Finite Fields Appl. 28 (2014) 67–78

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

FINITE FIELDS AND THEIR APPLICATIONS

Lattices from elliptic curves over finite fields

Lenny Fukshansky [a,1], Hiren Maharaj [b,*]

[a] *Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711, United States*
[b] *8543 Hillside Road, Rancho Cucamonga, CA 91701, United States*

ARTICLE INFO

Article history:
Received 22 October 2013
Received in revised form 9 January 2014
Accepted 10 January 2014
Available online 25 February 2014
Communicated by Neal Koblitz

MSC:
11H06
11G20

Keywords:
Function fields
Elliptic curves
Well-rounded lattices

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 $k \leqslant n$, and let $V = \operatorname{span}_{\mathbb{R}} L$ be the k-dimensional subspace of $\mathbb{R}^n$ spanned by L. The *minimum distance* of L is

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

[*] Corresponding author.
E-mail addresses: lenny@cmc.edu (L. Fukshansky), hmahara@g.clemson.edu (H. Maharaj).

[1] Supported by NSA Young Investigator Grant #1210223 and Simons Foundation Grants #208969, 279155.

1071-5797/$ – see front matter © 2014 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ffa.2014.01.007

where $\| \;\|$ is the usual Euclidean norm in $\mathbb{R}^n$. The *lattice* (*sphere*) *packing* in V associated with 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 $V = \operatorname{span}_{\mathbb{R}} L$ 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 $1 \leqslant n \leqslant 8$ [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 $\geqslant \zeta(n)/2^{n-1}$, where ζ stands for the Riemann zeta-function. Unfortunately, the known proofs of Minkowski–Hlawka theorem are nonconstructive, 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's. One such family, which produces particularly nice results as $n \to \infty$ are 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, $\sum_{i=1}^n v_i(f) = 0$ for each $f \in \mathcal{O}_{\mathcal{P}}^*$, and we let

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

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

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

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