Lattices in Function Fields and Applications

Christian Bagshaw
Joint work with Bryce Kerr

January 18, 2023

Lattices and Convex Bodies in $\mathbb{R}^n$

In $\mathbb{R}^n$ we define a **lattice** to be of the form $\mathcal{L} = A\mathbb{Z}^n$ for some $A \in \mathrm{GL}_n(\mathbb{R})$ (invertible $n \times n$ matrix).

We next define a **(symmetric) convex body** to be any open, convex set that is symmetric about the origin.

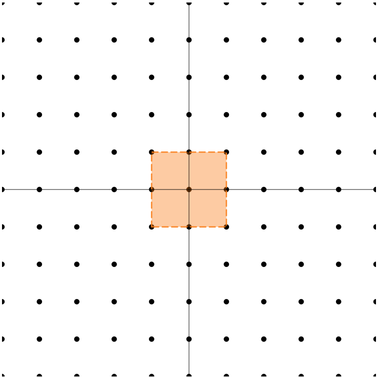
We will often be interested in convex bodies of the form

$$\mathcal{B} = B\mathbb{T}^n$$

for some $B \in \mathrm{GL}_n(\mathbb{R})$ where $\mathbb{T}^n$ is the unit box

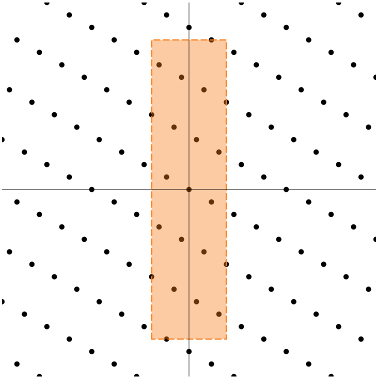
$$\mathbb{T}^n = \{(x_1, ..., x_n) \ : \ |x_i| < 1\}.$$

Examples



$$\mathcal{L} = \mathbb{Z}^2$$

$$\mathcal{B} = \mathbb{T}^2$$



$$\mathcal{L} = \begin{pmatrix} 13/5 & 2 \\ 0 & 1 \end{pmatrix} \mathbb{Z}^2$$

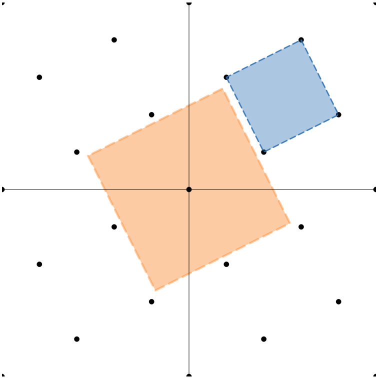
$$\mathcal{B} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \mathbb{T}^2$$

Geometry of Numbers

Minkowski's "Geometry of Numbers" is perhaps the most famous work with regards to lattices and convex bodies and their intersections $\mathcal{B} \cap \mathcal{L}$.

First crucial question considered by Minkowski: How big does a convex body need to be, to guarantee it contains a non-zero lattice point?

Minkowski's Theorem



We define $\mathrm{vol}\,\mathcal{B}$ to be its Lebesgue measure, and if $\mathcal{B} = B\mathbb{T}^n$ then

$$\mathrm{vol}\,\mathcal{B} = 2^n |\det B|.$$

We define $\det \mathcal{L}$ to be the measure of one of its "fundamental cells", and if $\mathcal{L} = A\mathbb{Z}^n$ then

$$\det \mathcal{L} = |\det A|.$$

Theorem (Minkowski, 1889)

If $\mathrm{vol}\,\mathcal{B} > 2^n \det \mathcal{L}$ then $\mathcal{B}$ contains a non-zero lattice point.

Why do we care?

You can represent a lot of interesting problems as the intersection of a convex body and a lattice.

Some famous examples of results that are often proved using Minkowski's Theorem:

- Finiteness of the class group of a number field,
- Dirichlets unit theorem,
- Lagrange's four-square theorem,
- Fermat's theorem on sums of two squares.

Successive Minima

For each integer k satisfying $1 \leq k \leq n$ we define the k-th successive minima of $\mathcal{L}$ with respect to $\mathcal{B}$ to be

$$\sigma_k = \inf\{\sigma \in \mathbb{R} \ : \ \sigma\mathcal{B} \text{ contains } k \text{ linearly independent vectors in } \mathcal{L}\}.$$

σ_k is how much you need to scale the convex body up by so that it contains k linearly independent vectors from $\mathcal{L}$.

Don't worry too much about the specifics, but the idea is that the successive minima are just some constants attached to the pair $(\mathcal{L}, \mathcal{B})$, and $\sigma_1 \leq \sigma_2 \leq ...$

Minkowski's Second Theorem

Perhaps the most famous result with regard to successive minima is the following, often referred to as Minkowski's Second Theorem:

Theorem (Minkowski, 1896)

$$\frac{2^n}{n!}\frac{\det \mathcal{L}}{\mathrm{vol}\,\mathcal{B}} \le \sigma_1 \ldots \sigma_n \le 2^n \frac{\det \mathcal{L}}{\mathrm{vol}\,\mathcal{B}}.$$

You can also bound $\mathcal{B} \cap \mathcal{L}$ using successive minima:

Theorem (Betke, Henk and Wills, 1993)

$$|\mathcal{B} \cap \mathcal{L}| \le \prod_{j=1}^{n} \left(\frac{2j}{\sigma_j} + 1 \right).$$

Together these results form a very powerful duo.

Applications in recent years

Techniques have been developed to apply these results to counting problems in number theory. These techniques seem to have been initially developed by Bourgain, Garaev, Konyagin and Shparlinski (around 2012).

We have been working on developing similar techniques in certain function fields over finite fields.

Moving to Function Fields

We are going to fix a prime power q, and let $\mathbb{F}_q$ denote the finite field of order q. We will then let $\mathbb{F}_q[T]$ be the set of polynomials with coefficients from $\mathbb{F}_q$. So elements look like

$$a_n T^n + ... + a_1 T + a_0.$$

We are going to let $\mathbb{F}_q(T)_\infty$ denote the set of Laurent series in $1/T$, so elements look like

$$\sum_{-\infty}^{n} a_i T^i = a_n T^n + ... + a_1 T + a_0 + a_{-1} T^{-1} + a_{-2} T^{-2} + ...$$

$\mathbb{F}_q[T]$ very naturally sits inside $\mathbb{F}_q(T)_\infty$ (polynomials are the Laurent series with no negative powers of T), and even any rational function can naturally be written as a Laurent series in this way (think long division of polynomials).

Function Field Analogy

Think about the relationship between $\mathbb{F}_q[T]$ and $\mathbb{F}_q(T)_\infty$ like the relationship between $\mathbb{Z}$ and $\mathbb{R}$:

$$\begin{array}{ccc} \mathbb{Z} & & \mathbb{F}_q[T] \\ \downarrow & \text{take the field of fractions} & \downarrow \\ \mathbb{Q} & & \mathbb{F}_q(T) \\ \downarrow & \text{complete w.r.t. } |\cdot| & \downarrow \\ \mathbb{R} & & \mathbb{F}_q(T)_\infty \end{array}$$

where on the right,

$$\Big|\sum_{-\infty}^{n} a_i T^i\Big| = q^n.$$

Because these spaces are so similar, we will define lattices, convex bodies, volume and successive minima in an almost identical way.

Lattices and Convex Bodies

In $\mathbb{F}_q(T)_\infty^n$, we are going to define a lattice to be of the form

$$\mathcal{L} = A\ \mathbb{F}_q[T]^n$$

for some $A \in \mathrm{GL}_n(\mathbb{F}_q(T)_\infty)$ (invertible $n \times n$ matrix).

We will define the unit box to be the set

$$\mathbb{T}^n = \{(x_1, ..., x_n)\ :\ |x_i| \leq 1\}$$

and define a convex body to be of the form

$$\mathcal{B} = B\ \mathbb{T}^n$$

for some $B \in \mathrm{GL}_n(\mathbb{F}_q(T)_\infty)$.

Determinants and Volume

We define $\det \mathcal{L}$ and $\mathrm{vol}\,\mathcal{B}$ almost identically.

$$\text{If } \mathcal{L} = A\mathbb{F}_q[T]^n \text{ then } \det \mathcal{L} = |\det A|.$$

$$\text{If } \mathcal{B} = B\mathbb{T}^n \text{ then } \mathrm{vol}\,\mathcal{B} = |\det B|.$$

These volumes can be interpreted using a Haar measure on $\mathbb{F}_q(T)_\infty$.

Mahler's Result on Successive Minima

We also define the successive minima in the same way:

$\sigma_k = \min\{|\sigma| \,:\, \sigma \in \mathbb{F}_q(T)_\infty$ and $\sigma\mathcal{B}$ contains k linearly independent vectors in $\mathcal{L}\}$.

Mahler proved an analogue of Minkowski's Second Theorem:

Theorem (Mahler, 1941)

$$\sigma_1 \ldots \sigma_n = \frac{\det \mathcal{L}}{\mathrm{vol}\, \mathcal{B}}.$$

This is much more precise than in Euclidean space.

Looking at Intersections

In order to develop techniques similar to those used in $\mathbb{R}^n$, we want to bound the intersection of a convex body and lattice in terms of successive minima.
We can again be much more precise in this setting.

Theorem (B. and Kerr, 2022)

$$|\mathcal{B} \cap \mathcal{L}| = \prod_{i=1}^{n} \max\left\{1, \frac{q}{\sigma_i}\right\}.$$

Building upon this result, one can derive a large number of more specific bounds useful for bounding intersections.

Something like Minkowski's Theorem

As a quick example of a corollary:

Corollary

$$|\mathcal{B} \cap \mathcal{L}| \geq q^n \frac{\operatorname{vol} \mathcal{B}}{\det \mathcal{L}}$$

An idea for how to apply this

To apply these results, we try to reduce a problem to counting a lattice-body intersection $|\mathcal{B} \cap \mathcal{L}|$, and divide the problem up into cases depending on the possible sizes of the successive minima.

For example, in 2 dimensions we have 3 cases:

- $\sigma_1 > 1$ and $\sigma_2 > 1$. This implies $|\mathcal{B} \cap \mathcal{L}| = 1$.
- $\sigma_1 \leq 1$ and $\sigma_2 > 1$. This one is trickier, but it implies that every vector in $\mathcal{B} \cap \mathcal{L}$ is an $\mathbb{F}_q[T]$ multiple of the shortest vector in $\mathcal{B} \cap \mathcal{L}$. This is much easier to count.
- $\sigma_1 \leq 1$ and $\sigma_2 \leq 1$. The previous results imply

$$|\mathcal{B} \cap \mathcal{L}| = q^2 \frac{\mathrm{vol}\,\mathcal{B}}{\det \mathcal{L}}.$$

An example - counting points on curves

Let $\mathbb{F}_{q^r}$ be the finite field of order q^r.

We will consider the problem of counting solutions to

$$y^2 = a_3x^3 + a_2x^2 + a_1x + a_0, \quad x, y \in V$$

with $a_0, a_1, a_2, a_3 \in \mathbb{F}_{q^r}$ and V an $\mathbb{F}_q$ subspace of $\mathbb{F}_{q^r}$.

A special case of this would be counting points on elliptic curves.

Finite Fields using Polynomials

Let $P \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree r. Then as fields

$$\mathbb{F}_{q^r} \cong \mathbb{F}_q[T]/P(T).$$

So our problem is equivalent to counting solutions to

$$y^2 \equiv a_3x^3 + a_2x^2 + a_1x + a_0 \pmod{P}, \quad x, y \in V.$$

A natural choice for V would be to count solutions to

$$y^2 \equiv a_3x^3 + a_2x^2 + a_1x + a_0 \pmod{P}, \quad \deg x, \deg y < m$$

for some $m \leq r$.

Counting Points

The following should be compared with some results of Kerr and Mohammadi in fields of prime order.

Theorem (B. and Kerr, 2022)

Suppose $\mathrm{char}(\mathbb{F}_q) > 3$. *Let* $P \in \mathbb{F}_q[T]$ *of degree* r *and let* $m \leq r$. *Let* $a_0, a_1, a_2, a_3 \in \mathbb{F}_q[T]$ *with* $\gcd(a_3, P) = 1$.

The number of solutions to

$$y^2 \equiv a_3x^3 + a_2x^2 + a_1x + a_0 \pmod{P}, \quad \deg x, \deg y < m$$

is bounded above by

$$q^{3m/2 - r/6 + o(m)} + q^{m/3 + o(m)}.$$

The trivial bound is $2q^m$.
This bound is strong for small m: it is non-trivial when $m < r/3$ and if $m < r/6$ then the bound becomes

$$q^{m/3 + \epsilon m}.$$

What does this have to do with lattices?

If you suppose that at least one point lies on the curve, then making a change of variables means that it suffices to count solutions to

$$y^2 + c_1 y \equiv b_3 x^3 + b_2 x^2 + b_1 x \pmod{P}, \quad \deg x, \deg y < m.$$

Now this means that if we have a solution (x, y), then

$$(x, x^2, x^3, y, y^2) \in \mathcal{L} \cap \mathcal{B}$$

where

$$\mathcal{L} = \{(x_1, x_2, x_3, y_1, y_2) \in \mathbb{F}_q[T]^5 : \\ y_2 + c_1 y_1 \equiv b_3 x_3 + b_2 x_2 + b_1 x_1 \pmod{P}\}$$

and

$$\mathcal{B} = \{(x_1, x_2, x_3, y_1, y_2) \in \mathbb{F}_q(T)_\infty^5 : \\ |x_1|, |y_1| < q^n, \ |x_2|, |y_2| < q^{2n}, \ |x_3| < q^{3n}\}.$$

The general idea and going forward

This idea often works for counting solutions to congruences $\pmod{P}$ when the variables have bounded degree - these correspond to solutions to equations in certain subspaces of finite fields.

Can this idea work for more general subspaces?

Thank you!