}}$ **then** *Include $T_2T_1^{-1}$ in S_1.*
21 **if** $c = 2$ *and* $T_2 G {T_2}^{\mathrm{tr}} < T_1 G {T_1}^{\mathrm{tr}}$ **then** $T_1 \leftarrow T_2$ *and* $S_1 \leftarrow S_2$.
22 **return** T_1T *and* $\langle -I_4,\ S_1\rangle$.
23 *Compute $h \in H$ such that $hGh^{\mathrm{tr}} = \min\{h'Gh'^{\mathrm{tr}} \mid h' \in H\}$.*
24 **return** hT *and* $\mathrm{Stab}_H(hGh^{\mathrm{tr}})$.

Proof. Suppose first that case 3 of Definition 4.3 applies to L. In this case the last two lines of the above algorithm do enumerate $\{\mathcal{G}(\tilde{B}) \mid \tilde{B} \in \mathcal{B}\}$.
Suppose case (4) of Definition 4.3 applies to L and let $\mathcal{B}'$ be as in Definition 4.3(4). Since $-\mathrm{id}_L \in O(L)$ and $-I_2 \in \mathrm{GO}_2^-(\mathbb{F}_q)$, the set $S := \{\mathcal{G}(B') \mid B' \in \mathcal{B}'\}$ equals $\{\mathcal{G}(g'T_k'T\cdot B) \mid g' \in H_k',\ 1 \le k \le c\}$ with T_k', H_k' and T as line 18. Further, it follows from Remark 4.2 and Corollary 5.5 that the transversal from line 14 has at most 2 elements. So lines 20-22 do compute $T \in \mathrm{GL}_4(\mathbb{F}_q)$ such that $\mathcal{G}(T\cdot B) = \min S$ as well as the stabilizer of $\min S$ in $\mathrm{Diag}(H_1, \dots, H_r)$ which is the matrix representation of $O(L)$ with respect to $T \cdot B$. Similarly one proves that the algorithm gives correct output if case (5) of Definition 4.3 applies to L. □

Proof of Theorem 2.4 for $n = 4$. Let m_r be the largest successive minimum of L. It follows from Theorem 2.4 for $n = 1, 2$ that the first two lines require $O(m_r)$ elementary operations and at most 16 square root computations. But note that this bound can only be achieved if Algorithm 5.1 is called twice and both times it computes the square root of -1 or $-\mathrm{Nr}(\alpha)$. Thus 15 square root computations suffice for step 1 of Algorithm 5.7.
Suppose now that lines 13-22 are executed. Each call to Algorithm 3.3 in line 16 computes up to two square roots. Since H_k' in line 17 has two elements and $c \in \{1, 2\}$, lines 13-22 require no more than 4 square root computations and $O(m_r)$ elementary operations. So the theorem holds in this case.
Suppose now that the condition in line 3 holds. If $|H'| \le 8$ then line 5 requires at most 10 square root computations (see Remark 3.10). Otherwise it computes only two square roots but then line 9 might also require up to 4 square root computations. So in any case, lines 4-11 require (besides $O(m_r)$ elementary operations) no more than 10 square root computations. Further, the group H' is given in Proposition 3.9 by at most three generators. So the condition in line 7 can be tested using $O(m_r)$ elementary operations. Moreover, it follows from loc. cit, Corollary 3.7 and Remark 3.11 that if the group H in line 11 does not fix G, it can have no more than 8 elements. Therefore, the final orbit enumeration in lines 23-24 requires $O(m_r)$ elementary operations.
Finally suppose that the conditions in lines 3 and 12 both do not hold for L. Then H_i might equal $\mathrm{GO}_2^-(\mathbb{F}_q)$ for some i by Corollary 5.5. But then L_i is perpendicular to every other lattice L_k by assumption. So in this case, $O(L)$ contains not only $-\mathrm{id}_L$, but also $O(L_i) = H_i$. Thus it follows from loc. cit. and Remark 4.2 that the orbit in line 23 contains no more than 8 elements. Since each H_i is given by at most two generators, the orbit enumeration in lines 23-24 can be done using $O(m_r)$ elementary operations. This finishes the proof. □

6. If -1 is a square in $\mathbb{F}_q$

Suppose $q-1$ is divisible by 4. In this section normal Gram matrices for definite forms over $\mathbb{F}_q[t]$ are presented that only depend on the total order $<$. Let r be the 2-adic valuation of $\frac{q-1}{2}$. Then one can compute r repeated square roots from -1. If in each step, one prefers the smaller root over the larger one (with respect to $<$), this ends in a nonsquare ε that only depends on $<$. Just like before let $\mathfrak{i} \in \mathbb{F}_{q^2}$ such that $\mathfrak{i} < -\mathfrak{i}$ and $\mathfrak{i}^2 = 1/\varepsilon$.

The definition of normal Gram matrices (see Definition 4.3) only depend on Propositions 3.2, 3.5, 3.9 and Corollary 3.7. So it suffices to replace the systems of

representatives from Propositions 3.2, 3.5, 3.9 and Corollary 3.7 by systems that only depend on $\mathfrak{i}$ and $<$.

Let N be the norm 1 subgroup of $\mathbb{F}_{q^2}^*$. The proofs of Propositions 3.2 and 3.5 work whenever $\alpha \in \mathbb{F}_{q^2}^*$ is a nonsquare and $\beta \in N \setminus N^2$.

Now if $\mathfrak{i}$ would be a square in $\mathbb{F}_{q^2}^*$, say $x^2 = \mathfrak{i}$ then $\mathrm{Nr}(x)^2 = \mathrm{Nr}(\mathfrak{i}) = 1/\varepsilon$ would be a contradiction. Similarly if $-1 = x^2$ for some $x \in N$ then the assumption on q implies that $x \in \mathbb{F}_q^*$. But then $1 = \mathrm{Nr}(x) = x^2$ is also a contradiction.

Thus, in Proposition 3.2 one can replace α by $\mathfrak{i}$. (For the stabilizers in Remark 3.4, one obviously gets $\mathrm{Stab}_{\mathrm{GO}_2^-(\mathbb{F}_q)}\left(\begin{smallmatrix}0\\b\end{smallmatrix}\right) = \langle \mathrm{Diag}(-1,1)\rangle$ for all $b \neq 0$.)

Similarly, in Proposition 3.5 one can replace α and β by $\mathfrak{i}$ and -1 respectively. But then this also holds for Corollary 3.7. (For the stabilizers one has to replace $s^n D$ by D in Corollary 3.7.)

Finally, Proposition 3.9 only depends on Propositions 3.2 and 3.5 as well as Remark 3.7. Thus also here one can replace α and β with $\mathfrak{i}$ and -1. Since the stabilizers also change somewhat, the new system of representatives is explicitly given below.

type	representative	stabilizer
1	$\varphi(0,0,0)$	$\mathrm{GO}_2^-(\mathbb{F}_q) \times \mathrm{GO}_2^-(\mathbb{F}_q)$
2	$\varphi(a,0,0)$	$\{(g,g) \mid g \in \mathrm{GO}_2^-(\mathbb{F}_q)\}$
3	$\varphi(0,a,0)$	$\langle (s,s),\ (D,-D)\rangle$
4	$\varphi(a,0,(-1)^n a)$	$\langle (-I_2,-I_2),\ (I_2,(-1)^n D),\ ((-1)^n D, I_2)\rangle$
5	$\varphi(0,a,(-1)^n a\mathfrak{i})$	$\big\langle (-I_2,-I_2),\ (I_2,(-1)^n D),\ (D(-1)^{1-n}, I_2)\big\rangle$
6	$\varphi(a,0,\pm c)$	$\langle (-I_2,-I_2),\ (D,D)\rangle$
7	$\varphi(0,a,\pm c\mathfrak{i})$	$\langle (-I_2,-I_2),\ (D,-D)\rangle$
8	$\varphi(a,0,\tilde{c}\mathfrak{i})$	$\langle (-I_2,-I_2)\rangle$

where $a, c, \tilde{c} \in \mathbb{F}_{q,<}^*$ such that $a < c$ and $n \in \{0,1\}$.

References

1. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.
2. D.Z. Djoković, *Hermitian matrices over polynomial rings*, J. Algebra **43** (1976), 359–374.
3. L. Gerstein, *Definite quadratic forms over* $\mathbb{F}_q[x]$, J. Algebra **268** (2003), no. 1, 252–263.
4. M. Kirschmer, *Algorithmic enumeration of ideal classes for quaternion orders over* $\mathbb{F}_q[t]$, In preparation.
5. M. Kneser and R. Scharlau, *Quadratische formen*, Springer Verlag, 2002.
6. F. Lübeck, *Tables of conway polynomials*, `http://www.math.rwth-aachen.de/~Frank.Luebeck/data/ConwayPol/index.html`.
7. H. Minkowski, *Über die positiven quadratischen Formen und über kettenbruchähnlichen Algorithmen*, J. Reine Angew. Math. **107** (1891), 278–297.
8. W. Plesken and B. Souvignier, *Computing isometries of lattices*, Journal of Symbolic Computation **24** (1997), 327–334.

Lehrstuhl D für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany

E-mail address: `markus.kirschmer@math.rwth-aachen.de`