Journal of Algebra 447 (2016) 560–579

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Lattices from Hermitian function fields ☆

Albrecht Böttcher [a], Lenny Fukshansky [b,*], Stephan Ramon Garcia [c], Hiren Maharaj [b]

[a] *Fakultät für Mathematik, TU Chemnitz, 09107 Chemnitz, Germany*
[b] *Department of Mathematics, Claremont McKenna College, 850 Columbia Ave, Claremont, CA 91711, USA*
[c] *Department of Mathematics, Pomona College, 610 N. College Ave, Claremont, CA 91711, USA*

ARTICLE INFO

Article history:
Received 22 February 2015
Available online xxxx
Communicated by
Eva Bayer-Fluckiger

MSC:
primary 11H06
secondary 11G20

Keywords:
Hermitian curves
Function fields
Well-rounded lattices
Kissing number
Automorphism group

ABSTRACT

We consider the well-known Rosenbloom–Tsfasman function field lattices in the special case of Hermitian function fields. We show that in this case the resulting lattices are generated by their minimal vectors, provide an estimate on the total number of minimal vectors, and derive properties of the automorphism groups of these lattices. Our study continues previous investigations of lattices coming from elliptic curves and finite Abelian groups. The lattices we are faced with here are more subtle than those considered previously, and the proofs of the main results require the replacement of the existing linear algebra approaches by deep results of Gerhard Hiss on the factorization of functions with particular divisor support into lines and their inverses.

☆ Fukshansky acknowledges support by Simons Foundation grant #279155 and NSA grant H98230-1510051, Garcia acknowledges support by NSF grant DMS-1265973.

* Corresponding author.
E-mail addresses: aboettch@mathematik.tu-chemnitz.de (A. Böttcher), lenny@cmc.edu (L. Fukshansky), stephan.garcia@pomona.edu (S.R. Garcia), hmahara@g.clemson.edu (H. Maharaj).

http://dx.doi.org/10.1016/j.jalgebra.2015.09.044
0021-8693/

1. Introduction

A lattice is a discrete subgroup in a Euclidean space $\mathbb{R}^n$. Lattice theory aims to understand geometric properties of lattices and to use them for a variety of applications, such as discrete optimization problems or coding theory. Some of the geometrically most interesting lattices, in particular those possessing many symmetries, come from several well-studied algebraic constructions. These include, for instance, ideal lattice constructions from number fields and polynomial rings; see, e.g., [1,2] and [8], respectively, for a detailed overview of these constructions. A series of prominent algebraic constructions of lattices are also presented in [14]. In this paper, we focus our attention on an important algebraic construction, originally introduced by Rosenbloom and Tsfasman in [10] and later described in [14], that of *function field lattices*.

The construction of function field lattices given in [14] is as follows. Let F be an algebraic function field (of a single variable) with the finite field $\mathbb{F}_q$ as its full field of constants, where q is a prime power. Let $\mathcal{P} = \{P_0, P_1, P_2, \dots, P_{n-1}\}$ be the set of rational places of F. For each place P_i, let v_i denote the corresponding normalized discrete valuation and let $\mathcal{O}_{\mathcal{P}}^*$ be the set of all nonzero functions $f \in F$ whose divisor has support contained in the set $\mathcal{P}$. Then $\mathcal{O}_{\mathcal{P}}^*$ is an Abelian group, $\sum_{i=0}^{n-1} v_i(f) = 0$ for each $f \in \mathcal{O}_{\mathcal{P}}^*$, and we define

$$\deg f := \sum_{v_i(f)>0} v_i(f) = \frac{1}{2} \sum_{i=0}^{n-1} |v_i(f)|.$$

Let $\varphi_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}}^* \to \mathbb{Z}^n$ be the group homomorphism given by

$$\varphi_{\mathcal{P}}(f) = (v_0(f), v_1(f), \dots, v_{n-1}(f)).$$

Then $L_{\mathcal{P}} := \mathrm{Image}(\varphi_{\mathcal{P}})$ is a finite-index sublattice of the root lattice

$$A_{n-1} = \left\{ \mathbf{x} = (x_0, \dots, x_{n-1}) \in \mathbb{Z}^n : \sum_{i=0}^{n-1} x_i = 0 \right\}$$

with minimum distance

$$d(L_{\mathcal{P}}) \geq \min \left\{ \sqrt{2 \deg f} : f \in \mathcal{O}_{\mathcal{P}}^* \setminus \mathbb{F}_q \right\}, \tag{1}$$

and

$$\det L_{\mathcal{P}} \leq \sqrt{n} h_F \leq \sqrt{n} \left(1 + q + \frac{n - q - 1}{g} \right)^g, \tag{2}$$

where g is the genus of F and h_F is the divisor class number of F, that is, the size of the group of divisor classes of F of degree 0, denoted by $\mathrm{Cl}^0(F)$. Here, as in [14], we

can identify $\mathbb{Z}^n$ with the set of all divisors with support in $\mathcal{P}$ and A_{n-1} with the set of all divisors of degree 0. We will often make use of this identification when working with lattice vectors by working with the corresponding divisors instead.

Unless stated otherwise, we will use notation as in [13]. We write $F/\mathbb{F}_q$ to mean that F is a global function field with full field of constants $\mathbb{F}_q$. Let $g = g(F)$ denote the genus of F. If P is a rational place of F, that is, a place of degree one, then v_P denotes the discrete valuation corresponding to P. We write $\operatorname{supp} A$ for the support of a divisor A. The divisor of a function $f \in F \setminus \{0\}$ is denoted by (f) and the divisor class of a divisor D by $[D]$.

We will study lattices from Hermitian function fields. The Hermitian function field $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ has defining equation $y^q + y = x^{q+1}$. The purpose of this paper is to show that the lattices which arise from Hermitian function fields are generated by minimal vectors and are hence well-rounded. Recall that a lattice L of rank k is called well-rounded if it contains k linearly independent minimal vectors, i.e., vectors of Euclidean norm equal to $d(L)$, and that L is said to be generated by minimal vectors if the set of all minimal vectors of L spans L over $\mathbb{Z}$. The statement that L is generated by minimal vectors is equivalent to the statement that L is well-rounded for $k \le 4$ and is strictly stronger for $k \ge 5$; in other words, there exist well-rounded lattices of rank 5 and greater whose minimal vectors generate a sublattice of index greater than 1. See [9] for further information.

In [4], we studied sublattices L_G of the root lattice A_{N-1} which are of the form

$$L_G = \left\{ \mathbf{x} = (x_0, \dots, x_{N-1}) \in A_{N-1} : \sum_{j=1}^{N-1} x_j g_j = 0 \right\}, \tag{3}$$

where $G = \{g_0 := 0, g_1, \dots, g_{N-1}\}$ is a finite (additively written) Abelian group. We showed that $\det L_G = N^{3/2}$ and that except for $G = \mathbb{Z}_4$, the lattice L_G always has a basis of minimal vectors and is hence well-rounded. Here and in what follows, $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$. Such lattices emerge in particular when applying the above construction to elliptic curves over $\mathbb{F}_q$. The groups G coming from elliptic curves were characterized by Rück [11], and for these groups, the results of [4] had previously been established by Min Sha [12].

The only elliptic curve among the Hermitian curves $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$ is the curve $y^2 + y = x^3$ over $\mathbb{F}_4$, which corresponds to $q = 2$; see [5]. In that case G is isomorphic to $\mathbb{Z}_3^2$, that is, we have $N = 9$ and $\det L_G = 27$.

Except for the case $q = 2$, the Hermitian function fields considered here lead to a class of lattices which are more general than the lattices (3). Namely, given a finite Abelian group G and a subset $S = \{g_0 := 0, g_1, \dots, g_{n-1}\}$ of G, we define the sublattice $L_G(S)$ of A_{n-1} by

$$L_G(S) = \left\{ \mathbf{x} = (x_0, \dots, x_{n-1}) \in A_{n-1} : \sum_{j=1}^{n-1} x_j g_j = 0 \right\}.$$

It turns out that unless $S = G$, in which case $L_G(G) = L_G$, the situation changes dramatically: there are many S for which $L_G(S)$ is well-rounded and there are many S for which $L_G(S)$ is not well-rounded. In general it is a delicate problem to decide which of the two possibilities occurs in a concrete case.

As the result of the abstract construction of function field lattices outlined above, we obtain $L_{\mathcal{P}} = L_G(S)$, where S is the set $S = \{[P_i - P_0] : 0 \le i \le n-1\}$ of divisor classes and G is the subgroup of the divisor class group $\mathrm{Cl}^0(F)$ generated by S. Thus, in this case S is not simply a subset of G, but a generating set for G. If the function field is specified to be $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ with the defining equation $y^q + y = x^{q+1}$, the group G can be shown to be isomorphic to $\mathbb{Z}_{q+1}^{q^2-q}$, which is just the above $\mathbb{Z}_3^2$ for $q = 2$, and S becomes a set of $q^3 + 1$ generators of G. For $q = 2$, S has 9 elements and therefore coincides with G. However, if $q > 2$, then the set S is much smaller than G. In the light of what was said at the end of the preceding paragraph, it is therefore a rather surprising fact that the lattices $L_{\mathcal{P}}$ coming from the curves $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$ are always well-rounded and even more, are generated by their minimal vectors.

To strengthen the surprise and to emphasize the subtlety of the matter we mention the following. The Klein curve K is defined by

$$(x+y+1)^4 + (xy+x+y)^2 + xy(x+y+1) = 0.$$

Over $\mathbb{F}_4$, the set $\mathcal{P}$ of $\mathbb{F}_4$-rational points of K contains 14 elements, and the curve yields a rank 13 lattice $L_{\mathcal{P}}$ of dimension 14. A quick computation using Magma [3] shows that the lattice $L_{\mathcal{P}}$ has 168 minimal vectors. These minimal vectors generate a sublattice of $L_{\mathcal{P}}$ of index 2. This implies that $L_{\mathcal{P}}$ is well-rounded but not generated by the minimal vectors.

This paper is organized as follows. In Section 2 we set the basic notation of Hermitian function fields. In Section 3 we give a detailed characterization of divisors coming from lines in a Hermitian function field. We derive formulas for the minimal distance and determinant of lattices coming from Hermitian function fields via the above construction in Sections 4 and 5, respectively. In Section 6 we establish our main result, which asserts that these lattices are generated by their minimal vectors. Our proof makes essential use of the results of Hiss [7]. We do not know of a proof along the linear algebra approaches developed in [4] and [12]. In Section 7 we investigate properties of automorphism groups of these lattices, as well as more general lattices coming from generating sets in Abelian groups. Finally, in Section 8 we establish a lower bound on the number of minimal vectors of lattices from Hermitian function fields, which is the same as the kissing number of these lattices.

2. Hermitian function fields: basic facts

The following are some basic facts about these function fields. Let H denote $\mathbb{F}_{q^2}(x,y)$ with the defining equation $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. Thus, we use H for the function

field F in the Rosenbloom–Tsfasman construction outlined above. The genus of H is $g = \frac{q(q-1)}{2}$ and H has $n = q^3 + 1$ places of degree 1 over $\mathbb{F}_{q^2}$, namely

- the common pole Q_∞ of x and y, and
- for each $\alpha \in \mathbb{F}_{q^2}$, there are q elements $\beta \in \mathbb{F}_{q^2}$ such that $\beta^q + \beta = \alpha^{q+1}$, and for each such pair (α, β) there is a unique place $P_{\alpha,\beta}$ of H of degree one with $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$.

Let

$$\mathcal{K} := \{(\alpha, \beta) \in \mathbb{F}_{q^2}^2 : \beta^q + \beta = \alpha^{q+1}\}.$$

We let $\mathcal{P}$ stand for the set of rational places of H: the place Q_∞ and the places $P_{\alpha,\beta}$ indexed by $(\alpha, \beta) \in \mathcal{K}$. For each $(\alpha, \beta) \in \mathcal{K}$, set

$$\tau_{\alpha,\beta} := y - \beta - \alpha^q(x - \alpha).$$

Observe that $\tau_{\alpha,\beta} = y - \alpha^q x + \beta^q$ and note that $\tau_{\alpha,\beta}$ is the tangent line to the Hermitian curve at the point (α, β). If one views H as a Kummer extension over $\mathbb{F}_{q^2}(y)$, the rational places of $\mathbb{F}_{q^2}(y)$ behave as follows:

- For each $\gamma \in \mathbb{F}_{q^2}$ such that $\gamma^q + \gamma = 0$, the place $y - \gamma$ is totally ramified. If $\gamma^q + \gamma \neq 0$, the place $y - \gamma$ splits completely in H.
- The pole of y is totally ramified.

We remark that

$$\tau_{\alpha,\beta}^q + \tau_{\alpha,\beta} = (x - \alpha)^{q+1}. \tag{4}$$

We therefore have $H = \mathbb{F}_{q^2}(x, y) = \mathbb{F}_{q^2}(\tau_{\alpha,\beta}, x)$, and so we may view H as a Kummer extension of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$. It follows that the divisor of $\tau_{\alpha,\beta}$ is

$$(\tau_{\alpha,\beta}) = (q+1)P_{\alpha,\beta} - (q+1)Q_\infty.$$

Following the usual convention for rational function fields, we denote the places of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ by their corresponding monic irreducible polynomials, except in the case of the place at infinity, which we denote by $P_\infty(\tau_{\alpha,\beta})$. For any $\gamma \in \mathbb{F}_{q^2}$ satisfying $\gamma^q + \gamma = 0$, we have $\tau_{\alpha,\beta} - \gamma = \tau_{\alpha,\beta+\gamma}$. Thus, we will write "the place $\tau_{\alpha,\beta+\gamma}$ in $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$" to mean the place $\tau_{\alpha,\beta} - \gamma$.

3. Divisors of lines

We will call functions of the form $ax + by + c$ ($a, b, c \in \mathbb{F}_{q^2}$ with not both a, b zero) lines. Furthermore, by points on the line $ax + by + c$ we mean the points of intersection

of the line $ax + by + c$ with the Hermitian curve $y^q + y = x^{q+1}$. In the next result we determine the divisor of every line and thus obtain the points (of $\mathcal{K}$) which lie on a line.

Lemma 3.1. *Let $H/\mathbb{F}_{q^2}$ denote a Hermitian function field and let $\gamma \in \mathbb{F}_{q^2}$.*

(a) *If $\gamma^q + \gamma = 0$, the place $\tau_{\alpha,\beta} - \gamma = \tau_{\alpha,\beta+\gamma}$ in $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ is totally ramified in the extension $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$. The divisor of $\tau_{\alpha,\beta} - \gamma$ is*

$$(\tau_{\alpha,\beta} - \gamma) = (q+1)P_{\alpha,\beta+\gamma} - (q+1)Q_\infty.$$

The line $\tau_{\alpha,\beta} - \gamma$ is a tangent line.

(b) *The pole $P_\infty(\tau_{\alpha,\beta})$ of $\tau_{\alpha,\beta}$ is totally ramified in the extension $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$.*

(c) *If $\gamma^q + \gamma \neq 0$, the place $\tau_{\alpha,\beta} - \gamma$ in $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ splits completely in the extension $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ and the divisor of $\tau_{\alpha,\beta} - \gamma$ is*

$$\sum_{i=0}^{q} P_{\alpha+\delta\zeta^i,\beta+\gamma+\alpha^q\delta\zeta^i} - (q+1)Q_\infty \tag{5}$$

where ζ is a primitive $(q+1)$st root of unity in $\mathbb{F}_{q^2}$ and $\delta \in \mathbb{F}_{q^2}^*$ is such that $\gamma^q + \gamma = \delta^{q+1}$. The points of $\mathcal{K}$ which lie on the line $\tau_{\alpha,\beta} - \gamma$ are precisely

$$(\alpha + \delta\zeta^i, \beta + \gamma + \alpha^q\delta\zeta^i) \ \ (0 \le i \le q).$$

The line $\tau_{\alpha,\beta} - \gamma$ is not a tangent line.

(d) *Suppose that $f = y + bx + c$. Let $\delta \in \mathbb{F}_{q^2}$ be such that $\delta^{q+1} = b^{q+1} - (c^q + c)$. Then the points of $\mathcal{K}$ which lie on the line f are precisely*

$$(-b^q + \delta\zeta^i, b^{q+1} - c - b\delta\zeta^i) \ \ (0 \le i \le q).$$

It follows that f is a tangent line if and only if $\delta = 0$ if and only if $(-b^q, c^q) \in \mathcal{K}$ (if and only if $(-b, c) \in \mathcal{K}$). If f is a tangent line then $f = \tau_{-b^q,c^q}$. If $\delta \neq 0$, then f contains exactly $q+1$ points from $\mathcal{K}$.

(e) *Suppose that $f = x - c$. Then the divisor of f is*

$$\sum_d P_{c,d} - qQ_\infty \tag{6}$$

where the sum is over the q solutions $d \in \mathbb{F}_{q^2}$ to $d^q + d = c^{q+1}$.

Proof. Parts (a), (b), (e) follow from viewing H as a Kummer extension of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$.

Proof of (c): The first statement of (c) follows from viewing H as a Kummer extension of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$. In order to get the divisor of $\tau_{\alpha,\beta} - \gamma$, we use Kummer's theorem [13, Theorem 3.3.7] to study the decomposition of the place $\tau_{\alpha,\beta} - \gamma$ in the extension $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$. The minimal polynomial of x over $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ is $\phi(T) := (T - \alpha)^{q+1} - \tau_{\alpha,\beta}^q - \tau_{\alpha,\beta} \in$

$\mathbb{F}_{q^2}(\tau_{\alpha,\beta})[T]$. The residue class field of the place $\tau_{\alpha,\beta}-\gamma$ of the rational function field $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ is isomorphic to $\mathbb{F}_{q^2}$. Using the notation of [13, Theorem 3.3.7] we wish to study the decomposition of the polynomial $\overline{\phi}(T)=(T-\alpha)^{q+1}-(\gamma^q+\gamma)\in\mathbb{F}_{q^2}[T]$ over this field. Since the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ is given by $z\mapsto z^q+z$ and the norm map $z\mapsto z^{q+1}$ from $\mathbb{F}_{q^2}^*$ to $\mathbb{F}_q^*$ is surjective, there exists a $\delta\in\mathbb{F}_{q^2}^*$ such that $\gamma^q+\gamma=\delta^{q+1}$. Let ζ be a primitive $(q+1)$st root of unity in $\mathbb{F}_{q^2}$. Then, using the notation of [13, Theorem 3.3.7] we get that $\overline{\phi}(T)=(T-\alpha)^{q+1}-\delta^{q+1}=\prod_{i=0}^{q}(T-\alpha-\delta\zeta^i)$. Thus the place $\tau_{\alpha,\beta}-\gamma$ splits completely in the extension $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ and the function $\tau_{\alpha,\beta}-\gamma$ has $q+1$ zeroes in H, say $Z_0,Z_1,\ldots,Z_q$, such that $x-\alpha-\delta\zeta^i\in Z_i$ for $0\le i\le q$. Since $\tau_{\alpha,\beta}-\gamma=y-\alpha^q x+\beta^q-\gamma=(y-\beta-\delta\alpha^q\zeta^i)-\alpha^q(x-\alpha-\delta\zeta^i)$, we see that a common zero of the functions $\tau_{\alpha,\beta}-\gamma$ and $x-\alpha-\delta\zeta^i$ must also be a zero of $y-\beta-\delta\alpha^q\zeta^i$. The functions $x-\alpha-\delta\zeta^i$ and $y-\beta-\delta\alpha^q\zeta^i$ have a unique common zero in H, namely $P_{\alpha+\delta\zeta^i,\beta+\delta\alpha^q\zeta^i}$. This implies that $Z_i=P_{\alpha+\delta\zeta^i,\beta+\delta\alpha^q\zeta^i}$ for $0\le i\le q$. Also, since $\tau_{\alpha,\beta}-\gamma=y-\alpha^q x+\beta^q-\gamma$ we see that any pole of $\tau_{\alpha,\beta}-\gamma$ must be pole of the functions x or y. From part (g) of [13, Proposition 6.4.1] we see that Q_∞ is the unique pole of $\tau_{\alpha,\beta}-\gamma$ and the order of the pole is $q+1$. This proves (c).

Proof of (d): First note that since $b^{q+1}-(c^q+c)\in\mathbb{F}_{q^2}$, there exists $\delta\in\mathbb{F}_{q^2}$ such that $\delta^{q+1}=b^{q+1}-(c^q+c)$. Let $\alpha=-b^q$. Then $b=-\alpha^q$. If $\beta\in\mathbb{F}_{q^2}$ satisfies $\beta^q+\beta=\alpha^{q+1}=b^{q+1}$, then $f=y-\alpha^q x+c=\tau_{\alpha,\beta}-\gamma$ where $\gamma=\beta^q-c$. Now observe that $\gamma^q+\gamma=b^{q+1}-(c^q+c)=\delta^{q+1}$. By (c), it follows that the points on the line f are $(\alpha+\delta\zeta^i,\beta+\gamma+\alpha^q\delta\zeta^i)=(-b^q+\delta\zeta^i,b^{q+1}-c-b\delta\zeta^i)$.

Observe that f is a tangent line to the Hermitian curve at the point $(B,C)\in\mathcal{K}$ iff $f=\tau_{B,C}=y-B^q x+C^q$ for some $(B,C)\in\mathcal{K}$ iff $(b,c)=(-B^q,C^q)$ for some $(B,C)\in\mathcal{K}$. Since $b=-B^q$ iff $B=-b^q$ and $c=C^q$ iff $C=c^q$ it follows that f is a tangent line iff $(-b^q,c^q)\in\mathcal{K}$. Now observe that $(-b^q,c^q)\in\mathcal{K}$ iff $(-b,c)\in\mathcal{K}$ iff $\delta=0$. □

4. The minimum distance of the lattice $L_{\mathcal{P}}$

Theorem 4.1. *The minimum distance of the lattice is $\sqrt{2q}$ and the minimum degree of every non-constant function in $\mathcal{O}_{\mathcal{P}}^*$ is q.*

Proof. Choose a point $P=(\alpha,\beta)$ on the affine Hermitian curve and choose two distinct non-tangent lines f_1, f_2 passing through P which are not 'vertical', that is, neither of the lines are of the form $x-\alpha$. Such a pair of lines is easily constructed. Indeed, choose two distinct nonzero slopes M_1 and $M_2\in\mathbb{F}_{q^2}$ such that M_1 and M_2 are both not equal to $-\alpha^q$. Then, by the surjectivity of the Frobenius endomorphism, there exist $m_1,m_2\in\mathbb{F}_{q^2}$ such that $M_1=m_1^q$ and $M_2=m_2^q$. Now let $f_1=y-\beta-m_1^q(x-\alpha)$ and $f_2=y-\beta-m_2^q(x-\alpha)$. Both these lines pass through P, by Theorem 3.1 (d) they cannot be tangential to the Hermitian curve at the point P because neither has slope $-\alpha^q$ and they cannot be tangential to the Hermitian curve at any other point because every tangent line passes through exactly one point of the Hermitian curve, namely the point of tangency. From Theorem 3.1 (c) it follows that the intersection of the supports of

the divisors of f_1 and f_2 consists only of Q_∞ and $P_{\alpha,\beta}$ and furthermore the lattice vector corresponding to f_1/f_2 has q ones, q minus ones, and that the remaining entries are all zero. The ℓ_1-norm of the corresponding lattice vector is $2q$ and the Euclidean norm of that lattice vector equals $\sqrt{2q}$. Thus, the minimum of the ℓ_1-norms of the nonzero lattice vectors is at most $2q$.

Now choose a function f corresponding to a nonzero lattice vector. Note that the sum of the positive entries of the corresponding lattice vector equals minus the sum of the negative entries, which also equals the degree $[H : \mathbb{F}_{q^2}(f)]$. Since H has q^3+1 rational places and $\mathbb{F}_{q^2}(f)$ has q^2+1 rational places, it follows that $q^3+1 \le [H : \mathbb{F}_{q^2}(f)](q^2+1)$, whence $[H : \mathbb{F}_{q^2}(f)] \ge (q^3+1)/(q^2+1)$ and thus $[H : \mathbb{F}_{q^2}(f)] \ge q$. Consequently, the minimum ℓ_1-norm is at least $2q$. From above it follows that the minimum ℓ_1 norm is exactly $2q$.

Now let f be a function which corresponds to a nonzero lattice vector of minimum ℓ_2-norm. Then $\|f\|_2^2 \ge \|f\|_1 \ge 2q$ with equality throughout if $f = f_1/f_2$. It follows that the minimum norm of the lattice is $\sqrt{2q}$. □

5. The exact determinant of the lattice $L_{\mathcal{P}}$

First we recall part of the proof of Tsfasman and Vladut for the upper bound (2) on the determinant of a lattice from a function field given in [14]. Let F be a function field over a finite field $\mathbb{F}_q$ and let $\mathcal{P}$ be a nonempty set of rational places of F. The set $O_{\mathcal{P}}^*$ is the set of all nonzero functions f whose support is contained in $\mathcal{P}$. Put $n = \#\mathcal{P}$. We use the obvious one-to-one correspondence between the set of divisors with support contained in $\mathcal{P}$ (we denote this set by $\mathrm{Div}_0(\mathcal{P})$) and the root lattice A_{n-1}. The set of all divisors of functions from $O_{\mathcal{P}}^*$ is a sublattice of A_{n-1} denoted by L. Now A_{n-1}/L is isomorphic to $\mathrm{Div}_0(\mathcal{P})/\mathrm{Princ}(\mathcal{P})$ where $\mathrm{Princ}(\mathcal{P})$ is the set of all principal divisors with support in $\mathcal{P}$. Thus $[A_{n-1} : L] = |\mathrm{Div}_0(\mathcal{P})/\mathrm{Princ}(\mathcal{P})|$ and it follows that

$$\mathrm{Vol}(\mathbb{R}^n/L) = \mathrm{Vol}(\mathbb{R}^n/A_{n-1})[A_{n-1} : L] = \sqrt{n}|\mathrm{Div}_0(\mathcal{P})/\mathrm{Princ}(\mathcal{P})|.$$

The group $\mathrm{Div}_0(\mathcal{P})/\mathrm{Princ}(\mathcal{P})$ is isomorphic to a subgroup of the divisor class group, and hence the volume is bounded above by $\sqrt{n}h_F$ where h_F is the class number of F.

Proposition 5.1. *The determinant of the lattice $L_{\mathcal{P}}$ is $\sqrt{q^3+1}\cdot(q+1)^{q^2-q}$.*

Proof. In the case of Hermitian function fields, the divisor classes $P - Q$ modulo $\mathrm{Princ}(\mathcal{P})$, where $P, Q \in \mathcal{P}$, generate the group $\mathrm{Div}_0(\mathcal{P})/\mathrm{Princ}(\mathcal{P})$ (see [6]). Thus the group $\mathrm{Div}_0(\mathcal{P})/\mathrm{Princ}(\mathcal{P})$ is isomorphic to the divisor class group of the Hermitian function field. The class group of the Hermitian function field is isomorphic to $\mathbb{Z}_{q+1}^{q^2-q}$, and so the class number is $(q+1)^{q^2-q}$. Since $n = q^3+1$, the result follows from the discussion above. □

6. The lattice $L_{\mathcal{P}}$ is generated by its minimal vectors

From Lemma 3.1 and Theorem 4.1 we infer the following lemma.

Lemma 6.1. *If f_1 and f_2 are two distinct lines then (f_1/f_2) (or (f_2/f_1)) is a minimal vector if one of the following holds:*

- *f_1 and f_2 are of the form $x-\alpha$,*
- *one of f_1, f_2 is of the form $x-\alpha$ and the other is a non-tangent line (of the form $y+bx+c$) and the lines have exactly one point of intersection,*
- *both f_1 and f_2 are non-tangent lines (of the form $y+bx+c$) with a point of intersection which lies in $\mathcal{K}$.*

G. Hiss [7] showed that every function in $\mathcal{O}_{\mathcal{P}}^*$ is the product of functions of the form $ax+by+c$ and their inverses. This fact is essential in the proof of the next result.

Theorem 6.2. *The lattice $L_{\mathcal{P}}$ is generated by the minimal vectors and is hence well-rounded.*

Proof. Since the lattice is generated by the divisors of the lines [7], it suffices to show that every such divisor is an integer linear combination of minimal vectors of the lattice. We call a line $f=ax+by+c$ *good* if the divisor of f is an integer linear combination of minimal vectors. Thus our goal is to show that all lines are good. We consider different cases. Throughout the proof, $\zeta\in\mathbb{F}_{q^2}$ denotes a primitive $(q+1)$st root of unity.

Case 1: Suppose that $d,e\in\mathbb{F}_{q^2}$ satisfy $d^q+d=e^{q+1}$ with $e\neq 0$. We show that the lines $y-d$ and $x-e$ are good. Let $d_1=d,d_2,\dots,d_q$ be all the solutions to $y^q+y=e^{q+1}$. Then

$$\prod_{i=1}^{q}(y-d_i)=y^q+y-e^{q+1}=x^{q+1}-e^{q+1}=\prod_{i=0}^{q}(x-\zeta^i e).$$

It follows that

$$x-e=\prod_{i=1}^{q}\left(\frac{y-d_i}{x-\zeta^i e}\right).$$

The lines $y-d_i$ and $x-e\zeta^i$ have just one point of intersection and $y-d_i$ is a non-tangent line (since d_i has nonzero trace). So by Lemma 6.1 it follows that the lattice vector corresponding to the function $\frac{y-d_i}{x-\zeta^i e}$ is a minimal vector. Since the divisor of $x-e$ is the sum of the divisors of the functions $\frac{y-d_i}{x-\zeta^i e}$, $1\le i\le q$, we arrive at the conclusion that the line $x-e$ is good.

On the other hand, we also have

$$y - d = (x - e)(x - e\zeta) \prod_{i=2}^{q} \left(\frac{x - e\zeta^i}{y - d_i} \right).$$

Since each factor on the right corresponds to a lattice vector which is either a minimal vector or which can be expressed as a linear combination of minimal vectors, it follows that the line $y - d$ is good.

Case 2: We show that every non-tangent line of the form $f = y + bx + c$ is good. Since f is a non-tangent line, we infer from Lemma 3.1 that $(-b, c) \notin \mathcal{K}$, that is, $c^q + c \neq (-b)^{q+1} = b^{q+1}$.

Let $\alpha = -b^q$, so that $b = -\alpha^q$. Note that $\alpha^{q+1} = b^{q+1}$ and let $\beta \in \mathbb{F}_{q^2}$ be any solution to $\beta^q + \beta = \alpha^{q+1}$ $(= b^{q+1})$. Then $f = y - \alpha^q x + \beta^q + c - \beta^q = \tau_{\alpha,\beta} - d$ where $d = \beta^q - c$. Observe that $d^q + d = \beta^q + \beta - (c^q + c) = b^{q+1} - (c^q + c) \neq 0$.

Choose $e \in \mathbb{F}_{q^2}$ such that $d^q + d = e^{q+1}$ (so $c^q + c = b^{q+1} - e^{q+1}$). Note that $e \neq 0$. Let $d_1 = d, d_2, \ldots, d_q \in \mathbb{F}_{q^2}$ be all the solutions to $y^q + y = e^{q+1}$. Writing τ for $\tau_{\alpha,\beta}$ we get that

$$\prod_{i=1}^{q} (\tau - d_i) = \tau^q + \tau - e^{q+1} = (x - \alpha)^{q+1} - e^{q+1} = \prod_{i=0}^{q} (x - \alpha - \zeta^i e). \tag{7}$$

It follows that

$$x - \alpha - e = \prod_{i=1}^{q} \left(\frac{\tau - d_i}{x - \alpha - \zeta^i e} \right). \tag{8}$$

Since $d_i^q + d_i = e^{q+1} = d^q + d \neq 0$, we obtain from Lemma 3.1 (c) that the lines $\tau - d_i$ are not tangent lines. The line $\tau - d_i$ intersects the line $x - \alpha - \zeta^i e$ at exactly one point: $(\alpha + \zeta^i e, \beta + d_i + e\alpha^q \zeta^i)$. Moreover, this point belongs to $\mathcal{K}$ because

$$\begin{aligned} &(\beta + d_i + e\alpha^q \zeta^i)^q + (\beta + d_i + e\alpha^q \zeta^i) \\ &\quad = \beta^q + \beta + d_i^q + d_i + e^q \alpha \zeta^{iq} + e\alpha^q \zeta^i \\ &\quad = \alpha^{q+1} + e^{q+1} + e^q \alpha \zeta^{iq} + e\alpha^q \zeta^i = (\alpha + \zeta^i e)^{q+1}. \end{aligned}$$

Thus the lattice vectors corresponding to functions $\frac{\tau - d_i}{x - \alpha - \zeta^i e}$ $(1 \leq i \leq q)$ are minimal vectors. It follows from equation (8) that the line $x - \alpha - e$ is good. Replacing e by ζe in the above argument, we see that $x - \alpha - \zeta e$ is also good. From equation (7) we get

$$f = \tau - d = (x - \alpha - e)(x - \alpha - e\zeta) \prod_{i=2}^{q} \left(\frac{x - \alpha - \zeta^i e}{\tau - d_i} \right). \tag{9}$$

Since each factor on the right corresponds to a lattice vector which is either a minimal vector or which can be expressed as a linear combination of minimal vectors, we conclude that the line f is good.

Note that Case 1 is actually implied as a special case of the proof of Case 2 with $b = 0$.

Case 3: We prove that the tangent line $\tau_{0,0} = y$ is good. First of all observe that

$$y^{q+1} - x^{q+1} = y^{q+1} - y^q - y = (y-1)^{q+1} - 1 = \prod_{i=0}^{q}(y - 1 - \zeta^i).$$

On the other hand we also have that $y^{q+1} - x^{q+1} = \prod_{i=0}^{q}(y - \zeta^i x)$, and so

$$\prod_{i=0}^{q}(y - 1 - \zeta^i) = \prod_{i=0}^{q}(y - \zeta^i x).$$

Since -1 is a $(q+1)$st root of unity, there is a unique index $j \in \{0, \dots, q\}$ such that $\zeta^j = -1$ (actually $j = 0$ in characteristic 2 and $j = (q+1)/2$ in odd characteristics). Then

$$y = (y - \zeta^j x) \prod_{i=0,\, i\neq j}^{q} \left(\frac{y - \zeta^i x}{y - 1 - \zeta^i} \right). \tag{10}$$

The points of $\mathcal{K}$ that lie on the line $y - (1+\zeta^i)$ are $((1+\zeta^i)\zeta^k, 1+\zeta^i)$ with $k = 0, 1, \dots, q$. This implies that the line $y - (1 + \zeta^i)$ (for $i \neq j$) intersects the line $y - \zeta^i x$ in exactly one point of $\mathcal{K}$, namely $((1 + \zeta^i)\zeta^{q+1-i}, 1 + \zeta^i)$. This point belongs to $\mathcal{K}$ because

$$\begin{aligned} \left((1 + \zeta^i)\zeta^{q+1-i}\right)^{q+1} &= (1 + \zeta^i)^{q+1} = (1 + \zeta^{iq})(1 + \zeta^i) \\ &= 1 + \zeta^{iq} + \zeta^i + 1 = (1 + \zeta^i)^q + (1 + \zeta^i). \end{aligned}$$

Note that the lines $y - \zeta^i x$ $(1 \leq i \leq q)$ are not tangent lines since $(\zeta^i)^{q+1} = 1 \neq 0$ and thus $(-\zeta^i, 0) \notin \mathcal{K}$.

It follows that the lattice vector corresponding to the functions $\frac{y-\zeta^i x}{y-1-\zeta^i}$ $(0 \leq i \leq q$, $i \neq j)$ is a minimal vector. As the line $y - \zeta^j x$ is not a tangent line, it is good by Case 2. It now results from (10) that the line y is good.

Case 4: For every $(\alpha, \beta) \in \mathcal{K}$, the tangent line $\tau_{\alpha,\beta} = y - \alpha^q x + \beta^q$ is good. Set $\tau := \tau_{\alpha,\beta}$ and $x_\alpha = x - \alpha$. Note that $(-\alpha, \beta^q) \in \mathcal{K}$. By [13, page 238], there exists a $\sigma \in \mathrm{Aut}(H/\mathbb{F}_{q^2})$ such that $\sigma(x) = x - \alpha$ and $\sigma(y) = y - \alpha^q x + \beta^q = \tau$. Observe that, in the notation of [13], we are using $(d, e) = (-\alpha, \beta^q)$. Applying σ to equation (10) we get

$$\tau = (\tau - \zeta^j x_\alpha) \prod_{i=0, i\neq j}^{q} \left(\frac{\tau - \zeta^i x_\alpha}{\tau - 1 - \zeta^i} \right). \tag{11}$$

Note that one could also derive this identity in the same way as in Case 3. By [13, Lemma 3.5.2], a place Q is a common zero of $\sigma(y-1-\zeta^i)$ and $\sigma(y-\zeta^i x)$ if and only if $\sigma^{-1}(Q)$ is a common zero of $y-1-\zeta^i$ and $y-\zeta^i x$. Thus, using the results from Case 3, we see that the line $\tau-1-\zeta^i=\sigma(y-1-\zeta^i)$ intersects the line $\tau-\zeta^i x_\alpha=\sigma(y-\zeta^i x)$ at exactly one point. Moreover, again by [13, Lemma 3.5.2], the lines $\tau-\zeta^i x_\alpha=\sigma(y-\zeta^i x)$ and $\tau-1-\zeta^i=\sigma(y-1-\zeta^i)$ are non-tangent lines, both of the form $y+ax+c$. Thus by Lemma 6.1, the lattice vectors corresponding to the functions $\frac{\tau-\zeta^i x_\alpha}{\tau-1-\zeta^i}$ $(0\le i\le q,\ i\ne j)$ are all minimal. Since the line $\tau-\zeta^j x_\alpha$ is good, it follows from equation (11) that the line τ is good as well.

Case 5: We finally show that the line x is good. We start with the observation that

$$y^q+y-(x^q+x)=x^{q+1}-x^q-x=(x-1)^{q+1}-1=\prod_{i=0}^{q}(x-1-\zeta^i).$$

On the other hand,

$$y^q+y-(x^q+x)=(y-x)^q+(y-x)=\prod_{i=1}^{q}(y-x-\rho_i),$$

where $\rho_1,\dots,\rho_q\in\mathbb{F}_{q^2}$ are all the solutions to $\rho^q+\rho=0$. Thus

$$\prod_{i=0}^{q}x-1-\zeta^i=\prod_{i=1}^{q}(y-x-\rho_i). \tag{12}$$

Let $z_1,z_2,\dots,z_q$ be a renumbering of $1+\zeta^0,1+\zeta^1,\dots,1+\zeta^{j-1},1+\zeta^{j+1},\dots,1+\zeta^q$ (recall that $\zeta^j=-1$). Then it follows from equation (12) that

$$x=\prod_{i=1}^{q}\left(\frac{y-x-\rho_i}{x-z_i}\right). \tag{13}$$

Observe that the two lines $x-(1+\zeta^m)$ and $y-x-\rho_i$ intersect at the point $(1+\zeta^m,1+\zeta^m+\rho_i)$. Moreover the point $(1+\zeta^m,1+\zeta^m+\rho_i)$ belongs to $\mathcal{K}$ since

$$(1+\zeta^m+\rho_i)^q+(1+\zeta^m+\rho_i)=\rho_i+\rho_i^q+1+\zeta^{mq}+1+\zeta^m=(1+\zeta^m)^{q+1}.$$

The line $y-x-\rho_i$ is a non-tangent line because $(1,-\rho_i)\notin\mathcal{K}$. Thus, by Lemma 6.1, the lattice vector corresponding to the function $\frac{y-x-\rho_i}{x-z_i}$ is a minimal vector. It therefore follows from equation (13) that the line x is good. □

7. Automorphism groups of lattices

In this section we discuss automorphisms of lattices coming from generating sets in Abelian groups and specifically address the case of Hermitian and other curves.

7.1. Lattices from Abelian groups

Let $G = \{g_0, g_1, \ldots, g_{n-1}, \ldots, g_{N-1}\}$ be an Abelian group with $g_0 = 0$, and let $S = \{g_0, g_1, \ldots, g_{n-1}\}$ be a subset of G. Put

$$L_G = \left\{ \left(x_1, \ldots, x_{N-1}, -\sum_{i=1}^{N-1} x_i \right) : x_1, \ldots, x_{N-1} \in \mathbb{Z},\ \sum_{i=1}^{N-1} x_i g_i = 0 \right\} \subseteq A_{N-1}$$

and

$$L_G(S) = \left\{ \left(x_1, \ldots, x_{n-1}, -\sum_{i=1}^{n-1} x_i \right) : x_1, \ldots, x_{n-1} \in \mathbb{Z},\ \sum_{i=1}^{n-1} x_i g_i = 0 \right\} \subseteq A_{n-1}.$$

Hence L_G and $L_G(S)$ are full-rank sublattices of the root lattices A_{N-1} and A_{n-1}, respectively. We denote the vectors in $L_G(S)$ by $X = \left(x, -\sum_{i=1}^{n-1} x_i\right)$ with $x = (x_1, \ldots, x_{n-1})$ in $\mathbb{Z}^{n-1}$. The automorphism group $\mathrm{Aut}(L_G(S))$ is defined as the group of all maps of $L_G(S)$ onto itself which extend to linear isometries of $\mathrm{span}_{\mathbb{R}} A_{n-1}$. It is easily seen that a map $\tau \in \mathrm{Aut}(L_G(S))$ is necessarily of the form

$$\tau(X) = \tau\left(x_1, \ldots, x_{n-1}, -\sum_{i=1}^{n-1} x_i \right) = \left(Ux, -\sum_{i=1}^{n-1} (Ux)_i \right),$$

where $U \in \mathrm{GL}_{n-1}(\mathbb{Z})$, since it is an automorphism of a sublattice of $\mathbb{Z}^{n-1}$. We therefore identify $\mathrm{Aut}(L_G(S))$ with a subgroup of $\mathrm{GL}_{n-1}(\mathbb{Z})$. Moreover, we identify the symmetric group S_{n-1} with the group of all permutation matrices in $\mathrm{GL}_{n-1}(\mathbb{Z})$. For the analogous notation regarding the lattice L_G, we refer to [4].

If S is a subgroup of G and $\mathrm{Aut}(S)$ denotes for the automorphism group of S, then $\mathrm{Aut}(L_G(S)) \cap S_{n-1} \cong \mathrm{Aut}(S)$ by Theorem 1.4 of [4]. More generally, if S is any subset of G, let us define

$$\mathrm{Aut}(G, S) := \{\sigma \in \mathrm{Aut}(G) : \sigma(g_i) \in S\ \forall g_i \in S\}.$$

Notice that every element of $\mathrm{Aut}(G)$ fixes 0 and permutes $g_1, \ldots, g_{N-1}$, which allows us to identify $\mathrm{Aut}(G)$ with a subgroup of S_{N-1}, the group of permutations on $N-1$ letters. Think of S_{n-1} as the subgroup of S_{N-1} consisting of all permutations of the first $n-1$ letters. Each element of $\mathrm{Aut}(G, S)$ induces a permutation of S, and hence gives rise to an element of S_{n-1}. Let us write $\mathrm{Aut}(G, S)^*$ for the group of permutations of S which are extendable to automorphisms of G. In other words, every element of $\mathrm{Aut}(G, S)^*$ is a restriction $\sigma|_S : S \to S$ of some element $\sigma \in \mathrm{Aut}(G, S)$ and every element of $\mathrm{Aut}(G, S)$ arises as an extension $\hat{\tau} : G \to G$ of some element $\tau \in \mathrm{Aut}(G, S)^*$.

Theorem 7.1. *With notation as above,* $\mathrm{Aut}(G,S)^*$ *is isomorphic to a subgroup of* $\mathrm{Aut}(L_G(S)) \cap S_{n-1}$. *If* S *is a generating set for* G, *then*

$$\mathrm{Aut}(G,S)^* \cong \mathrm{Aut}(L_G(S)) \cap S_{n-1}.$$

Proof. First notice that every element of $\mathrm{Aut}(G,S)^*$ fixes 0 and permutes the elements $g_1,\dots,g_{n-1}$. Hence $\mathrm{Aut}(G,S)^*$ can be identified with a subgroup of the symmetric group S_{n-1}. We denote this subgroup by Q. Our first objective is to construct an injective group homomorphism $\Phi : Q \to \mathrm{Aut}(L_G(S)) \cap S_{n-1}$.

Let $\sigma \in Q$. Then, for every $g_i \in S$, $\sigma(g_i) = g_{\sigma(i)}$ and $\sigma(0) = 0$. If

$$X = \left(x_1,\dots,x_{n-1},-\sum_{i=1}^{n-1} x_i\right) \in L_G(S),$$

then $\sum_{i=1}^{n-1} x_i g_i = 0$. Notice that σ^{-1} is also in Q, and so

$$0 = \sigma^{-1}(0) = \sum_{i=1}^{n-1} x_i g_{\sigma^{-1}(i)} = \sum_{i=1}^{n-1} x_{\sigma(i)} g_i.$$

Now define $\tau = \Phi(\sigma)$ on $L_G(S)$ by

$$\tau\left(x_1,\dots,x_{n-1},-\sum_{i=1}^{n-1} x_i\right) := \left(x_{\sigma(1)},\dots,x_{\sigma(n-1)},-\sum_{i=1}^{n-1} x_{\sigma(i)}\right).$$

It is clear that τ maps $L_G(S)$ onto itself. The matrix $U \in \mathrm{GL}_{n-1}(\mathbb{Z})$ corresponding to τ is obviously a permutation matrix. Consequently, τ is in $\mathrm{Aut}(L_G(S)) \cap S_{n-1}$. Finally, it is readily seen that Φ is an injective group homomorphism. Hence $\Phi(Q) \le \mathrm{Aut}(L_G(S)) \cap S_{n-1}$.

Now assume that S is a generating set for G. We will show that $\Phi(Q) = \mathrm{Aut}(L_G(S)) \cap S_{n-1}$. Indeed, let $\tau \in \mathrm{Aut}(L_G(S)) \cap S_{n-1}$. If

$$X = \left(x_1,\dots,x_{n-1},-\sum_{i=1}^{n-1} x_i\right) \in L_G(S),$$

then $\tau(X) = (x_{\sigma(1)},\dots,x_{\sigma(n-1)},-\sum_{i=1}^{n-1} x_{\sigma(i)})$ with some $\sigma \in S_{n-1}$, and since both X and $\tau(X)$ belong to $L_G(S)$, it follows that $0 = \sum_{i=1}^{n-1} x_i g_i = \sum_{i=1}^{n-1} x_{\sigma(i)} g_i$. We have $\tau = \Phi(\sigma)$ with $\sigma : S \to S$ defined by $\sigma(g_i) := g_{\sigma(i)}$ and $\sigma(0) := 0$.

To complete the proof, we only need to show that σ extends to an automorphism of G. For this, notice that every element $g \in G$ can be written as $g = \sum_{i=1}^{n-1} a_i g_i$ with $a_1,\dots,a_{n-1} \in \mathbb{Z}$, since S generates G. Then define

$$\sigma(g) := \sum_{i=1}^{n-1} a_i \sigma(g_i) = \sum_{i=1}^{n-1} a_i g_{\sigma(i)}.$$

To check that this is well-defined, suppose that $\sum_{i=1}^{n-1} a_i g_i = \sum_{i=1}^{n-1} b_i g_i$ for some integers $a_1, \dots, a_{n-1}$, $b_1, \dots, b_{n-1}$, and hence $\sum_{i=1}^{n-1}(a_i - b_i)g_i = 0$. Then

$$Y := \left(a_1 - b_1, \dots, a_{n-1} - b_{n-1}, \sum_{i=1}^{n-1}(b_i - a_i) \right) \in L_G(S),$$

and so

$$\tau^{-1}(Y) = \left(a_{\sigma^{-1}(1)} - b_{\sigma^{-1}(1)}, \dots, a_{\sigma^{-1}(n-1)} - b_{\sigma^{-1}(n-1)}, \sum_{i=1}^{n-1}(b_{\sigma^{-1}(i)} - a_{\sigma^{-1}(i)}) \right)$$

is in $L_G(S)$, meaning that $0 = \sum_{i=1}^{n-1}(b_{\sigma^{-1}(i)} - a_{\sigma^{-1}(i)})g_i = \sum_{i=1}^{n-1}(b_i - a_i)g_{\sigma(i)}$. Hence $\sum_{i=1}^{n-1} a_i g_{\sigma(i)} = \sum_{i=1}^{n-1} b_i g_{\sigma(i)}$, and so σ is well-defined.

Our definition readily implies that σ is a group homomorphism. To see that it is surjective, suppose that $g \in G$. Then $g = \sum_{i=1}^{n-1} a_i g_i$ for some $a_1, \dots, a_{n-1} \in \mathbb{Z}$. For each $1 \le i \le n-1$, $\sigma^{-1}(i) \in \{1, \dots, n-1\}$ and $\sigma^{-1}(i) \ne \sigma^{-1}(j)$ whenever $1 \le i \ne j \le n-1$, since $\sigma, \sigma^{-1} \in S_{n-1}$ are bijections. Then let $h = \sum_{i=1}^{n-1} a_i g_{\sigma^{-1}(i)}$, and notice that $\sigma(h) = g$, hence $\sigma : G \to G$ is a surjective group homomorphism. Since G is finite, infectivity of σ is implied, thus $\sigma \in \mathrm{Aut}(G)$, and so $\tau \in \Phi(Q)$. This completes the proof. □

7.2. An example

Let $G = \{0, 1, 2, 3, 4, 5, 6\} = \mathbb{Z}_7$ (:= $\mathbb{Z}/7\mathbb{Z}$). Then every subset $S \subseteq G$ containing 0 and at least one other element is a generating set of G. Let, for instance, $S = \{0, 1, 2, 4\}$, which, in the above notation, is an example of $S = \{0, g_1, \dots, g_{n-1}\}$ with $n - 1 = 3$. The lattice $L_G(S)$ is

$$\{(x_1, x_2, x_3, -(x_1 + x_2 + x_3)) \in \mathbb{Z}^4 : x_1 + 2x_2 + 4x_3 = 0 \bmod 7\} \subseteq A_3.$$

It can be checked directly that the minimal distance $d(L_G(S))$ equals $\sqrt{6}$ and that $L_G(S)$ has exactly 6 minimal vectors, the three vectors $(-2, 1, 0, 1)$, $(0, -2, 1, 1)$, $(1, 0, -2, 1)$ and their negatives. As the first three of these vectors are linearly independent, it follows that $L_G(S)$ is well-rounded. For $j = 1, \dots, 6$, we denote by $\sigma_j \in \mathrm{Aut}(G)$ the automorphism which sends 1 to j and thus k to kj modulo 7. Clearly, $\mathrm{Aut}(G) = \{\sigma_1, \dots, \sigma_6\}$. The automorphisms σ_i which leave S invariant are just $\sigma_1, \sigma_2, \sigma_4$. Consequently, $\mathrm{Aut}(G, S)^* = \{\sigma_1, \sigma_2, \sigma_4\}$ and Theorem 7.1 tells us that $\mathrm{Aut}(L_G(S)) \cap S_3 \cong \{\sigma_1, \sigma_2, \sigma_4\}$.

Table 1 below reveals what happens if S ranges over all possible proper subsets of $G = \mathbb{Z}_7$. The column of the table headed by $n - 1 = k$ shows the numbers $g_1 \dots g_k$ for the $\binom{6}{k}$ possible sets $S = \{0, g_1, \dots, g_k\}$. The lattice $L_G(S)$ is well-rounded if and only if the corresponding numbers $g_1 \dots g_k$ are in boldface. We also indicated the minimal distance of $L_G(S)$. For example, the first 8 lattices in the column $n - 1 = 3$ have the

Table 1
Well-roundedness and automorphism groups of lattices from $\mathbb{Z}_7$.

$n-1=1$	$n-1=2$	$n-1=3$	$n-1=4$	$n-1=5$
$d=\sqrt{98}$	$d=\sqrt{14}$	$d=\sqrt{6}$	$d=24$	$d=2$
$\mathbf{1}\{\sigma_1\}$	$\mathbf{13}\{\sigma_1\}$	$\mathbf{124}\{\sigma_1,\sigma_2,\sigma_4\}$	$1234\{\sigma_1\}$	$\mathbf{12\,345}\{\sigma_1\}$
$\mathbf{2}\{\sigma_1\}$	$\mathbf{15}\{\sigma_1\}$	$\mathbf{125}\{\sigma_1\}$	$1235\{\sigma_1\}$	$\mathbf{12\,346}\{\sigma_1\}$
$\mathbf{3}\{\sigma_1\}$	$\mathbf{23}\{\sigma_1\}$	$\mathbf{136}\{\sigma_1\}$	$1236\{\sigma_1\}$	$\mathbf{12\,356}\{\sigma_1\}$
$\mathbf{4}\{\sigma_1\}$	$\mathbf{26}\{\sigma_1\}$	$\mathbf{146}\{\sigma_1\}$	$1245\{\sigma_1\}$	$\mathbf{12\,456}\{\sigma_1\}$
$\mathbf{5}\{\sigma_1\}$	$\mathbf{45}\{\sigma_1\}$	$\mathbf{234}\{\sigma_1\}$	$1246\{\sigma_1\}$	$\mathbf{13\,456}\{\sigma_1\}$
$\mathbf{6}\{\sigma_1\}$	$\mathbf{46}\{\sigma_1\}$	$\mathbf{256}\{\sigma_1\}$	$1256\{\sigma_1,\sigma_6\}$	$\mathbf{23\,456}\{\sigma_1\}$
	$d=\sqrt{6}$	$\mathbf{345}\{\sigma_1\}$	$1345\{\sigma_1\}$	
	$12\{\sigma_1\}$	$\mathbf{356}\{\sigma_1,\sigma_2,\sigma_4\}$	$1346\{\sigma_1,\sigma_6\}$	
	$14\{\sigma_1\}$	$d=2$	$1356\{\sigma_1\}$	
	$16\{\sigma_1,\sigma_6\}$	$123\{\sigma_1\}$	$1456\{\sigma_1\}$	
	$24\{\sigma_1\}$	$126\{\sigma_1\}$	$2345\{\sigma_1,\sigma_6\}$	
	$25\{\sigma_1,\sigma_6\}$	$134\{\sigma_1\}$	$2346\{\sigma_1\}$	
	$34\{\sigma_1,\sigma_6\}$	$135\{\sigma_1\}$	$2356\{\sigma_1\}$	
	$35\{\sigma_1\}$	$145\{\sigma_1\}$	$2456\{\sigma_1\}$	
	$36\{\sigma_1\}$	$156\{\sigma_1\}$	$3456\{\sigma_1\}$	
	$56\{\sigma_1\}$	$235\{\sigma_1\}$		
		$236\{\sigma_1\}$		
		$245\{\sigma_1\}$		
		$246\{\sigma_1\}$		
		$346\{\sigma_1\}$		
		$456\{\sigma_1\}$		

minimal distance $\sqrt{6}$ and the remaining 12 lattices in the column $n-1=3$ have the minimal distance 2. Also added is the group $\mathrm{Aut}(G,S)^*$ in each case.

Altogether we have $62=2^6-2$ lattices. Exactly 26 of them are well-rounded and the remaining 36 lattices are not well-rounded. It is not a surprise that the group $\mathrm{Aut}(G,S)^*$ is nontrivial if the lattice is well-rounded, but it is surprising that this group may also be nontrivial for lattices which are not well-rounded.

7.3. Lattices from function fields

We use the notation of Section 1. In particular, F is an algebraic function field (of a single variable) with the finite field $\mathbb{F}_q$ as its full field of constants and $\mathcal{P}:=\{P_0,P_1,P_2,\ldots,P_{n-1}\}$ is the set of rational places of F. The automorphisms of F permute all places of a given degree and hence induce automorphisms of the lattice $L_{\mathcal{P}}$. Let $\mathrm{Inv}(\mathcal{P})$ be the set of all those automorphisms of F which act trivially on each of the places in $\mathcal{P}$. Then we may regard $\mathrm{Aut}(F)/\mathrm{Inv}(\mathcal{P})$ as a subgroup of $\mathrm{Aut}(L_{\mathcal{P}})\cap S_{n-1}$. Furthermore, each automorphism σ of the divisor class group $\mathrm{Cl}^0(F)$ which permutes the divisor classes $[P_i-P_0]$ $(1\le i\le n-1)$ also induces an automorphism of the lattice $L_{\mathcal{P}}$. First, note that we may view σ as an element of the symmetric group S_{n-1} by writing $\sigma([P_i-P_0])=[P_{\sigma(i)}-P_0]$ for $1\le i\le n-1$. Second, for every $f\in O_{\mathcal{P}}^*$, $[(f)]$ is the identity element of $\mathrm{Cl}^0(F)$ and so, if $(f)=\sum_{i=1}^{n-1}a_i(P_i-P_0)$, then $\sigma([(f)])=0$, that is, the divisor $\sum_{i=1}^{n-1}a_i(P_{\sigma(i)}-P_0)$ is again principal, or equivalently, $\sum_{i=1}^{n-1}a_i(P_{\sigma(i)}-P_0)$ corresponds to a lattice point in $L_{\mathcal{P}}$. Put $S:=\{[P_i-P_0]:0\le i\le n-1\}$. Let G be the subgroup of $\mathrm{Cl}^0(F)$ which is generated by S. Note that if F is the Hermitian function

field then $G = \mathrm{Cl}^0(F)$ (see [6]). Recall from Section 1 we have that $L_{\mathcal{P}} = L_G(S)$ and from Section 7.1 recall that $\mathrm{Aut}(G,S)^*$ is the group of all permutations of S which are extendable to automorphism of G. From Theorem 7.1 it follows that

$$\mathrm{Aut}(G,S)^* \cong \mathrm{Aut}(L_{\mathcal{P}}) \cap S_{n-1}.$$

Now let H be the Hermitian function field and let $\mathcal{P}$ be the set of rational places of H as defined in Section 1. We show that in this case the group $\mathrm{Inv}(\mathcal{P})$ is trivial. In order to do this we need the following facts about $\mathrm{Aut}(H)$ which we list for the reader's convenience:

Theorem 7.2. (See [13, page 238].)

(a) *For each pair $(d,e) \in \mathcal{K}$ there is an automorphism $\sigma \in \mathrm{Aut}(H)$ such that $\sigma(x) = x + d$ and $\sigma(y) = y + d^q x + e$. These automorphisms form a subgroup V of $\mathrm{Aut}(H)$ of order q^3.*

(b) *For each $c \in \mathbb{F}_{q^2}^{\times}$ there is an automorphism $\rho \in \mathrm{Aut}(H)$ such that $\rho(x) = cx$ and $\rho(y) = c^{q+1}y$. These automorphisms form a subgroup W of order $q^2 - 1$.*

(c) *Let U be the subgroup of $\mathrm{Aut}(H)$ generated by V and W. Then $|U| = q^3(q^2-1)$, V is a normal subgroup of U, for every $\rho \in \mathrm{Aut}(H)$ we have that $\rho \in U$ iff $\rho(Q_\infty) = Q_\infty$ and the group U acts transitively on $\{P_{\alpha,\beta} : (\alpha,\beta) \in \mathcal{K}\}$.*

The reader can check that if $(d_1,e_1),(d_2,e_2) \in \mathcal{K}$ and $\sigma_1,\sigma_2 \in V$ are the respective corresponding automorphisms as in part (a) of the theorem above, then $\sigma_1\sigma_2$ corresponds to the element $(d_1+d_2, e_1+e_2+d_2^q d_1)$ of $\mathcal{K}$, that is $\sigma_1\sigma_2(x) = x+d_1+d_2$ and $\sigma_1\sigma_2(y) = y + (d_1+d_2)^q x + e_1 + e_2 + d_2^q d_1$.

Lemma 7.3. *If H is the Hermitian function field, $\mathrm{Inv}(H)$ is trivial.*

Proof. We use the notation of Theorem 7.2 freely throughout the proof. Let $\lambda \in \mathrm{Inv}(H)$. Since $\sigma(Q_\infty) = Q_\infty$ it follows that $\lambda \in U$. From Theorem 7.2, since V is a normal subgroup of U, it follows that $\lambda = \lambda_1\lambda_2$ for some $\lambda_1 \in V$ and $\lambda_2 \in W$. Now λ_2 is the product of automorphisms of the type ρ listed in part (b) of Theorem 7.2. Thus $\lambda_2(x) = Cx$ and $\lambda_2(y) = C^{q+1}y$ for some $C \in \mathbb{F}_{q^2}^{\times}$. Also λ_1 is the product of automorphisms of the type σ listed in part (a) of Theorem 7.2. Thus $\lambda_1(x) = x + D$ for some $D \in \mathbb{F}_{q^2}$ and $\lambda_1(y) = y + D^q x + E$ for some $E \in \mathbb{F}_{q^2}$. Thus $\lambda(x) = C(x+D)$. Since $\lambda(P_{0,0}) = P_{0,0}$ it follows that $D = 0$. We also have $\lambda(y) = C^{q+1}(y + D^q x + E) = C^{q+1}(y+E)$. Again, since $\lambda(P_{0,0}) = P_{0,0}$ it follows that $E = 0$. Thus $\lambda(x) = Cx$ and $\lambda(y) = C^{q+1}y$. Since $\lambda(x-\alpha) = Cx - \alpha \in P_{\alpha,\beta}$ it follows that $C = 1$. This implies that $\lambda(x) = x$ and $\lambda(y) = y$ so λ is the trivial element of $\mathrm{Aut}(H)$ as required. □

Theorem 7.4. *Let H be a Hermitian function field. Then $\mathrm{Aut}(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(L_{\mathcal{P}}) \cap S_{n-1}$ and also to a subgroup of $\mathrm{Aut}(\mathrm{Cl}^0(H))$.*

Proof. From the discussion at the beginning of this section, we know that $\mathrm{Aut}(H)/\mathrm{Inv}(\mathcal{P})$ is isomorphic to a subgroup of $\mathrm{Aut}(L_{\mathcal{P}}) \cap S_{n-1}$. The first claim of the theorem follows from Lemma 7.3.

We write P_0 for the place Q_∞. In this proof, the remaining places of H are $P_1, P_2, \ldots, P_{n-1}$ where $n = q^3 + 1$. From the discussion above we can write G for the group $\mathrm{Cl}^0(H)$. If $\sigma \in \mathrm{Aut}(H)$, then one can define a map $\phi_\sigma : G \to G$ by $\phi_\sigma([\sum_P a_P P]) = [\sum_P a_P \sigma(P)]$. This map is well-defined: two degree zero divisor classes $D_1 := [\sum_P a_P P]$, $D_2 := [\sum_P b_P P]$ are equal if and only if $[\sum_P (a_P - b_P)P]$ is the zero divisor class, that is, for some function f, $(f) = \sum_P (a_P - b_P)P$. This is equivalent to $(\sigma(f)) = \sum_P (a_P - b_P)\sigma(P)$, that is, to $[\sum_P (a_P - b_P)\sigma(P)]$ being the zero divisor class. This is in turn tantamount to saying that $[\sum_P a_P \sigma(P)] = [\sum_P b_P \sigma(P)]$, that is $\phi_\sigma(D_1) = \phi_\sigma(D_2)$. It follows from this argument that ϕ_σ is well-defined and injective. Since G is finite, ϕ_σ is also surjective. Moreover, ϕ_σ is a group homomorphism and hence an automorphism of G. Thus we have a map $\phi : \mathrm{Aut}(H) \to \mathrm{Aut}(G)$ given by $\sigma \mapsto \phi_\sigma$. It is quickly checked that ϕ is a homomorphism.

Next we show that ϕ is injective. Suppose that ϕ_σ is trivial for some $\sigma \in \mathrm{Aut}(H)$. Then, for $1 \le i \le n$, $\phi_\sigma([P_i - P_0]) = [P_i - P_0]$, that is, $\sigma(P_i) - P_i + P_0 - \sigma(P_0)$ is principal, and thus the divisor of a function, say f_i, of degree at most 2. Since F is not the rational function field $\sigma(P_i) = P_i$ iff $\sigma(P_0) = P_0$. Suppose that $\sigma(P_i) = P_0$ and $\sigma(P_0) = P_i$ for some $1 \le i \le n$ so that $(f_i) = 2P_0 - 2P_i$ and hence the divisor class $[P_i - P_0]$ has order exactly 2. From Theorem 4.1 it follows that $q = 2$. If $P_i = P_{\alpha,\beta}$ we know that $(\tau_{\alpha,\beta}) = (q+1)(P_i - P_0) = 3(P_i - P_0)$. This contradicts that the divisor class $[P_i - P_0]$ has order 2. Thus we must have that $\sigma(P_0) = P_0$ and $\sigma(P_i) = P_i$ for $1 \le i \le n$, that is, $\sigma \in \mathrm{Inv}(H)$. From Lemma 7.3 we see that σ must the be the identity of $\mathrm{Aut}(H)$ and so the map ϕ is injective. □

Theorem 7.5. *Let* $\mathrm{Aut}(F)^*$ *be the group of all automorphisms of* F *which fix the place* P_0. *Suppose that* F *is not the rational function field. Then the group* $\mathrm{Aut}(F)^*/\mathrm{Inv}(\mathcal{P})$ *is isomorphic to a subgroup of* $\mathrm{Aut}(\mathrm{Cl}^0(F))^*$. *In particular, for the Hermitian function field* H, *the group* $\mathrm{Aut}(H)^*$ *is isomorphic to a subgroup of* $\mathrm{Aut}(\mathrm{Cl}^0(H))^*$.

Proof. First note that $\mathrm{Inv}(\mathcal{P})$ is a normal subgroup of $\mathrm{Aut}(F)^*$ so the quotient $\mathrm{Aut}(F)^*/\mathrm{Inv}(\mathcal{P})$ is well defined. Put $A = \mathrm{Aut}(F)^*$. If $\sigma \in \mathrm{Aut}(F)$, then one can define a map $\phi_\sigma : \mathrm{Cl}^0(F) \to \mathrm{Cl}^0(F)$ by $\phi_\sigma([\sum_P a_P P]) = [\sum_P a_P \sigma(P)]$. As in the proof of Theorem 7.4, this gives rise to a homomorphism $\phi : A \to \mathrm{Aut}(\mathrm{Cl}^0(F))$ via $\sigma \mapsto \phi_\sigma$. We show that the kernel of ϕ is $\mathrm{Inv}(\mathcal{P})$. Clearly $\mathrm{Inv}(\mathcal{P})$ is contained in the kernel of ϕ. Next we show the reverse inclusion. Suppose that ϕ_σ is trivial for some $\sigma \in A$. Then, for $1 \le i \le n$, $\phi_\sigma([P_i - P_0]) = [P_i - P_0]$, that is, $\sigma(P_i) - P_i$ is a principal divisor. Since F is not the rational function field, $\sigma(P_i) = P_i$ for $1 \le i \le n$. This implies that $\sigma \in \mathrm{Inv}(\mathcal{P})$.

Since $\phi_\sigma([P_i - P_0]) = [\sigma(P_i) - P_0]$ for $1 \le i \le n-1$ is a permutation of the divisor classes $[P_i - P_0]$ $(1 \le i \le n-1)$, it follows that ϕ is in fact a homomorphism from A to $\mathrm{Aut}(\mathrm{Cl}^0(F))^*$. □

In the case of the Hermitian function field, the automorphism group $\mathrm{Aut}(H)$ is well understood, see [13, page 238]. The subgroup $\mathrm{Aut}(H)^*$ is the group U in Theorem 7.2. Furthermore, the divisor class group of H is $\mathbb{Z}_{q+1}^{q^2-q}$.

8. A lower bound on the number of minimal vectors of $L_{\mathcal{P}}$

Theorem 8.1. *The lattice $L_{\mathcal{P}}$ contains at least $q^7 - q^5 + q^4 - q^2$ minimal lattice vectors.*

Proof. If $q = 2$ then H has genus 1 and so is an elliptic function field. From [5, Theorem 3.2] the number of minimal vectors of $L_{\mathcal{P}}$ in this case is exactly: $\frac{9(9-1)(9-3)}{4} = 108$ which equals $q^7 - q^5 + q^4 - q^2$. In what follows we assume that $q > 2$.

We count the number of functions of the form $f = f_1/f_2$ where f_1, f_2 are lines which satisfy the conditions given in Lemma 6.1 for (f) to be a minimal vector. We consider each of the cases listed in Lemma 6.1.

Case 1: f_1 and f_2 are of the form $x - \alpha$. There are $q^2(q^2-1)$ functions of this form.

Case 2: One of f_1, f_2 is of the form $x - \alpha$ and the other is a non-tangent line (of the form $y + ax + c$) and both lines have exactly one point of intersection. Suppose that $(a, b) \in \mathcal{K}$ is the point of intersection. Then the lines $f_1 = x - a$ and $f_2 = y - b - m(x - a)$ are two lines of the required form provided that $m \in \mathbb{F}_{q^2}$ such that $m \neq a^q$ (by Lemma 3.1). Thus there are $q^3(q^2-1)$ possibilities for f. Since the function $1/f$ gives the lattice vector $-(f)$, we obtain $2q^3(q^2-1)$ minimal lattice vectors in this way.

Case 3: Both f_1 and f_2 are non-tangent lines (of the form $y + ax + c$) with a common point of intersection. Suppose that $(a, b) \in \mathcal{K}$ is given. Then the lines $f_1 = y - b - m_1(x - a)$ and $f_2 = y - b - m_2(x - a)$ are two lines of the required form provided that m_1, m_2 are distinct elements of $\mathbb{F}_{q^2}$ neither of which is equal to a^q (by Lemma 3.1). These are $q^3(q^2-1)(q^2-2)$ possibilities for the function f.

Adding the numbers of minimal vectors obtained from each of the above cases will yield the desired result once we show that we have not double counted functions, that is, the forms f_1/f_2 above are unique. Suppose that $f_1/f_2 = f_3/f_4$ where the pairs f_1, f_2 and f_3, f_4 both satisfy the conditions of Lemma 6.1. Then $f_1 f_4 - f_2 f_3 = 0$ is a polynomial equation in x and y whose degree d in y is at most 2. Since H is not the rational function field d cannot be 1. If $d = 2$ then the polynomial $f_1 f_4 - f_2 f_3$ must be irreducible (otherwise y would have degree 1) and so q must equal to 2, since the minimal polynomial of y over $\mathbb{F}_{q^2}(x)$ had degree q. But we are assuming that $q > 2$. Thus $d \neq 2$. It follows that the functions f_i are of the form $x - a_i$ for some $a_i \in \mathbb{F}_{q^2}$. In this case the reader can easily check that $f_1 = f_3$ and $f_2 = f_4$. This completes the proof. □

Here is an alternative proof of the above result. Let $\sigma \in \mathrm{Aut}(H)$. If f_1, f_2 satisfy the conditions of Lemma 6.1 then one can check that $\sigma(f_1/f_2)$ is of the form $c \cdot f_1'/f_2'$ where f_1', f_2' are again a pair of lines which satisfy one of the conditions of Lemma 6.1 and c is a nonzero constant. Thus, if we let T be the collection of all functions of the form $c \cdot f_1/f_2$ where f_1, f_2 satisfy the conditions of Lemma 6.1 and c is a nonzero constant, then the

group $\mathrm{Aut}(H)$ acts on the set T. Let a, b be two distinct elements of $\mathbb{F}_{q^2}$. Then the function $f := (x-a)/(x-b)$ belongs to T. We show that the orbit of f under the action of $\mathrm{Aut}(H)$ has $q^2(q^2-1)(q^3+1) = q^7 - q^5 + q^4 - q^2$ elements. Let $\sigma \in \mathrm{Aut}(H)$. Then $\sigma(f) = f$ if and only if $(\sigma(x)-a)/(\sigma(x)-b) = (x-a)/(x-b)$ if and only if $\sigma(x) = x$ if and only if σ belongs to the Galois group of the extension $H/\mathbb{F}_{q^2}(x)$, which has order q. Since $|\mathrm{Aut}(H)| = q^3(q^2-1)(q^3+1)$ (see [13, page 238]), Theorem 8.1 follows. A corollary of the above argument is that the group $\mathrm{Aut}(H)$ acts transitively on the set T.

Acknowledgment

We sincerely thank the referee for the outstanding care devoted to the manuscript and for the many corrections and suggestions, which have improved the paper considerably.

References

[1] E. Bayer-Fluckiger, Lattices and number fields, Contemp. Math. 241 (1999) 69–84.
[2] E. Bayer-Fluckiger, Ideal lattices, in: A Panorama of Number Theory or the View from Baker's Garden, Zürich, 1999, Cambridge Univ. Press, Cambridge, 2002, pp. 168–184.
[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997) 235–265.
[4] A. Böttcher, L. Fukshansky, S.R. Garcia, H. Maharaj, On lattices generated by finite Abelian groups, SIAM J. Discrete Math. 29 (2015) 382–404.
[5] L. Fukshansky, H. Maharaj, Lattices from elliptic curves over finite fields, Finite Fields Appl. 28 (2014) 67–78.
[6] F. Hess, Computing relations in divisor class groups of algebraic curves over finite fields, J. Symbolic Comput. (2015), submitted for publication.
[7] G. Hiss, Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups, Indag. Math. (N.S.) 15 (2004) 223–243.
[8] V. Lyubashevsky, D. Micciancio, Generalized compact knapsacks are collision resistant, in: Automata, Languages and Programming, Part II, in: Lecture Notes in Comput. Sci., vol. 4052, Springer-Verlag, Berlin, 2006, pp. 144–155.
[9] J. Martinet, Perfect Lattices in Euclidean Spaces, Springer-Verlag, Berlin, 2003.
[10] M.Y. Rosenbloom, M.A. Tsfasman, Multiplicative lattices in global fields, Invent. Math. 101 (1990) 687–696.
[11] H.-G. Rück, A note on elliptic curves over finite fields, Math. Comp. 49 (1987) 301–304.
[12] M. Sha, On the lattices from elliptic curves over finite fields, Finite Fields Appl. 31 (2015) 84–107.
[13] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd edition, Springer, Berlin, 2009.
[14] M.A. Tsfasman, S.G. Vladut, Algebraic–Geometric Codes, Kluwer Academic Publishers, Dordrecht, 1991.