The Geometry of Numbers in Function Fields

Christian Bagshaw
Joint work with Bryce Kerr

September 23, 2023

Lattices in $\mathbb{R}^n$

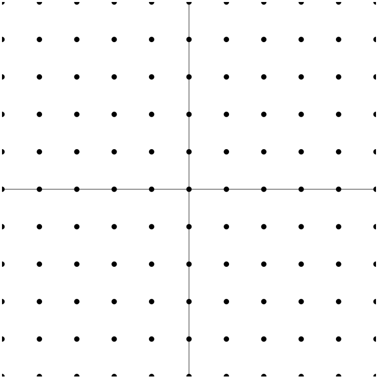
In n-dimensional space, we will define a **lattice** to be a set obtained by applying an invertible linear transformation (invertible matrix) to the set of points with integer coordinates.

More formally, in $\mathbb{R}^n$ we define a **lattice** $\mathcal{L}$ to be a set of the form

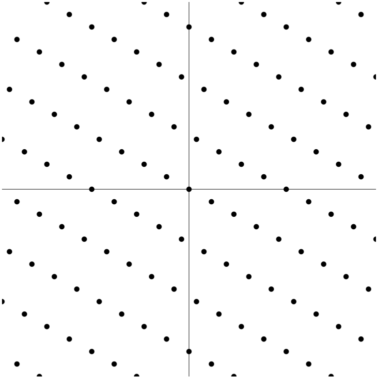
$$\mathcal{L} = A\mathbb{Z}^n \text{ for some } A \in \mathrm{GL}_n(\mathbb{R}).$$

Just picture a patterned arrangement of points in space.

Examples of Lattices



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



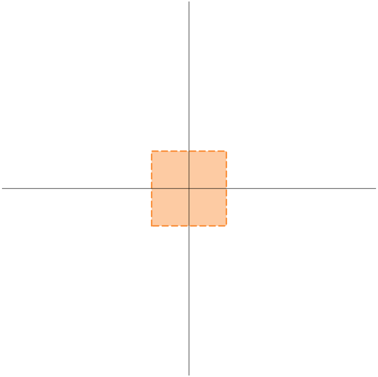
$$\mathcal{L} = \begin{pmatrix} 13/5 & 2 \\ 0 & 1/3 \end{pmatrix} \mathbb{Z}^2$$

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

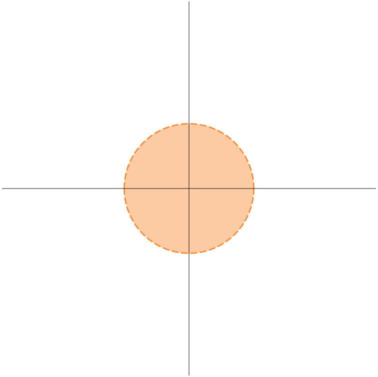
We will next define a **convex body** $\mathcal{B}$ to be any set that is open, convex, and symmetric about the origin.

In general, just picture a convex and symmetric shape that is centered at the origin.

Examples of Convex Bodies



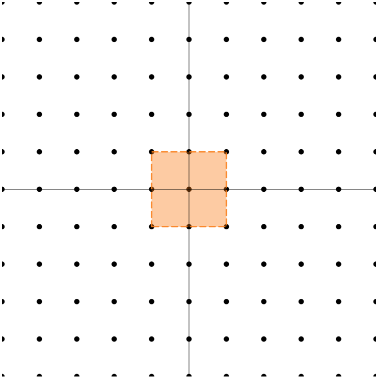
$$\mathcal{B} = \{(x, y) : |x|, |y| < 1\}$$



$$\mathcal{B} = \{(x, y) : x^2 + y^2 < 3\}$$

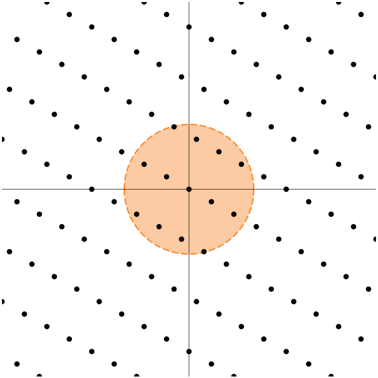
Intersection of Lattices and Convex Bodies

We are going to be interested in looking at the *intersection* $\mathcal{B} \cap \mathcal{L}$



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

$$\mathcal{B} = \{(x, y) : |x|, |y| < 1\}$$



$$\mathcal{L} = \begin{pmatrix} 13/5 & 2 \\ 0 & 1/3 \end{pmatrix} \mathbb{Z}^2$$

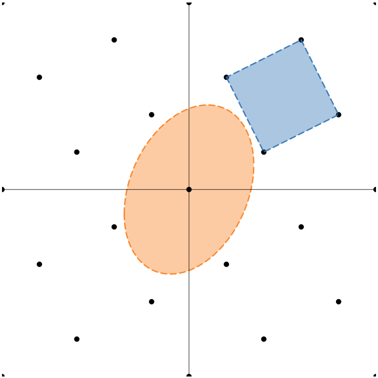
$$\mathcal{B} = \{(x, y) : x^2 + y^2 < 3\}$$

Geometry of Numbers

Minkowski's "Geometry of Numbers" (his book from 1896) is perhaps the most famous work with regards these 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 $\operatorname{vol}\mathcal{B}$ to be its volume.

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

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

Theorem (Minkowski, 1889)

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

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

$$\sigma_k = \inf\{\sigma \in \mathbb{R} \ : \ \sigma\mathcal{B} \text{ contains } k \text{ linearly independent vectors in } \mathcal{L}\}$$
$$= \text{"the smallest amount you can scale the convex body by so that it contains } k \text{ linearly independent vectors from } \mathcal{L}\text{"}$$

Don't worry too much about the specifics; the idea is that the successive minima are just some numbers associated with the lattice $\mathcal{L}$ and the convex body $\mathcal{B}$.

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)

$$\frac{2^n}{n!}\frac{\det \mathcal{L}}{\operatorname{vol} \mathcal{B}} \leq \sigma_1 \cdots \sigma_n \leq 2^n \frac{\det \mathcal{L}}{\operatorname{vol} \mathcal{B}}.$$

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

Theorem (Betke, Henk and Wills, 1993)

$$\#(\mathcal{B} \cap \mathcal{L}) \leq \prod_{k=1}^{n} \left(\frac{2k}{\sigma_k} + 1 \right).$$

Applications

Techniques have been developed to apply these results to counting problems in number theory. These techniques (in their modern form) seem to first appear in some work by Bourgain, Garaev, Konyagin and Shparlinski (around 2012).

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

So we are now going to move into a more abstract setting and see how a similar theory can be developed, but keep in mind our intuition for lattices and convex bodies in $\mathbb{R}^n$.

Moving to Function Fields

We will fix a prime power q, and let $\mathbb{F}_q$ denote the finite field of order q. If you are unfamiliar with finite fields, just think of q as a prime and $\mathbb{F}_q$ as the integers modulo q.
We will then let $\mathbb{F}_q[X]$ be the set of polynomials with coefficients from $\mathbb{F}_q$. So elements look like

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

with $a_i \in \mathbb{F}_q$.

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

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

$\mathbb{F}_q[X]$ very naturally sits inside $\mathbb{F}_q(X)_\infty$ (polynomials are the Laurent series with no negative powers of X).

Function Field Analogy

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

A somewhat superficial (but very helpful) way to gain intuition is the following:

Integers are just real numbers with no negative powers of 10 in their decimal expansion.

Polynomials are just Laurent series with no negative powers of X in their series expansion.

So although we will be now thinking about lattices and convex bodies over $\mathbb{F}_q(X)_\infty$, just picture in your mind lattices and convex bodies over $\mathbb{R}$.

Lattices and Convex Bodies

We are going to define a lattice $\mathcal{L} \subseteq \mathbb{F}_q(X)_\infty^n$ to be any set of the form

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

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

We will define a convex body $\mathcal{B} \subseteq \mathbb{F}_q(X)_\infty^n$ to be any open, convex set that is symmetric about the origin. Of course for this to make sense we need a topology and a notion of convexity, but we don't need to worry about that for this talk.

Determinants, Volume and Successive Minima

We can define a "metric" and "Haar measure" on this space (ways measuring size and volume). The Haar measure satisfies certain properties that you want when measuring volumes (ex. the Lebesgue measure is a Haar measure).

So we can define $\det \mathcal{L}$, $\mathrm{vol}\,\mathcal{B}$, and the successive minima almost identically.

$$\det \mathcal{L} \text{ denotes the volume of one of the fundamental cells of } \mathcal{L},$$

$$\mathrm{vol}\,\mathcal{B} \text{ denotes the volume of } \mathcal{B},$$

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

Don't try to digest these definitions fully. Just know that $\det \mathcal{L}$ and $\mathrm{vol}\,\mathcal{B}$ capture the "sizes" of the lattice and convex body, and the σ_k's are just some constants associated with the lattice and body.

Mahler's Result on Successive Minima

Firstly, Mahler proved an analogue of Minkowski's Second Theorem:

Theorem (Mahler, 1941)

$$\sigma_1 \cdots \sigma_n = q^n \frac{\det \mathcal{L}}{\mathrm{vol}\, \mathcal{B}}.$$

This is much more precise than in Euclidean space.

Looking at Intersections

But we may be looking for something like Minkowski's (first) Theorem, or the result from Betke, Henk, and Wills for bounding intersections more explicitly.

We can again be much more precise in this setting.

Theorem (B. and Kerr, 2022)

$$\#(\mathcal{B} \cap \mathcal{L}) = \prod_{k=1}^{n} \max\left\{1, \frac{q}{\sigma_k}\right\}.$$

Building upon this result, one can derive more specific bounds useful for bounding intersections, which we have then applied to a number of counting problems in number theory.

Something like Minkowski's Theorem

As a quick example of a corollary:

$$
\begin{aligned}
\#(\mathcal{B} \cap \mathcal{L}) &= \prod_{k=1}^{n} \max\left\{1, \frac{q}{\sigma_k}\right\} \\
&\geq \prod_{k=1}^{n} \frac{q}{\sigma_k} \\
&= \frac{q^n}{\sigma_1 \cdots \sigma_n} \\
&= \frac{\operatorname{vol} \mathcal{B}}{\det \mathcal{L}}.
\end{aligned}
$$

This implies an analogue of Minkowski's Theorem!

Corollary

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

Thank you!