7-1-2014

Lattices from Elliptic Curves over Finite Fields

Lenny Fukshansky
Claremont McKenna College

Hiren Maharaj
Clemson University

LATTICES FROM ELLIPTIC CURVES OVER FINITE FIELDS

LENNY FUKSHANSKY AND HIREN MAHARAJ

Abstract. In their well known book [6] Tsfasman and Vladut introduced a construction of a family of *function field lattices* from algebraic curves over finite fields, which have asymptotically good packing density in high dimensions. In this paper we study geometric properties of lattices from this construction applied to elliptic curves. In particular, we determine the generating sets, conditions for well-roundedness and a formula for the number of minimal vectors. We also prove a bound on the covering radii of these lattices, which improves on the standard inequalities.

1. Introduction

Let $L \subset \mathbb{R}^n$ be a lattice of rank $k \leq n$, and let $V = \text{span}_{\mathbb{R}} L$ be the k-dimensional subspace of $\mathbb{R}^n$ spanned by L. The *minimum distance* of L is

$$d(L) = \min\{\|\mathbf{x}\| : \mathbf{x} \in L\},$$

where $\| \ \|$ is the usual Euclidean norm in $\mathbb{R}^n$. The *lattice (sphere) packing* in V associated to L is the arrangement of balls of radius $d(L)/2$ centered at points of L, and the *density* $\Delta(L)$ of such packing is the proportion of V taken up by this arrangement, i.e.

$$\Delta(L) = \frac{\omega_k d(L)^k}{2^k \det L}, \tag{1}$$

where $\omega_k = \frac{\pi^{\frac{k}{2}}}{\Gamma(\frac{k}{2}+1)}$ is the volume of a k-dimensional unit ball. Given a k-dimensional subspace V of $\mathbb{R}^n$, the lattice packing problem in V is to find a lattice $L \subset V$ such that $V = \text{span}_{\mathbb{R}} L$ and $\Delta(L)$ is maximal among all lattice packing densities in V. It is easy to see that the lattice packing density problem in V is equivalent to this problem in $\mathbb{R}^k$, where we denote the maximal lattice packing density achieved by Δ_k. The values of Δ_n are currently only known for dimensions $1 \leq n \leq 8$ [2] and $n = 24$ [1] with explicit constructions of lattices achieving these densities. More generally, the famous Minkowski-Hlawka theorem states that in every dimension n there exists a lattice whose packing density is $\geq \zeta(n)/2^{n-1}$, where ζ stands for the Riemann zeta-function. Unfortunately, the known proofs of Minkowski-Hlawka theorem are non-constructive, and for arbitrary dimensions constructions of lattices satisfying this bound are not known. On the other hand, the mere existence of this bound motivated various constructions of asymptotic families of lattices, one in every dimension, whose packing density comes as close as possible to Minkowski-Hlawka. One such family, which produces particularly nice results as $n \to \infty$ are

2010 *Mathematics Subject Classification.* Primary: 11H06, 11G20.

Key words and phrases. function fields, elliptic curves, well-rounded lattices.

The first author was partially supported by NSA Young Investigator Grant #1210223 and Simons Foundation grants #208969, 279155.

the so-called *function field lattices*, constructed by Tsfasman and Vladut (see [6], pp. 578–583).

We use notation of [5]. The construction of function field lattices given in [6] 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. Let $\mathcal{P} = \{P_0, P_1, P_2, \dots, P_{n-1}\}$ be the set of rational places of F. Corresponding to 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 let

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

Define the homomorphism $\phi_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}}^* \to \mathbb{Z}^n$ (here $n = |\mathcal{P}|$, the number of rational places of F) by

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

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

$$A_{n-1} = \left\{ \mathbf{x} \in \mathbb{Z}^n : \sum_{i=0}^{n-1} x_i = 0 \right\}$$

with minimum distance

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

and

$$\det L_{\mathcal{P}} \leq \sqrt{n} h_F \leq \sqrt{n}\left(1 + q + \frac{n-q-1}{g}\right)^g, \tag{3}$$

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 $\text{Cl}^0(F)$. Here, as in [6], we can identify $\mathbb{Z}^n$ with the set of all divisors with support in $\mathcal{P}$ and A_{n-1} with all such divisors of degree 0. We will often make use of this identification when working with lattice vectors by working with the corresponding divisors instead.

Equation (1) above indicates that to maximize the packing density one should take a lattice with the quotient of minimum distance to the determinant as large as possible. In the Tsfasman-Vladut construction above, this can be achieved when the quotient n/g is relatively large, as indicated in [6]. In particular, Tsfasman and Vladut consider families of curves for which the packing density of the corresponding lattices is asymptotically good as n grows. On the other hand, it is well known (see, for instance [4]) that lattices in $\mathbb{R}^n$ with particularly high packing density are usually *well-rounded*, i.e., their sets of minimal nonzero vectors (with respect to Euclidean norm) contain n linearly independent ones. This observation prompted us to ask the following natural question.

Question 1.1. *For which algebraic function fields F is the corresponding lattice $L_{\mathcal{P}}$ well-rounded?*

The main goal of this note is to provide the following partial answer to this question.

Theorem 1.2. *Let F be an algebraic function field over $\mathbb{F}_q$ with $g = 1$ and $n \geq 5$. Then the corresponding lattice $L_{\mathcal{P}}$ is generated by its minimal vectors, and hence well-rounded.*

We also investigate a variety of geometric properties of the lattice $L_{\mathcal{P}}$ when F has genus 1, i.e., when the underlying curve is elliptic, in particular establishing formulas for the minimum distance (Lemma 3.1) and the number of minimal vectors (Theorem 3.2) of $L_{\mathcal{P}}$, and conclude with a non-trivial bound on the covering radii of such lattices (Theorem 3.4). In Section 2 we set the notation and prove several preliminary lemmas on elliptic curves and corresponding function fields, in particular obtaining an explicit description for a generating set of the lattice $L_{\mathcal{P}}$ in the case of elliptic curves (Theorem 2.3). We then prove our main results in Section 3. We are now ready to proceed.

2. Notation and preliminary results

In this section we establish some necessary preliminaries on elliptic curves. An elliptic curve is a pair (E, O), where E is a curve of genus 1 and $O \in E$. In this paper, the elliptic curves are always defined over a finite field $K := \mathbb{F}_q$. It can be shown [5, Proposition 6.1.2] that if $\mathrm{char}(K) \neq 2$ then $K(E) = K(x, y)$, where $y^2 = f(x)$ and $f(x) \in K[x]$ is square-free of degree three, and if $\mathrm{char}(K) = 2$ then $K(E) = K(x, y)$, where either $y^2 + y = f(x)$ (here $f(x) \in K[x]$ has degree 3) or $y^2 + y = x + \frac{1}{ax+b}$ with $a, b \in K$ and $a \neq 0$.

Let $\mathcal{P}$ denote the set of places of $K(E)$ of degree 1. There is a unique common pole of x and y which we denote by Q_∞. This place has degree 1 and so belongs to $\mathcal{P}$. Define the map

$$\Phi : \mathcal{P} \to \mathrm{Cl}^0(E)$$

by $\Phi(P) = [P - Q_\infty]$. This map [5, Proposition 6.1.7] is a bijection and induces an (abelian) group structure on $\mathcal{P}$: $P \oplus Q = \Phi^{-1}(\Phi(P) + \Phi(Q))$. The place Q_∞ is the identity element of this group. It follows that if P and Q are rational places, then $P - Q$ is a principal divisor if and only if $P = Q$. Thus the Riemann-Roch space $\mathcal{L}(P - Q)$ has positive dimension if and only if $P = Q$.

We need to distinguish between the operations of the group of divisors and the elliptic curve group law; and we also need to distinguish between places and their corresponding points on the elliptic curve. We do so as follows. Each place P of $K(E)$ corresponds to a unique point on the elliptic curve defined by any one of the above given equations. We denote the corresponding point in bold font $\mathbf{P}$. Thus the sum $P + Q$ is a divisor of the function field $K(E)$ while the sum $\mathbf{P} + \mathbf{Q}$ is really another point on E according to the elliptic curve group law. Henceforth we assume that $K(E) = K(x, y)$ where x and y are related by any one of the defining equations above for an elliptic curve.

Suppose the degree 1 places of $K(E)$ are $P_0, P_1, P_2, \ldots, P_{n-1}$ where $P_0 := Q_\infty$ is the unique common pole of x and y. In accordance with the notation introduced above, $\mathcal{P}$ denotes the set of places $P_0, P_1, \ldots, P_{n-1}$. For a place P, we denote by P' the place of $K(E)$ corresponding to the additive inverse of $\mathbf{P}$ (so $\mathbf{P} + \mathbf{P}' = \mathbf{Q}_\infty$). Note that $x(\mathbf{P}) = x(\mathbf{P}')$.

We define $m(\mathbf{P}, \mathbf{Q})$ to be the line through $\mathbf{P}$ and $\mathbf{Q}$ if both $P, Q \neq Q_\infty$, that is $m(\mathbf{P}, \mathbf{Q}) = ax + by + c$ for some $a, b, c \in \mathbb{F}_q$ and the points $\mathbf{P}, \mathbf{Q}$ lie on this line. Note that if $Q = P$ $(\neq Q_\infty)$ then $m(\mathbf{P}, \mathbf{Q})$ is the tangent line to E at the point $\mathbf{P}$. If $Q = P'$ $(\neq Q_\infty)$ then $m(\mathbf{P}, \mathbf{Q}) = x - x(\mathbf{P}) = x - x(\mathbf{Q})$. If $P = Q_\infty$ or $Q = Q_\infty$ then we define $m(\mathbf{P}, \mathbf{Q}) := 1 \in \mathbb{F}_q$.

If $P \neq Q_\infty$ and $Q \neq Q_\infty$ and $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ then it is well known that $m(P,Q)$ has three points of intersection with the elliptic curve and thus

$$(m(\mathbf{P},\mathbf{Q})) = P + Q + R' - 3Q_\infty.$$

Here it is possible that $R' = Q_\infty$, in which case $Q = P'$. If $Q = P'$, then

$$m(\mathbf{P},\mathbf{Q}) = x - x(\mathbf{P}) = x - x(\mathbf{Q})$$

and

$$(m(\mathbf{P},\mathbf{Q})) = P + P' - 2Q_\infty.$$

Thus, if $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ and $R \neq Q_\infty$, it follows that

$$\left(\frac{m(\mathbf{P},\mathbf{Q})}{x - x(\mathbf{R})}\right) = P + Q - R - Q_\infty.$$

Suppose that $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. Then we define the following function:

$$F(\mathbf{P},\mathbf{Q}) := \begin{cases} \frac{x - x(\mathbf{R})}{m(\mathbf{P},\mathbf{Q})} & \text{if } \mathbf{P},\mathbf{Q},\mathbf{R} \neq \mathbf{Q}_\infty \\ \frac{1}{m(\mathbf{P},\mathbf{Q})} & \text{if } \mathbf{P},\mathbf{Q} \neq \mathbf{Q}_\infty \text{ but } \mathbf{R} = \mathbf{Q}_\infty \\ 1 & \text{if } \mathbf{P} = \mathbf{Q}_\infty \text{ or } \mathbf{Q} = \mathbf{Q}_\infty. \end{cases}$$

One easily checks in all three cases the divisor of $F(\mathbf{P},\mathbf{Q})$ is

$$(F(\mathbf{P},\mathbf{Q})) = -P - Q + R + Q_\infty.$$

We repeatedly use the result that if D is a divisor and f a function in an algebraic function field, then $f\mathcal{L}(D) = \mathcal{L}(D - (f))$.

Proposition 2.1. *Let P, Q be rational places of $K(E)$. Then for a rational place R of $K(E)$, $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ if and only if $\mathcal{L}(P + Q - R - Q_\infty) \neq 0$, in which case*

$$\mathcal{L}(P + Q - R - Q_\infty) = \mathrm{span}_{\mathrm{K}}(F(\mathbf{P},\mathbf{Q})).$$

PROOF: The forward implication is obvious. For the reverse implication, let R be a rational place of $K(E)$ and suppose that

$$\mathcal{L}(P + Q - R - Q_\infty) \neq 0.$$

We need to show that $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. First suppose that $P, Q \neq Q_\infty$, then

$$\frac{1}{F(\mathbf{P},\mathbf{Q})}\mathcal{L}(P + Q - R - Q_\infty) = \mathcal{L}(S - R),$$

where $\mathbf{S}$ is the additive inverse of the third point of intersection of the line $m(\mathbf{P},\mathbf{Q})$ with the elliptic curve E (it may happen that $S = Q_\infty$). Since $\mathcal{L}(S-R)$ has positive dimension, it follows that $R = S$ and $\mathcal{L}(S - R) = \mathbb{F}_q$ so that

$$\mathcal{L}(P + Q - R - Q_\infty) = \mathrm{span}_{\mathrm{K}}(F(\mathbf{P},\mathbf{Q})).$$

If $P = Q_\infty$, then $\mathbf{P} + \mathbf{Q} = \mathbf{Q}$ and $\mathcal{L}(P + Q - R - Q_\infty) = \mathcal{L}(Q - R)$ is nontrivial by assumption and it follows that $R = Q$ so $\mathbf{R} = \mathbf{P} + \mathbf{Q}$ and $\mathcal{L}(P + Q - R - Q_\infty) = \mathrm{span}_{\mathrm{K}}\{1\} = \mathrm{span}_{\mathrm{K}}(F(\mathbf{P},\mathbf{Q}))$.

Likewise, the reverse implication is true if $\mathbf{Q} = \mathbf{Q}_\infty$. □

Theorem 2.2. *For an integer $n \geq 1$, $n\mathbf{P} = \mathbf{Q}_\infty$ if and only if*

$$\mathcal{L}(nP - nQ_\infty) = \mathrm{span}_{\mathrm{K}}\{F(\mathbf{P},\mathbf{P})F(\mathbf{P},2\mathbf{P})\dots F(\mathbf{P},(n-1)\mathbf{P})\}.$$

PROOF: For $n = 1$ this result is trivial so we assume that $n > 1$. For $k \geq 1$, we put $\mathbf{P}_k := k\mathbf{P}$. Observe that for $k \geq 2$, $\mathbf{P} + \mathbf{P}_{k-1} = \mathbf{P}_k$, and so

$$\mathcal{L}(P + P_{k-1} - P_k - Q_\infty) = \mathrm{span}_{\mathrm{K}}\{F(\mathbf{P}, \mathbf{P}_{k-1})\}.$$

We will use this fact repeatedly. Suppose that $n\mathbf{P} = \mathbf{Q}_\infty$. Then $\mathbf{P} + \mathbf{P}_{n-1} = \mathbf{Q}_\infty$, whence

$$\mathcal{L}(P + P_{n-1} - 2Q_\infty) = \mathrm{span}_{\mathrm{K}}\{F(\mathbf{P}, \mathbf{P}_{n-1})\}.$$

Since $\mathbf{P} + \mathbf{P}_{n-i-1} = \mathbf{P}_{n-i}$ for $i = 1, 3, \ldots n-2$, the following identities are true:

$$\begin{aligned}
\mathcal{L}(P + P_{n-2} - P_{n-1} - Q_\infty) &= \mathrm{span}_{\mathrm{K}}\{F(\mathbf{P}, \mathbf{P}_{n-2})\} \\
\mathcal{L}(P + P_{n-3} - P_{n-2} - Q_\infty) &= \mathrm{span}_{\mathrm{K}}\{F(\mathbf{P}, \mathbf{P}_{n-3})\} \\
&\vdots \\
\mathcal{L}(P + P - P_2 - Q_\infty) &= \mathrm{span}_{\mathrm{K}}\{F(\mathbf{P}, \mathbf{P})\}.
\end{aligned}$$

Notice that if $\mathcal{L}(D_1) = \mathrm{span}_{\mathrm{K}}\{f_1\}$ and $\mathcal{L}(D_2) = \mathrm{span}_{\mathrm{K}}\{f_2\}$ then $\mathcal{L}(D_1 + D_2) = \mathrm{span}_{\mathrm{K}}\{f_1 f_2\}$. Combining this observation with the above identities, we obtain

$$\mathcal{L}(nP - nQ_\infty) = \mathrm{span}_{\mathrm{K}}\{F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, \mathbf{P}_2) \ldots F(\mathbf{P}, \mathbf{P}_{n-1})\}. \tag{4}$$

On the other hand, assume that (4) holds. Since the divisor of

$$F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, \mathbf{P}_2) \ldots F(\mathbf{P}, \mathbf{P}_{n-2})$$

is

$$\begin{aligned}
(-P - P + P_2 + Q_\infty) + (-P - P_2 + P_3 + Q_\infty) \\
+ \ldots + (-P - P_{n-2} + P_{n-1} + Q_\infty) \\
= -(n-1)P + P_{n-1} + (n-2)Q_\infty,
\end{aligned}$$

we have that

$$\frac{1}{F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, \mathbf{P}_2) \ldots F(\mathbf{P}, \mathbf{P}_{n-2})} \mathcal{L}(nP - nQ_\infty) = \mathcal{L}(P + P_{n-1} - 2Q_\infty)$$

is nontrivial. By Proposition 2.1 it follows that $\mathbf{P} + \mathbf{P}_{n-1} = \mathbf{Q}_\infty$, that is, $n\mathbf{P} = \mathbf{Q}_\infty$, as required. □

Theorem 2.3. *Let*

$$D := rQ_\infty + \sum_{i=1}^{n-1} a_i P_i$$

be a divisor of degree 0. *Then D is principal if and only if*

$$\sum_{i=1}^{n-1} a_i \mathbf{P}_i = \mathbf{Q}_\infty.$$

If D is principal, then $D = (f)$, where f is the product of functions of the form $F(\mathbf{P}, \mathbf{Q})$ with $P, Q \in \mathcal{P}$. The group $\mathcal{O}_{\mathcal{P}}^*$ is generated by the functions $F(\mathbf{P}, \mathbf{Q})$ where $\mathbf{P}, \mathbf{Q} \in \mathcal{P}$. Consequently, the lattice $L_{\mathcal{P}}$ is generated by vectors of the form $P + Q - R - Q_\infty$ where $\mathbf{P} + \mathbf{Q} = \mathbf{R}$.

PROOF: We can assume without loss of generality that $a_i \geq 0$ for $1 \leq i \leq n-1$. Indeed, for a place $P \in \mathcal{P}$ and integer $k \geq 2$, let

$$T_k(\mathbf{P}) := F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, 2\mathbf{P}) \dots F(\mathbf{P}, (k-1)\mathbf{P}).$$

Suppose that $a_j < 0$ and let k_j be the order of the point $\mathbf{P}_j$. By Theorem 2.2, the divisor of $T_{k_j}(P_j)$ is $-k_jP_j + k_jQ_\infty$. Therefore

$$\left(\frac{1}{T_{k_j}(\mathbf{P}_j)}\right)^\ell \mathcal{L}(D) = \mathcal{L}(D'),$$

where

$$D' := (r - \ell k_j)Q_\infty + \sum_{i=1, i\neq j}^{n-1} a_iP_i + (a_j + \ell k_j)P_j$$

and $a_j + \ell k_j \geq 0$ for sufficiently large ℓ. Moreover, D' is a principal divisor if and only if D is a principal divisor and

$$\sum_{i=1, i\neq j}^{n-1} a_i\mathbf{P}_i + (a_j + \ell k_j)\mathbf{P}_j = \sum_{i=1}^{n-1} a_i\mathbf{P}_i.$$

Now write

$$D = rQ_\infty + Q_1 + Q_2 + \ldots + Q_t,$$

where repetitions among the Q_i's are allowed and $t = -r$. Put

$$S_i := Q_{t-i} + Q_{t-i+1} + \ldots + Q_t, \quad \mathbf{T}_i := \mathbf{Q}_{t-i} + \mathbf{Q}_{t-i+1} + \ldots + \mathbf{Q}_t.$$

In accordance with the notation above, T_i is the place corresponding to the point $\mathbf{T}_i$. Put

$$f := F(\mathbf{Q}_{t-1}, \mathbf{Q}_t)F(\mathbf{Q}_{t-2}, \mathbf{T}_1)F(\mathbf{Q}_{t-3}, \mathbf{T}_2) \dots F(\mathbf{Q}_1, \mathbf{T}_{t-2}).$$

We claim that

$$\frac{1}{f}\mathcal{L}(D) = \mathcal{L}(-Q_\infty + T_{t-1}).$$

This follows from the fact that the divisor of the function $\frac{1}{f}$ is

$$\begin{aligned} & (Q_{t-1} + Q_t - T_1 - Q_\infty) + (Q_{t-2} + T_1 - T_2 - Q_\infty) \\ + \quad & (Q_{t-3} + T_2 - T_3 - Q_\infty) + \ldots + (Q_1 + T_{t-2} - T_{t-1} - Q_\infty) \\ = \quad & Q_t + Q_{t-1} + ... + Q_1 - T_{t-1} - (t-1)Q_\infty, \end{aligned}$$

and

$$D - (1/f) = -Q_\infty + T_{t-1}.$$

The result now follows, since the divisor $-Q_\infty + T_{t-1}$ is principal if and only if $\mathbf{T}_{t-1} = \mathbf{Q}_\infty$, that is, $\mathbf{Q}_1 + \mathbf{Q}_2 + \ldots + \mathbf{Q}_t = \mathbf{Q}_\infty$. Furthermore, $-Q_\infty + T_{t-1}$ is principal if and only if $\frac{1}{f}\mathcal{L}(D) = \mathcal{L}(-Q_\infty + T_{t-1}) = \mathrm{span}_{\mathrm{K}}\{1\}$, that is, $\mathcal{L}(D) = \mathrm{span}_{\mathrm{K}}\{f\}$.

The remaining statement of the theorem now follows quickly. Note that each function $F(\mathbf{P}, \mathbf{Q})$ has its support in $\mathcal{P}$, that is $F(\mathbf{P}, \mathbf{Q}) \in \mathcal{O}_\mathcal{P}^*$. Further observe that the set $\mathcal{O}_\mathcal{P}^*$ is the union of all $\mathcal{L}(D) \setminus \{0\}$ where D runs over all principal divisors with support in $\mathcal{P}$. From the above, we see that $\mathcal{L}(D)$ is the span of products of functions of the form $F(\mathbf{P}, \mathbf{Q})$ where $P, Q \in \mathcal{P}$. This completes the proof. $\square$

3. Lattices from elliptic curves

We are now ready to prove our main results. We first establish an explicit value for the minimum distance of the lattice $L_{\mathcal{P}}$ in case of elliptic curves.

Lemma 3.1. *Suppose that $n \geq 4$. Then the minimum distance of $L_{\mathcal{P}}$ is 2 and the minimal vectors of $L_{\mathcal{P}}$ are of the form $P + Q - R - S$ where $P, Q, R, S \in \mathcal{P}$ are distinct and $\mathbf{P} + \mathbf{Q} = \mathbf{R} + \mathbf{S}$. If $n = 3$ then the minimum distance of $L_{\mathcal{P}}$ is $\sqrt{6}$ and the minimal vectors are of the form $\pm(P + Q - 2Q_\infty)$, $\pm(P - 2Q + Q_\infty)$ and $\pm(-2P + Q + Q1_\infty$ where $\mathcal{P} = \{P, Q, Q_\infty\}$.*

Proof: Since a divisor $P - Q$ is principal if and only if $P = Q$, it follows that $\deg f \neq 1$ for any $f \in K(E)$. First assume that $n \geq 4$. Then there are two distinct points $\mathbf{P}, \mathbf{Q}$, both not equal to $\mathbf{Q}_\infty$, such that $\mathbf{P} \neq \mathbf{Q}'$. Hence $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ where $\mathbf{R} \neq \mathbf{P}, \mathbf{Q}, \mathbf{Q}_\infty$. The divisor of the function $F(\mathbf{P}, \mathbf{Q})$ is $-P - Q + R + Q_\infty$, so $d(L_{\mathcal{P}}) \leq 2$. On the other hand, (2) guarantees that $d(L_{\mathcal{P}}) \geq 2$. Thus $d(L_{\mathcal{P}}) = 2$.

Now consider a minimal vector v of $L_{\mathcal{P}}$. Then v must be of the form $P+Q-R-S$ where P, Q, R, S are distinct rational places. Note also that $P + Q - R - S$ is a principal divisor. Suppose that $\mathbf{P} + \mathbf{Q} = \mathbf{R}_1$. Then $P + Q - R_1 - Q_\infty$ is a principal divisor and so is $(P + Q - R_1 - Q_\infty) - (P + Q - R - S) = R + S - R_1 - Q_\infty$. From Proposition 2.1 we see that $\mathbf{R} + \mathbf{S} = \mathbf{R}_1$. Thus the minimal vectors of $L_{\mathcal{P}}$ are of the form $P + Q - R - S$ where $P, Q, R, S \in \mathcal{P}$ are distinct and $\mathbf{P} + \mathbf{Q} = \mathbf{R} + \mathbf{S}$.

Next assume that $n = 3$. Then $\mathcal{P} = \{Q_\infty, P, Q\}$ where $\mathbf{Q} = 2\mathbf{P}$. The following are vectors of $L_{\mathcal{P}}$: $3P - 3Q_\infty$, $3Q - 3Q_\infty$, $2P - Q - Q_\infty$, $P - 2Q + Q_\infty$. Thus if $a_1P + b_1Q + c_1Q_\infty$ is a lattice vector, then so is $a_2P + b_2Q + c_2Q_\infty$ where $a_2 = a_1 \bmod 3$ and $b_2 = b_1 \bmod 3$ and $c_2 = -a_2 - b_2$. One easily checks that the only possibilities for the minimum vectors are $\pm(P + Q - 2Q_\infty)$, $\pm(P - 2Q + Q1)$ and $\pm(-2P + Q + Q1)$, so $d(L_{\mathcal{P}}) = \sqrt{6}$. □

Next we prove a formula for the number of minimal vectors in $L_{\mathcal{P}}$.

Theorem 3.2. *Assume that $n \geq 4$ and let ϵ denote the number of 2-torsion points of E. Then the number of minimal vectors in $L_{\mathcal{P}}$ is*

$$\frac{n}{\epsilon} \cdot \frac{(n-\epsilon)(n-\epsilon-2)}{4} + \left(n - \frac{n}{\epsilon}\right) \cdot \frac{n(n-2)}{4}. \tag{5}$$

Proof: Define the homomorphism $\tau : E \to E$ by $\tau(\mathbf{P}) = 2\mathbf{P}$. Then the kernel of τ is the set $E[2]$ of 2-torsion points of E and the image of τ has n/ϵ points.

Fix a point $\mathbf{A}$ of E. First we count the number of solutions to the equation $\mathbf{P} + \mathbf{Q} = \mathbf{A}$ where $\mathbf{P}, \mathbf{Q}$ are distinct points of E. Observe that $\mathbf{P} = \mathbf{Q}$ if and only if $\mathbf{A} \in \text{Image}(\tau)$.

If $\mathbf{A} \in \text{Image}(\tau)$ there are ϵ solutions $\mathbf{P}$ to $2\mathbf{P} = \mathbf{A}$. Thus there are $n - \epsilon$ possible points $\mathbf{P}$ such that $\mathbf{Q} := \mathbf{A} - \mathbf{P} \neq \mathbf{P}$, and so there are $(n-\epsilon)/2$ pairs $\mathbf{P}, \mathbf{Q}$ such that $\mathbf{P} + \mathbf{Q} = \mathbf{A}$ and $\mathbf{P} \neq \mathbf{Q}$. Hence the number of pairs $\mathbf{R}, \mathbf{S}$, disjoint from $\{\mathbf{P}, \mathbf{Q}\}$, such that $\mathbf{R} + \mathbf{S} = \mathbf{A}$, is $(n - \epsilon - 2)/2$. In total, there are $(n-\epsilon)/2 \cdot (n - \epsilon - 2)/2 = (n-\epsilon)(n-\epsilon-2)/4$ possible minimal vectors $P + Q - R - S$ such that $\mathbf{P} + \mathbf{Q} = \mathbf{A} = \mathbf{R} + \mathbf{S}$. The size of the image of τ is $\frac{n}{\epsilon}$ so the total number of possible minimal vectors $P + Q - R - S$ such that $\mathbf{P} + \mathbf{Q} = \mathbf{A} = \mathbf{R} + \mathbf{S}$ with $\mathbf{A} \in \text{Image}(\tau)$ is $\frac{n}{\epsilon} \cdot \frac{(n-\epsilon)(n-\epsilon-2)}{4}$.

If $\mathbf{A} \notin \text{Image}(\tau)$ there are no solutions $\mathbf{P}$ to $2\mathbf{P} = \mathbf{A}$. Then similar reasoning as above shows that there are $(n - \frac{n}{\epsilon}) \cdot \frac{n(n-2)}{4}$ minimal vectors $P + Q - R - S$ with

$\mathbf{P} + \mathbf{Q} \notin \text{Image}(\tau)$. Thus by the above argument and Lemma 3.1, the number of minimal vectors of $L_{\mathcal{P}}$ is given by (5). □

We are now ready to prove our main result, which is just a restatement of Theorem 1.2.

Theorem 3.3. *Suppose that E has at least 5 points. Then the lattice $L_{\mathcal{P}}$ is generated by its minimal vectors. In particular, this means that it is well-rounded.*

PROOF: We know from Theorem 2.3 that the lattice $L_{\mathcal{P}}$ is generated by nonzero vectors of the form $v := -P - Q + R + Q_\infty$ where $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. It suffices to show that each such vector can be written in terms of minimal vectors. Suppose that v is not a minimal vector, that is, suppose that P, Q, R, Q_∞ are not all distinct. Notice that, since v is a nonzero principal divisor, it cannot happen that P or Q equals Q_∞. Similarly, it also cannot happen that $P = R$ or $Q = R$. Thus one of the following must be true: $P = Q$ or $R = Q_\infty$.

Suppose that $P = Q$. Then $v = -2P + R + Q_\infty$ and $2\mathbf{P} = \mathbf{R}$. Since E has at least five points, we can choose a rational place U such that $\mathbf{U}$ is not any of $\mathbf{Q}_\infty, \mathbf{P}, 2\mathbf{P}$ or $-\mathbf{P}$. Put $\mathbf{S} := \mathbf{P} + \mathbf{U}$ and observe that

$$-2P + R + Q_\infty = (-P - U + S + Q_\infty) - (P + S - R - U)$$

We claim that $-P - U + S + Q_\infty$ and $P + S - R - U$ are minimal vectors.

By choice $U \neq P, Q_\infty$. Also $U \neq S$ otherwise $\mathbf{P} = \mathbf{Q}_\infty$. Further, $S \neq P$ otherwise $U = Q_\infty$. Finally, $S \neq Q_\infty$ otherwise $\mathbf{P} + \mathbf{U} = \mathbf{Q}_\infty$ whence $\mathbf{U} = -\mathbf{P}$, which is not true. Thus $-P - U + S + Q_\infty$ is a minimal vector.

Observe that $\mathbf{P} + \mathbf{S} = 2\mathbf{P} + \mathbf{U} = \mathbf{R} + \mathbf{U}$ so $P + S - R - U$ is a lattice vector. We already know that S, P, U are distinct. We must show that none of S, U equals R (we pointed out above that $R \neq P$). If $R = S$ then $\mathbf{U} = \mathbf{P}$, which is not possible. If $R = U$ then $\mathbf{U} = \mathbf{R} = 2\mathbf{P}$, which is not possible. Thus $P + S - R - U$ is a minimal vector.

We have shown that if $P = Q$, then v is the difference of two minimal vectors.

Next assume that $R = Q_\infty$, so $v = -P - Q + 2Q_\infty$ and $\mathbf{P} + \mathbf{Q} = \mathbf{Q}_\infty$. Since E contains at least 5 rational places, we can choose a rational point $\mathbf{U}$ different from the points $\mathbf{Q}_\infty, \mathbf{P}, \mathbf{Q}, 2\mathbf{P}$. Put $\mathbf{S} := \mathbf{Q} + \mathbf{U}$ and note that $U \neq S$ otherwise $Q = Q_\infty$. Also $Q + U - S - Q_\infty$ is a lattice point and $\mathbf{P} + \mathbf{S} = \mathbf{P} + \mathbf{Q} + \mathbf{U} = \mathbf{U}$ so that $P + S - U - Q_\infty$ is also a lattice point. Now

$$v = P + Q - 2Q_\infty = (Q + U - S - Q_\infty) + (P + S - U - Q_\infty)$$

is the sum of two lattice points. We claim that $Q + U - S - Q_\infty$ and $P + S - U - Q_\infty$ are minimal vectors.

First we show that $Q + U - S - Q_\infty$ is a minimal vector. We must show that the places Q, U, S, Q_∞ are distinct. By our choice $U \neq Q, Q_\infty$. We already pointed out that $U \neq S$. It is not possible for $Q = S$, for otherwise $\mathbf{Q} = \mathbf{S} = \mathbf{Q} + \mathbf{U}$ whence $\mathbf{U} = \mathbf{Q}_\infty$, that is $U = Q_\infty$ thus contradicting our choice of $\mathbf{U}$. Finally, $S \neq Q_\infty$, otherwise $\mathbf{U} = -\mathbf{Q} = \mathbf{P}$. Thus $Q + U - S - \mathbf{Q}_\infty$ is a minimal vector.

Next we show that $P + S - U - Q_\infty$ is a minimal vector. From the argument above we know that S, U, Q_∞ are distinct. Since $d(L_{\mathcal{P}}) = 2$, we also know that $P \neq U$ and $P \neq Q_\infty$. If $P = S$ then $\mathbf{U} = \mathbf{P} + \mathbf{S} = 2\mathbf{P}$, which is not possible by the choice of U. Thus $P + S - U - Q_\infty$ is a minimal vector.

We have shown that v is the sum of two minimal vectors, which completes the proof of the theorem. □

Finally, we provide an estimate on the covering radius of $L_{\mathcal{P}}$. Recall that the covering radius (also called the inhomogeneous minimum) $\mu(L)$ of a lattice L is defined as

$$\mu(L) = \inf\{r \in \mathbb{R}_{>0} : B_V(r) + L = V\},$$

where $V = \mathrm{span}_{\mathbb{R}} L$ and $B_V(r)$ is the closed ball of radius r centered at the origin in V. In addition to an estimate on $\mu(L_{\mathcal{P}})$, our next theorem can also be interpreted as a result about the closest vector problem on such lattices.

Theorem 3.4. *The covering radius of $L_{\mathcal{P}}$ satisfies the inequality*

$$\mu(L_{\mathcal{P}}) \leq \frac{1}{2}\left(\sqrt{n^2+4n+8}+\sqrt{n}\right). \tag{6}$$

In other words, if $V = \mathrm{span}_{\mathbb{R}} A_{n-1} = \mathrm{span}_{\mathbb{R}} L_{\mathcal{P}} \subset \mathbb{R}^n$ and $v \in V$, then there exists a lattice point in $L_{\mathcal{P}}$ within distance $\frac{1}{2}\left(\sqrt{n^2+4n+8}+\sqrt{n}\right)$ from v. Furthermore, if $v \in A_{n-1}$ then there is a lattice point in $L_{\mathcal{P}}$ within distance $\sqrt{2}$ from v.

Proof: Suppose that $v := (r_0, r_1, \ldots, r_{n-1})$ is a point in V, so $r_0 + \ldots + r_{n-1} = 0$. Let $w_1 := (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}^n$ where a_i is the nearest integer to r_i (note that if r_i is a half integer, then a_i is just the floor of r_i). Now $a_0\mathbf{P}_0 + a_1\mathbf{P}_1 + \ldots + a_{n-1}\mathbf{P}_{n-1}$ equals a point $\mathbf{P}_j$ for some j, $0 \leq j \leq n-1$.

First suppose that $j \neq 0$. Put $A_0 := -a_1 - a_2 - \ldots - a_{n-1} + 1$. Then by Theorem 2.3, the vector $w_2 := (A_0, a_1, \ldots, a_{j-1}, a_j - 1, a_{j+1}, \ldots, a_{n-1})$ is a lattice point and the distance between w_2 and v is

$$\begin{aligned} & ||v - w_2|| \\ \leq\ & ||v - w_1|| + ||w_1 - w_2|| \\ \leq\ & \sqrt{n/4} + \sqrt{(A_0 - a_0)^2 + 1} \\ =\ & \sqrt{n/4} + \sqrt{(a_0 + a_1 + \ldots + a_{n-1} - 1)^2 + 1} \\ =\ & \sqrt{n}/2 + \sqrt{S^2 - 2S + 2}, \end{aligned} \tag{7}$$

where $S = a_0 + a_1 + \ldots + a_{n-1}$. Now

$$\begin{aligned} |S| &= |a_0 + a_1 + \cdots + a_{n-1}| = |(a_0 - r_0) + ... + (a_{n-1} - r_{n-1})| \\ &\leq |a_0 - r_0| + ...|a_{n-1} - r_{n-1}| \leq n/2. \end{aligned}$$

Thus

$$||v - w_2|| \leq \sqrt{n}/2 + \sqrt{n^2/4 + 2(n/2) + 2} = \frac{1}{2}\left(\sqrt{n} + \sqrt{n^2+4n+8}\right),$$

as required.

If $j = 0$, put $A_0 = -a_1 - a_2 - \ldots - a_{n-1}$ and $w_2 = (A_0, a_1, \ldots, a_{n-1})$. Then

$$||v - w_2|| \leq ||v - w_1|| + ||w_1 - w_2|| \leq \sqrt{n/4} + \sqrt{(A_0 - a_0)^2} = \sqrt{n}/2 + |S| \leq \sqrt{n}/2 + n/2,$$

by the argument above. This is still less than the claimed bound (6).

The remaining assertion of the theorem easily follows from the above argument: if $v \in A_{n-1}$ then $S = 0$ and $v = w_1$, so from (7) we obtain that $||v - w_2|| \leq \sqrt{2}$, as claimed. □

Remark 3.5. *Suppose that $n \geq 5$, then $L_{\mathcal{P}}$ is well-rounded by Theorem 3.3, and $d(L_{\mathcal{P}}) = 2$ by Lemma 3.1. In this case, the standard bounds on covering radius of a lattice (see* [3]*) guarantee that*

$$\mu(L_{\mathcal{P}}) \leq n - 1,$$

which is weaker than our bound (6) *when* n *is sufficiently large (this would imply that* q *is also large, since* $n \leq q + 1 + 2\sqrt{q}$ *by Hasse's theorem).*

4. Acknowledgement

The authors would like to thank Dr Min Sha for his indepth reading, corrections and comments on the previous version of the manuscript. He also pointed out that Theorem 3.3 is still true if the elliptic curve has fewer than 5 points.

References

[1] H. Cohn and A. Kumar. Optimality and uniqueness of the Leech lattice among lattices. *Ann. of Math. (2)*, 170(3):1003–1050, 2009.
[2] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices, and Groups*. Springer-Verlag, 3rd edition, 1999.
[3] P. M. Gruber and C. G. Lekkerkerker. *Geometry of numbers*. North-Holland Publishing Co., 2nd edition, 1987.
[4] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, 2003.
[5] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer, Berlin, 2nd edition, 2009.
[6] M. A. Tsfasman and S. G. Vladut. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, 1991.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711
E-mail address: lenny@cmc.edu

8543 Hillside Road, Rancho Cucamonga, CA 91701
E-mail address: hmahara@g.clemson.edu