# Lattices from Abelian groups

Lenny Fukshansky
Claremont McKenna College

(*joint work with Albrecht Böttcher,
Stephan R. Garcia, and Hiren Maharaj*)

Workshop on "Lattices and applications in number theory"
January 17 - 23, 2016

# My co-authors

A. Böttcher
(TU Chemnitz)

S. R. Garcia
(Pomona College)

H. Maharaj
(Pomona College)

# Function field lattices

Let

$$A_{n-1} = \left\{ \boldsymbol{a} \in \mathbb{Z}^n : \sum_{i=1}^{n} a_i = 0 \right\}$$

be the well-known root lattice. The following construction of sublattices of $A_{n-1}$ is due independently to Quebbemann (1989) and Rosenbloom & Tsfasman (1990).

$p$ is prime, $q$ is a power of $p$, $\mathbb{F}_q$ is the field with $q$ elements
$X$ a smooth curve of genus $g$ over $\mathbb{F}_q$, $K = \mathbb{F}_q(X)$
$X(\mathbb{F}_q) = \{P_1, \ldots, P_n\}$ with corresponding valuations $v_1, \ldots, v_n$
$\mathcal{O}^*_{X,q} = \{f \in K \setminus \{0\} : \mathrm{Supp}(f) \subseteq X(\mathbb{F}_q)\}$

For each $f \in \mathcal{O}^*_{X,q}$, we have the principal divisor

$$(f) = \sum_{i=1}^{n} v_i(f) P_i, \ \sum_{i=1}^{n} v_i(f) = 0, \ \deg(f) := \sum_{i=1}^{n} |v_i(f)|.$$

# Function field lattices

Define the map $\phi : \mathcal{O}^*_{X,q} \to \mathbb{Z}^n$ given by $\phi(f) = (v_1(f), \ldots, v_n(f))$, then $L_{X,q} := \phi(\mathcal{O}^*_{X,q}) \subseteq A_{n-1}$ is a sublattice of finite index with

$$\begin{aligned} |L_{X,q}| &:= \min\{\|\boldsymbol{x}\| : \boldsymbol{x} \in L_{X,q} \setminus \{\mathbf{0}\}\} \\ &\geq \min\left\{\sqrt{\deg(f)} : f \in \mathcal{O}^*_{X,q} \setminus \mathbb{F}_q\right\}, \end{aligned}$$

where $\| \; \|$ is Euclidean norm, and

$$\det(L_{X,q}) \leq \sqrt{n}\left(1 + q + \frac{n-q-1}{g}\right)^g .$$

This construction famously led to some families of asymptotically dense lattices.

# Abelian group lattices

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

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

In case $G$ is the subgroup of the degree zero divisor class group $\mathrm{Cl}^0(K)$ of $K = \mathbb{F}_q(X)$ generated by a set of divisor classes

$$S = \{[P_i - P_1] : P_i \in X(\mathbb{F}_q), 1 \leq i \leq n\}$$

we have

$$L_G(S) = L_{X,q}.$$

In other words, our Abelian group lattices are a generalization of function field lattices.

# Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?
- 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?
- Do these lattices give rise to spherical designs?

The answers to these questions certainly depend on the group $G$ and the set $S$. In this talk we present some results we have obtained thus far.

# Some results

Specifically, we have addressed the questions raised above in several situations:

- Function field lattices from elliptic curves over 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 H.-G. Rück in 1987.
- 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.
- Function field lattices from Hermitian curves over finite fields, in which case the generating set $S$ is a proper subset of the group $G$.

# Three conditions on lattices

We first recall some notation. Given a lattice $L \subseteq \mathbb{R}^n$ with $\operatorname{rk} L = n$, we define its set of **minimal vectors** as

$$S(L) = \{\boldsymbol{x} \in \Lambda : \|\boldsymbol{x}\| = |L|\},$$

where $|L| = \min\{\|\boldsymbol{x}\| : \boldsymbol{x} \in L \setminus \{\mathbf{0}\}\}$ is its **minimal norm**.

- A lattice $L$ is **well-rounded** (WR) if $\operatorname{span}_{\mathbb{R}} L = \operatorname{span}_{\mathbb{R}} S(L)$.
- If $\operatorname{rk} L > 4$, a strictly stronger condition is that $L$ is **generated by minimal vectors**, i.e. $L = \operatorname{span}_{\mathbb{Z}} S(L)$.
- It has been shown by Conway & Sloane (1995) and Martinet & Schürmann (2011) that there are lattices of rank $\geq 10$ generated by minimal vectors which do not contain a **basis of minimal vectors**.

# Automorphism groups

Let $\mathrm{GL}(L)$ be the subgroup of $\mathrm{GL}_n(\mathbb{R})$ that permutes $L$. The **automorphism group** of a lattice $L \subseteq \mathbb{R}^n$ is

$$\mathrm{Aut}(L) := \mathrm{GL}(L) \cap O(\mathbb{R}^n),$$

where $\mathrm{GL}(L)$ is discrete and $O(\mathbb{R}^n)$ is the compact group of orthogonal transformations of $\mathbb{R}^n$ onto itself $\Longrightarrow$ $\mathrm{Aut}(L)$ is finite.

For all $n \neq 2, 4, 6, 7, 8, 9, 10$ the largest (with respect to order) $\mathrm{Aut}(L)$ is

$$\mathrm{Aut}(\mathbb{Z}^n) = (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n.$$

# Results on lattices from full Abelian group

**Theorem 1 (Böttcher, F., Garcia, Maharaj (2014))**

*Let $n = |G|$ and write $L_G$ for the lattice $L_G(G)$. Then:*

1. *For any $G$,* $\det L_G = n^{3/2}$.
2. $|L_G| = \begin{cases} \sqrt{8} & \textit{if } G = \mathbb{Z}/2\mathbb{Z}, \\ \sqrt{6} & \textit{if } G = \mathbb{Z}/3\mathbb{Z}, \\ 2 & \textit{for any other } G. \end{cases}$
3. *For $G = \mathbb{Z}/4\mathbb{Z}$, the lattice $L_G$ is not WR.*
4. *For any $G \neq \mathbb{Z}/4\mathbb{Z}$, the lattice $L_G$ has a basis of minimal vectors.*
5. *Let $\varepsilon = |\{g \in G : 2g = 0\}|$, then*
$$|S(L_G)| = \frac{n}{4\varepsilon}\left((n-\varepsilon)(n-\varepsilon-2) + n(n-2)(\varepsilon-1)\right).$$
6. *For any $G$,* $\mathrm{Aut}(L_G) \cap S_{n-1} \cong \mathrm{Aut}(G)$.

# Remarks

If $X$ is an elliptic curve over $\mathbb{F}_q$, a result of H.-G. Rück (1987) states that

$$X(\mathbb{F}_q) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

for some $m_1 \mid m_2, q - 1$.

In the special case when $G$ is a subgroup of some $X(\mathbb{F}_q)$, parts 1 – 4 of Theorem 1 were also independently established by Min Sha (2014).

In the special case when $G$ is a cyclic group, the lattices $L_G$ recover the well known family of Barnes lattices:

$$\mathcal{B}_{n-1} = \left\{ \boldsymbol{a} \in A_{n-1} : \sum_{i=1}^{n} i x_i \equiv 0 \pmod{n} \right\}.$$

# Proof outline for Theorem 1

**Part 1.** Define an additive group homomorphism

$$\varphi : A_{n-1} \to G$$

by

$$\varphi\left(x_1, \ldots, x_{n-1}, -\sum_{i=1}^{n-1} x_i\right) = \sum_{i=1}^{n-1} x_i P_i.$$

Then $\varphi$ is surjective and

$$\mathrm{Ker}(\varphi) = L_G.$$

Hence $G \cong A_{n-1}/L_G$, and so

$$n = |G| = |A_{n-1}/L_G| = \det L_G / \det A_{n-1} = \det L_G / \sqrt{n}.$$

# Proof outline for Theorem 1

**Parts 2–5.** We explicitly construct bases of minimal vectors. Let $n \geq 5$ and consider the cyclic group

$$G := \mathbb{Z}/n\mathbb{Z} = \{\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n-1}\}\,.$$

Then $G$ has relations :

$$(-1)\mathbf{1} + (-1)\mathbf{2} + (1)\mathbf{3} = \mathbf{0},$$

$$(1)\mathbf{1} + (-1)\mathbf{2} + (-1)\mathbf{3} + (1)\mathbf{4} = \mathbf{0},$$

$$(-1)\mathbf{1} + (-1)\mathbf{3} + (1)\mathbf{4} = \mathbf{0},$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

In other words, the corresponding lattice $L_G$ has $n$ linearly independent vectors with 4 nonzero coordinates, all equal to $\pm 1$. These are minimal vectors in $L_G$, and hence $|L_G| = 2$.

# Proof outline for Theorem 1

Let $A$ be the matrix whose columns are these minimal vectors. Then $A^tA$ is a certain (cornered) Toeplitz matrix. Using Cauchy-Binet formula, we show that

$$\left|\det(A^tA)\right| = n^3 = (\det L_G)^2$$

which means that $A$ is a basis matrix for $L_G$. This establishes parts 2–4 of the theorem for cyclic groups of order $\geq 5$. Small cyclic groups are treated separately.

A general abelian group $G$ can be presented as a direct product of cyclic groups. We show that a minimal basis matrix can be constructed as an upper block-triangular matrix with blocks corresponding to minimal basis matrices of lattices coming from the cyclic group factors.

Finally, since we can explicitly construct minimal vectors, we can also directly count them. This completes the proof.

# Proof outline for Theorem 1

**Part 6.** If

$$G = \{P_0, P_1, \ldots, P_{n-1}\},$$

with $P_0$ the identity, as above, then any automorphism of $G$ fixes $P_0$ and permutes $P_1, \ldots, P_{n-1}$. Hence $\mathrm{Aut}(G)$ can be identified with some subgroup $H$ of $S_{n-1}$.

We explicitly construct a map

$$\Phi : H \to \mathrm{Aut}(L_G) \cap S_{n-1},$$

given by $\Phi(\sigma) = \tau$ for every $\sigma \in H$, where

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

We then show that $\Phi$ is a group isomorphism.

# Covering radius

An important invariant of a lattice $L$ is its covering radius:

$$\mu(L) = \inf \left\{ \mu \in \mathbb{R}_{>0} : B(\mu) + L = \operatorname{span}_{\mathbb{R}} L \right\},$$

where $B(\mu)$ is the ball of radius $\mu$ centered at the origin in $\operatorname{span}_{\mathbb{R}} L$.

In 2013, we produced a bound on the covering radius of lattices $L_G$, which was then improved by Min Sha (2014): if $|G| = n$, then

$$\mu(L_G) \leq \frac{1}{2}\sqrt{n} + \sqrt{2}. \tag{1}$$

In fact, if $G = \mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$, we can do a little better (2014):

$$\mu(L_G) \leq \frac{1}{2}\sqrt{n + 4\log(n-2) + 6 - 4\log 2 + 10/(n-1)}. \tag{2}$$

# Covering radius: some data

Here is data (chopped after the fourth digit after the decimal point) for $\mu(L_G)$ of several cyclic groups $G = \mathbb{Z}/n\mathbb{Z}$:

| $n$ | Bound (2) | Bound (1) |
|---:|---:|---:|
| 4 | 1.8257 | 2.4142 |
| 5 | 1.9443 | 2.5097 |
| 6 | 2.0477 | 2.6390 |
| 7 | 2.1408 | 2.7235 |
| 21 | 3.0210 | 3.7029 |
| 51 | 4.1831 | 4.9842 |
| 101 | 5.5387 | 6.4389 |
| 1 001 | 16.0613 | 17.2335 |
| 10 001 | 50.1026 | 51.4167 |
| 100 001 | 158.1536 | 159.5289 |
| 1 000 001 | 500.0149 | 501.4145 |

## Spherical designs

Let $n \geq 2$. A collection of points $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ on the unit sphere $\Sigma_{n-2}$ in $\mathbb{R}^{n-1}$ is called a **spherical $t$-design** for an 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 $f(\boldsymbol{X}) = f(X_1, \ldots, X_{n-1})$ with real coefficients of degree $\leq t$, where $\nu$ is the surface measure so that $\nu(\Sigma_{n-2}) = 1$. 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. The Abelian group lattices $L_G$ can be viewed as full-rank lattices in $\mathbb{R}^{n-1}$.

### Theorem 2 (Böttcher, F., Garcia, Maharaj (2015))

*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 $k \geq 1$.*

# General subsets of an Abelian group

Let $S \subseteq G$ contain the identity, $|G| = n \geq |S| = m$. Define

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

$$\mathrm{Aut}(G,S)^* := \{\sigma|_S : S \to S \ : \ \sigma \in \mathrm{Aut}(G,S)\}.$$

**Theorem 3 (Böttcher, F., Garcia, Maharaj (2015))**

*With notation as above:*

1. $|L_G(S)| = 2$ *if* $m(m-1) \geq 2(n+1)$
2. $|L_G(S)| \leq \sqrt{6}$ *if* $m(m-1)(m-2) \geq 6(n+1)$
3. $\mathrm{Aut}(G,S)^*$ *is isomorphic to a subgroup of* $\mathrm{Aut}(L_G(S)) \cap S_{m-1}$. *If $S$ is a generating set for $G$, then*

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

# Lattices from Hermitian curves

When the lattice $L_G(S)$ comes from a Hermitian curve $X$:

$$y^q + y = x^{q+1}$$

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

## Theorem 4 (Böttcher, F., Garcia, Maharaj (2015))

*Let $L_G(S)$ come from a Hermitian curve $X$ over $\mathbb{F}_{q^2}$, i.e.*

$$S = \{[P_i - P_1] : P_i \in X(\mathbb{F}_{q^2}), 1 \leq i \leq m\} \subset \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$$

*and $G \leq \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$ is generated by $S$. Then:*

1. $|L_G(S)| = \sqrt{2q}$ *and* $\det L_G(S) = \sqrt{q^3+1}(q+1)^{q^2-q}$.
2. $L_G(S)$ *is generated by minimal vectors.*
3. $L_G(S)$ *contains at least* $q^7 - q^5 + q^4 - q^2$ *minimal vectors.*
4. $\mathrm{Aut}(\mathbb{F}_{q^2}(X)) \cong$ *to a subgroup of* $\mathrm{Aut}(L_G(S)) \cap S_{m-1}$.

# Idea of proof

- We first characterize divisors of all lines in the Hermitian function field $K = \mathbb{F}_{q^2}(X)$, that is functions of the form $ax + by + c$ ($a, b, c \in \mathbb{F}_{q^2}$ with $a, b$ not both zero).
- We show that minimal vectors in the lattice $L_G(S)$ come precisely from divisors of functions of the form $(f_1/f_2)$, where $f_1$ and $f_2$ are two distinct lines satisfying some additional conditions, which we explicitly describe and count. We use this description to compute the minimal norm of the lattice.
- G. Hiss (2004) showed that every function in $\mathcal{O}^*_{X,q^2}$ (in case $X/\mathbb{F}_{q^2}$ is a Hermitian curve) is the product of functions of the form $ax + by + c$ and their inverses. We use Hiss's result, along with our above description of minimal vectors, to prove that the lattice $L_G(S)$ is generated by minimal vectors.
- In the Hermitian case, $A_{n-1}/L_G(S) \cong \mathrm{Cl}^0(K)$, and so determinant of $L_G(S)$ can be related to the class number of $K$, which is well-known.

# Remarks

- In general, lattices of the form $L_G(S)$ may be WR and non-WR. For example, if $G = \mathbb{Z}/7\mathbb{Z}$ and $S$ runs over all non-trivial subsets of $G$ containing 0, then out of the 62 resulting lattices of the form $L_G(S)$, 26 are WR and 36 are not. Interestingly, the group $\mathrm{Aut}(G, S)^*$ can be non-trivial even when $L_G(S)$ is not WR.
- The function field lattice corresponding to the Klein curve

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

  over $\mathbb{F}_4$ has rank 13 in $\mathbb{R}^{14}$ and 168 minimal vectors, which generate a sublattice of index 2: it is WR, but not generated by its minimal vectors.
- In recent work, L. Ates and H. Stichtenoth (2015) obtained many examples of function field lattices from hyperelliptic curves over finite fields which are not WR.

# References

1. L. Fukshansky, H. Maharaj, *Lattices from elliptic curves over finite fields*, Finite Fields and Their Applications, vol. 28 (July 2014), pg. 67–78
2. A. Böttcher, L. Fukshansky, S. R. Garcia, H. Maharaj, *On lattices generated by finite Abelian groups*, SIAM Journal on Discrete Mathematics, vol. 29 no. 1 (2015), pg. 382–404
3. A. Böttcher, L. Fukshansky, S. R. Garcia, H. Maharaj, *Lattices from Hermitian function fields*, Journal of Algebra, vol. 447 (2016), pg. 560–579
4. A. Böttcher, L. Fukshansky, S. R. Garcia, H. Maharaj, *Spherical 2-designs and lattices from Abelian groups*, preprint (2015)

These papers are available at:

`http://math.cmc.edu/lenny/research.html`

# Thank you!