LATTICES FROM ABELIAN GROUPS

ALBRECHT BÖTTCHER, LENNY FUKSHANSKY, STEPHAN RAMON GARCIA, AND HIREN MAHARAJ

Abstract. We report on our recent progress investigating geometric properties of lattices obtained via an algebraic construction from finite Abelian groups. These lattices generalize the well-known function field lattices of Rosenbloom and Tsfasman and have many interesting properties. In particular, we prove that many of them have bases of minimal vectors, are strongly eutactic, and have large automorphism groups.

Function field lattices were originally introduced by Rosenbloom and Tsfasman in [6], where they were studied for their good asymptotic packing density properties. This construction is reviewed in [9] 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

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

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 $L_{\mathcal{P}} := \mathrm{Image}(\phi_{\mathcal{P}})$ is a finite-index sublattice of the root lattice A_{n-1}.

We discuss an algebraic construction of lattices which generalizes the function field lattices. 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

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

The general problem we consider is the following.

Investigate geometric properties of lattices $L_G(S)$. Specifically, what are their minimal norms and determinants? How many minimal vectors do these lattices have? Are they well-rounded? Generated by their minimal vectors? Have bases of minimal vectors? What can be said about their automorphism groups?

2010 *Mathematics Subject Classification.* 11G20, 11H06, 11H31.

Key words and phrases. well-rounded lattice, finite Abelian group, minimal vector, covering radius, automorphism group, spherical design.

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

The answers to these questions certainly depend on the group G and the set S. As the result of the abstract construction of function field lattices outlined above, we obtain $L_{\mathcal{P}} = L_G(S)$, where

$$S = \{[P_i - P_0] : 0 \le i \le n-1\}$$

is a set 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, and lattices defined in (1) are a generalization of function field lattices. In [4], [2], [1] we addressed the questions raised above in several situations:

- The field F is the function field of an elliptic curve of a finite field, in which case $G = S$ and the groups that can appear this way are always of the form $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ (with further restrictions on the pairs (m_1, m_2)) as characterized by Rück [7].
- The Abelian group G is arbitrary, but the set S coincides with all of G; this is a generalization of function field lattices from elliptic curves.
- The field F is a Hermitian function field, in which case the generating set S is a proper subset of the group G.

Here we state our results. For an Abelian group G, write L_G for the lattice $L_G(G)$. The automorphism group $\mathrm{Aut}(L_G)$ can be identified with a finite subgroup of $\mathrm{GL}_{n-1}(\mathbb{Z})$. We also identify S_{n-1}, the group of permutations on $n-1$ letters, with the corresponding subgroup of $\mathrm{GL}_{n-1}(\mathbb{Z})$ consisting of permutation matrices.

Theorem 1 ([2])**.** *Let G be an Abelian group of order n. Then:*

(1) *For every G,* $\det L_G = n^{3/2}$.

(2) $|L_G| = \begin{cases} \sqrt{8} & \textit{if } G = \mathbb{Z}/2\mathbb{Z}, \\ \sqrt{6} & \textit{if } G = \mathbb{Z}/3\mathbb{Z}, \\ 2 & \textit{for every other } G. \end{cases}$

(3) *For $G = \mathbb{Z}/4\mathbb{Z}$, the lattice L_G is not well-rounded.*

(4) *For every $G \ne \mathbb{Z}/4\mathbb{Z}$, the lattice L_G has a basis of minimal vectors.*

(5) *For every G,* $\mathrm{Aut}(L_G) \cap S_{n-1} \cong \mathrm{Aut}(G)$.

As mentioned above, the lattices coming from elliptic curves via the Rosenbloom-Tsfasman construction were considered in [4] and [8], and they are a special case of the lattices L_G in Theorem 1. In addition to these results, we also have a formula for the number of minimal vectors in lattices L_G.

Theorem 2. *Assume that $n \ge 4$ and let κ denote the order of the subgroup $G_2 := \{x \in G : 2x = 0\}$ of G. Then the number of minimal vectors in L_G is*

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

The result of Theorem 2 was established for lattices from elliptic curves in [4], but the argument is the same for any lattice of the form L_G. Furthermore, we obtained bounds for the covering radii of the lattices L_G. Recall that the *covering radius* of a lattice L is defined as

$$\mu(L) = \inf \left\{ r \in \mathbb{R}_{>0} : \bigcup_{\boldsymbol{x} \in L} (B(r) + \boldsymbol{x}) = \mathrm{span}_{\mathbb{R}} L \right\},$$

where $B(r)$ is the ball of radius r centered at the origin in $\operatorname{span}_{\mathbb{R}} L$. In [8], Min Sha, building on our previous results from [4], proved that

$$\mu(L_G) \leq \mu(A_{n-1}) + \sqrt{2}, \tag{3}$$

where

$$\mu(A_m) = \begin{cases} \frac{1}{2}\sqrt{m+1} & \text{if } m \text{ is odd,} \\ \frac{1}{2}\sqrt{m+1-1/(m+1)} & \text{if } m \text{ is even;} \end{cases}$$

see [3, Chap. 4, Sec. 6.1]. In [2], we derived an improvement of (3) for the case when G is a cyclic group:

$$\mu\left(L_{\mathbb{Z}/n\mathbb{Z}}\right) < \frac{1}{2}\sqrt{(n-1)+4\log(n-2)+7-4\log 2+10/(n-1)}. \tag{4}$$

We also have some partial results on the properties of the lattices $L_G(S)$ in the more general situation when S is a proper subset of G containing the identity. Suppose $|G| = n$ and $|S| = m \leq n$. Define

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

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

Theorem 3 ([1])**.** *With notation as above,* $\operatorname{Aut}(G,S)^*$ *is isomorphic to a subgroup of* $\operatorname{Aut}(L_G(S)) \cap S_{m-1}$*. If S is a generating set for G, then*

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

In the more concrete situation where the lattice $L_G(S)$ comes from a Hermitian curve

$$y^q + y = x^{q+1} \tag{5}$$

over a finite field $\mathbb{F}_{q^2}$, where q is a prime power, we obtained some further results.

Theorem 4 ([1])**.** *Let $L_G(S)$ come from a Hermitian curve over $\mathbb{F}_{q^2}$ as in* (5)*. Then:*

(1) $|L_G(S)| = \sqrt{2q}$.
(2) $\det L_G(S) = \sqrt{q^3+1}(q+1)^{q^2-q}$.
(3) *The lattice $L_G(S)$ is generated by minimal vectors.*
(4) *The lattice $L_G(S)$ contains at least $q^7 - q^5 + q^4 - q^2$ minimal vectors.*

Additional observations on these lattices involve a connection to spherical designs. Let $n \geq 2$. A collection of points $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ on the unit sphere Σ_{n-2} in $\mathbb{R}^{n-1}$ is called a *spherical t-design* for some integer $t \geq 1$ if

$$\int_{\Sigma_{n-2}} f(\boldsymbol{X})\, d\nu(\boldsymbol{X}) = \frac{1}{m}\sum_{k=1}^{m} f(\boldsymbol{y}_k)$$

for every polynomial $f(\boldsymbol{X}) = f(X_1, \dots, X_{n-1})$ with real coefficients of degree $\le t$, where ν is the surface measure normalized so that $\nu(\Sigma_{n-2}) = 1$. For $n = 2$, this means that

$$f(-1) \cdot \frac{1}{2} + f(1) \cdot \frac{1}{2} = \frac{1}{m} \sum_{k=1}^{m} f(y_k)$$

with $y_1, \dots, y_m \in \{-1, 1\}$. Recall that a full-rank lattice in $\mathbb{R}^{n-1}$ is called *strongly eutactic* if its set of minimal vectors (normalized to lie on the unit sphere) forms a spherical 2-design. Strongly eutactic lattices are of great importance in extremal lattice theory (see [5]). The lattices L_G coming from Abelian groups are full-rank sublattices of A_{n-1} and may hence be viewed as full-rank lattices in $\mathbb{R}^{n-1}$. For these lattices, we have the following result.

Theorem 5. *The lattice L_G is strongly eutactic if and only if the Abelian group G has odd order or $G = (\mathbb{Z}/2\mathbb{Z})^k$ for some $k \ge 1$.*

References

[1] A. Böttcher, L. Fukshansky, S. R. Garcia, and H. Maharaj. Lattices from Hermitian function fields. *To appear; arXiv:1502.06198*, 2015.

[2] A. Böttcher, L. Fukshansky, S. R. Garcia, and H. Maharaj. On lattices generated by finite Abelian groups. *SIAM J. Discrete Math.*, 29(1):382–404, 2015.

[3] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices, and Groups.* Springer-Verlag, 1988.

[4] L. Fukshansky and H. Maharaj. Lattices from elliptic curves over finite fields. *Finite Fields Appl.*, 28:67–78, 2014.

[5] J. Martinet. *Perfect Lattices in Euclidean Spaces.* Springer-Verlag, 2003.

[6] M. Y. Rosenbloom and M. A. Tsfasman. Multiplicative lattices in global fields. *Invent. Math.*, 101:687–696, 1990.

[7] H.-G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, 1987.

[8] M. Sha. On the lattices from ellptic curves over finite fields. *Finite Fields Appl.*, 31:84–107, 2015.

[9] M. A. Tsfasman and S. G. Vladut. *Algebraic-Geometric Codes.* Kluwer Academic Publishers, 1991.

Fakultät für Mathematik, TU Chemnitz, 09107 Chemnitz, Germany
E-mail address: aboettch@mathematik.tu-chemnitz.de

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

Department of Mathematics, Pomona College, 610 N. College Ave, Claremont, CA 91711, USA
E-mail address: stephan.garcia@pomona.edu

Department of Mathematics, Pomona College, 610 N. College Ave, Claremont, CA 91711, USA
E-mail address: hiren.maharaj@pomona.edu