An Introduction to Lattices, Lattice Reduction, and Lattice-Based Cryptography

Joseph H. Silverman

Brown University

PCMI Lecture Series

July 6–10, 2020

Lecture 1. Lattices and Hard Lattice Problems

Lattices — Definition and Notation

Definition. A **lattice** L of rank (or dimension) n is a discrete subgroup of $\mathbb{R}^n$ containing an $\mathbb{R}$-basis for $\mathbb{R}^n$.

Equivalently, a lattice is the $\mathbb{Z}$-linear span of a set of n vectors linearly independent over $\mathbb{R}$:

$$L = \{a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n : a_1, a_2, \ldots, a_n \in \mathbb{Z}\}.$$

The set $\mathcal{B} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a **basis** for L. Lattices have many bases. Some bases are "better" than others.

The **fundamental domain** for the quotient $\mathbb{R}^n/L$ associated to the basis $\mathcal{B}$ is the set

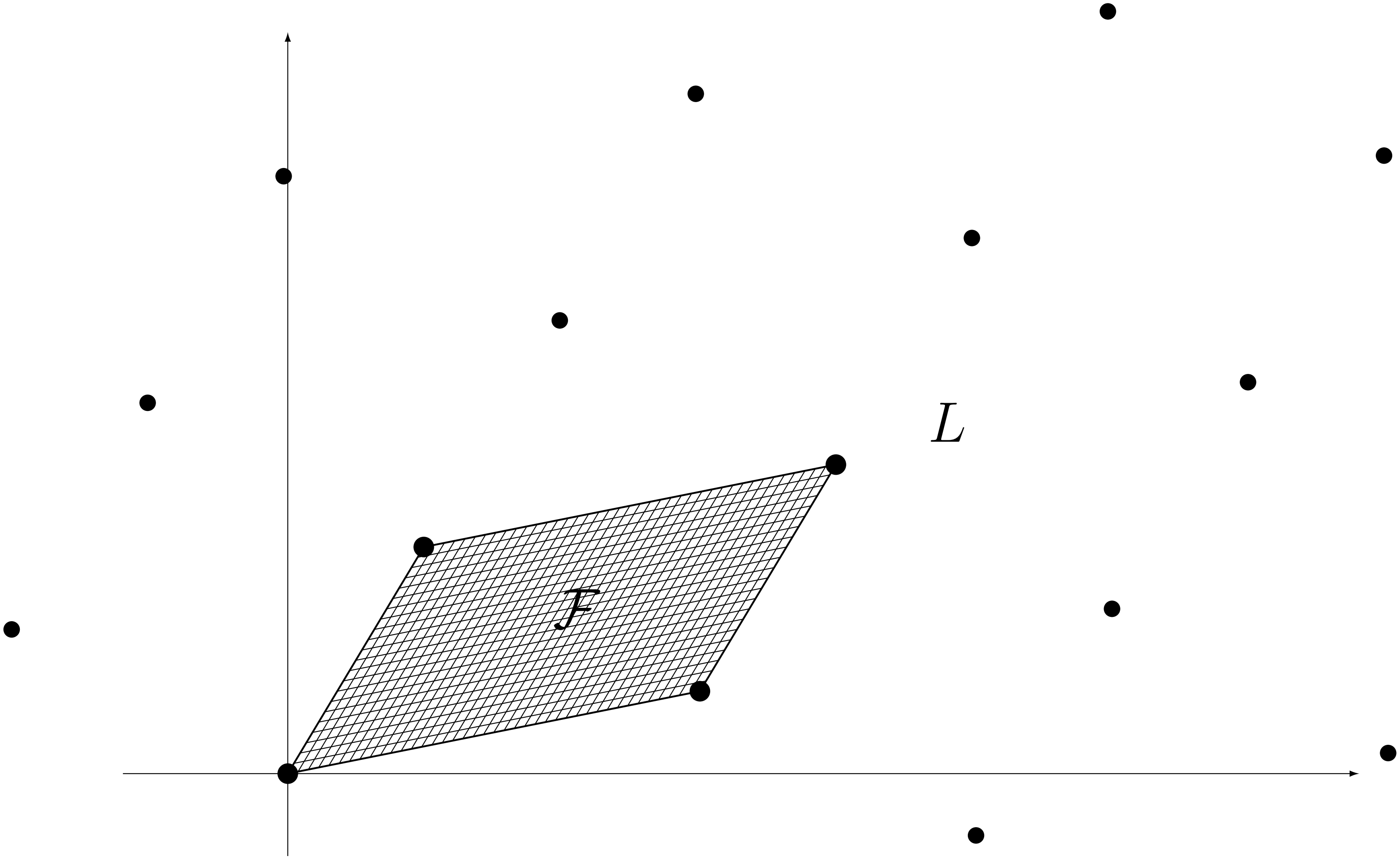
$$\mathcal{F}(\mathcal{B}) = \{t_1\boldsymbol{v}_1 + t_2\boldsymbol{v}_2 + \cdots + t_n\boldsymbol{v}_n : 0 \le t_i < 1\}.$$

The **(absolute) determinant** (or "volume") of L is

$$\operatorname{Det}(L) = \operatorname{Volume}(\mathcal{F}(\mathcal{B})) = \left|\det\big(\boldsymbol{v}_1|\boldsymbol{v}_2|\cdots|\boldsymbol{v}_n\big)\right|.$$

It is independent of the choice of basis.

A Two Dimensional Example



A 2-dimensional lattice L with fundamental domain $\mathcal{F}$

The Two Fundamental Hard Lattice Problems

Let L be a lattice of dimension n. The two most important computational problems are:

Shortest Vector Problem (SVP)

Find a shortest nonzero vector in L.

Closest Vector Problem (CVP)

Given a target vector $\boldsymbol{t} \in \mathbb{R}^n$, find a vector in L that is closest to $\boldsymbol{t}$.

More generally, one may ask for a vector that is not too much longer than the shortest, or a vector that is not too much further away than the closest. These are the

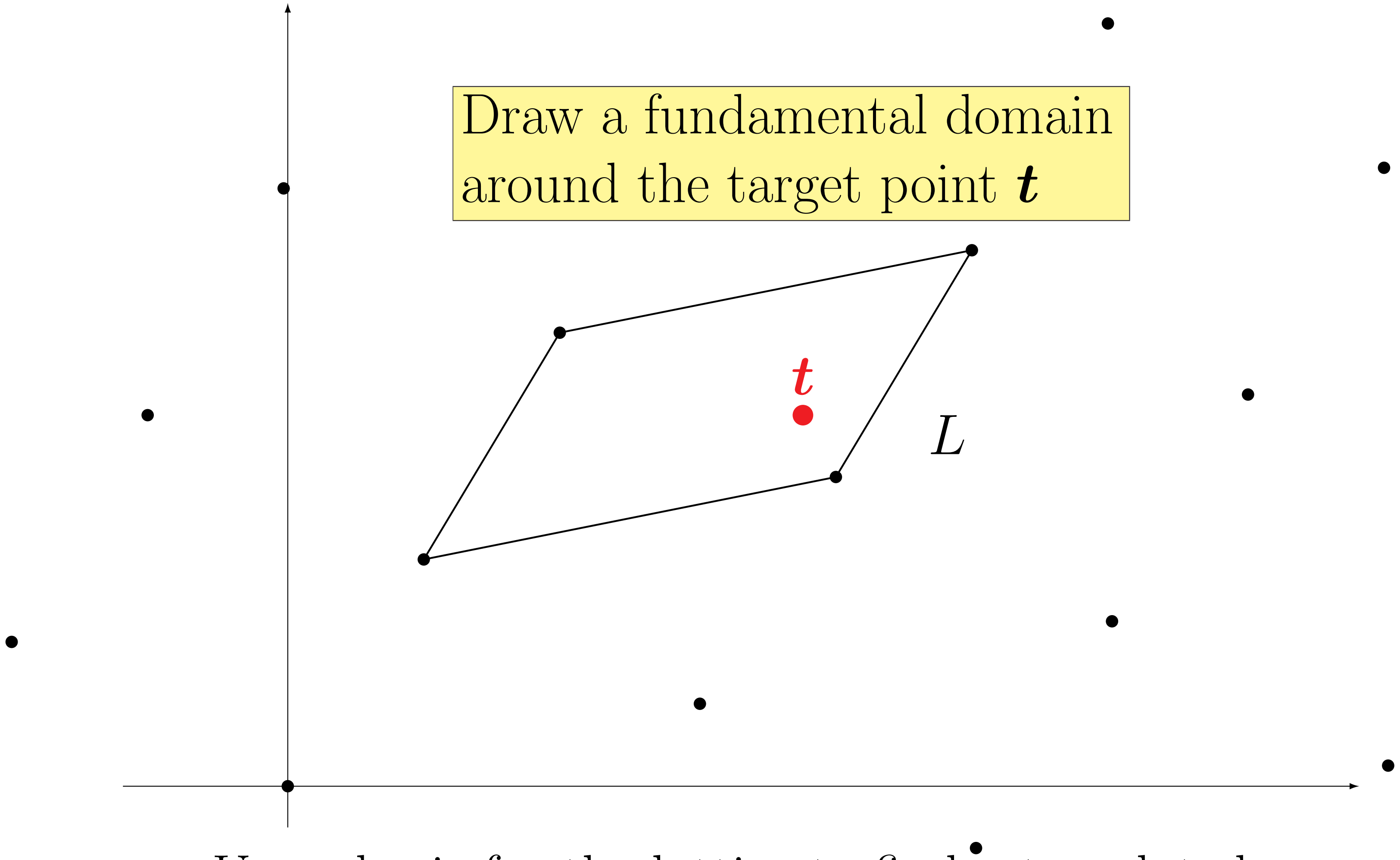
Approximate Shortest Vector Problem

and

Approximate Closest Vector Problem,

denoted **apprSVP** and **apprCVP**.

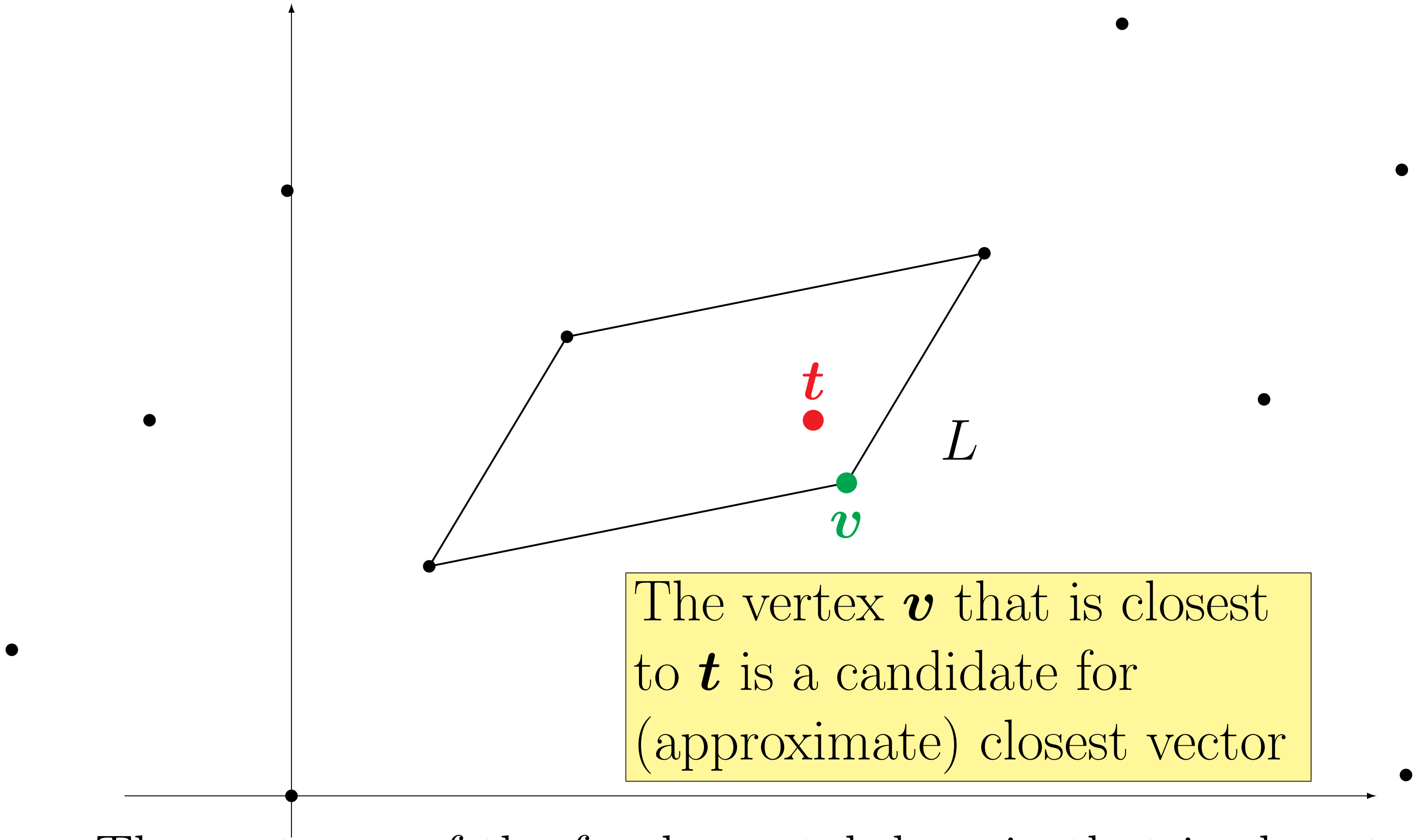
Using a Basis to Try to Solve the Closest Vector Problem



Draw a fundamental domain around the target point $\boldsymbol{t}$

Use a basis for the lattice to find a translated fundamental domain containing the target point.

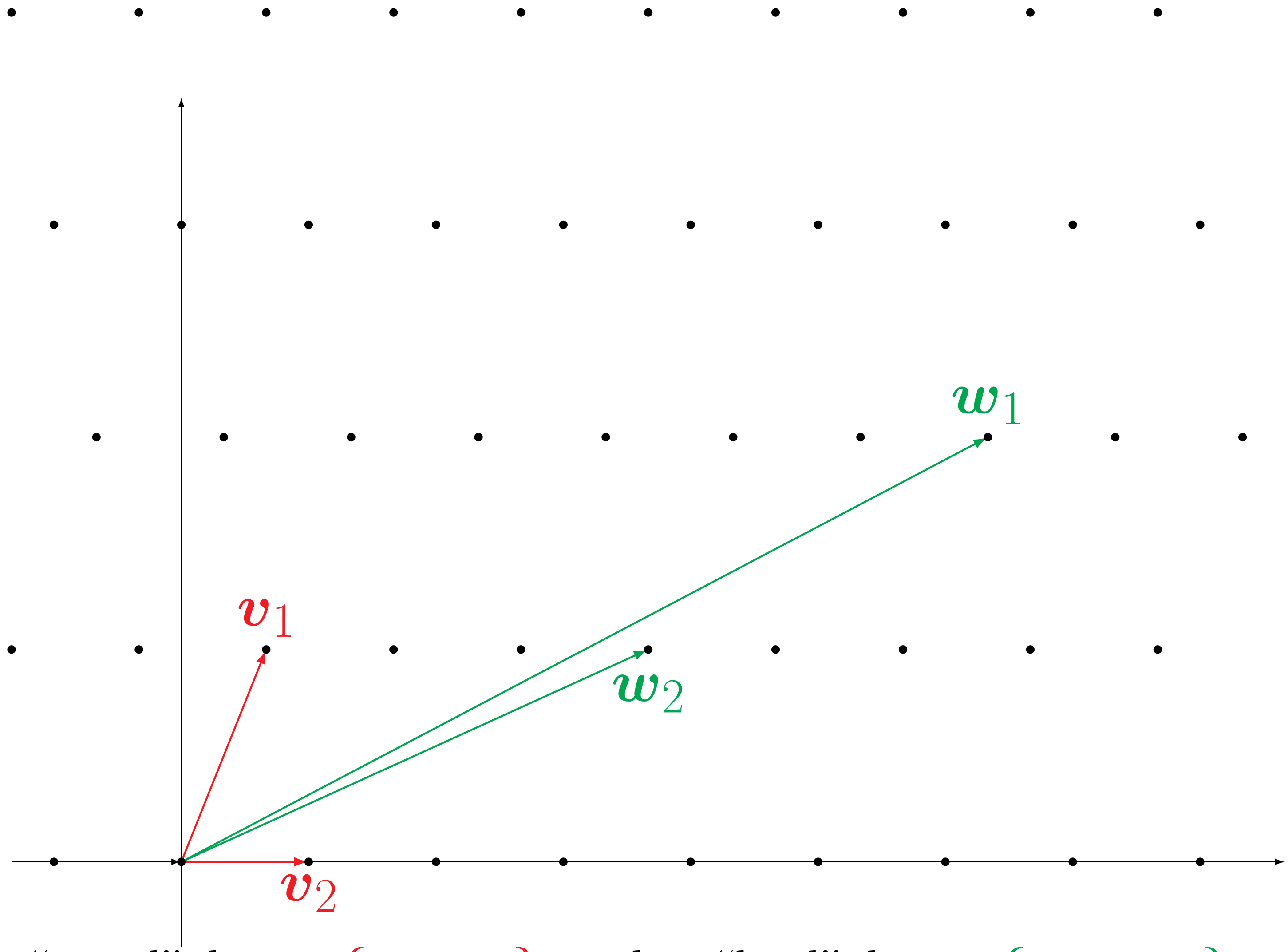
Babai’s Closest Vertex Solution to the apprCVP



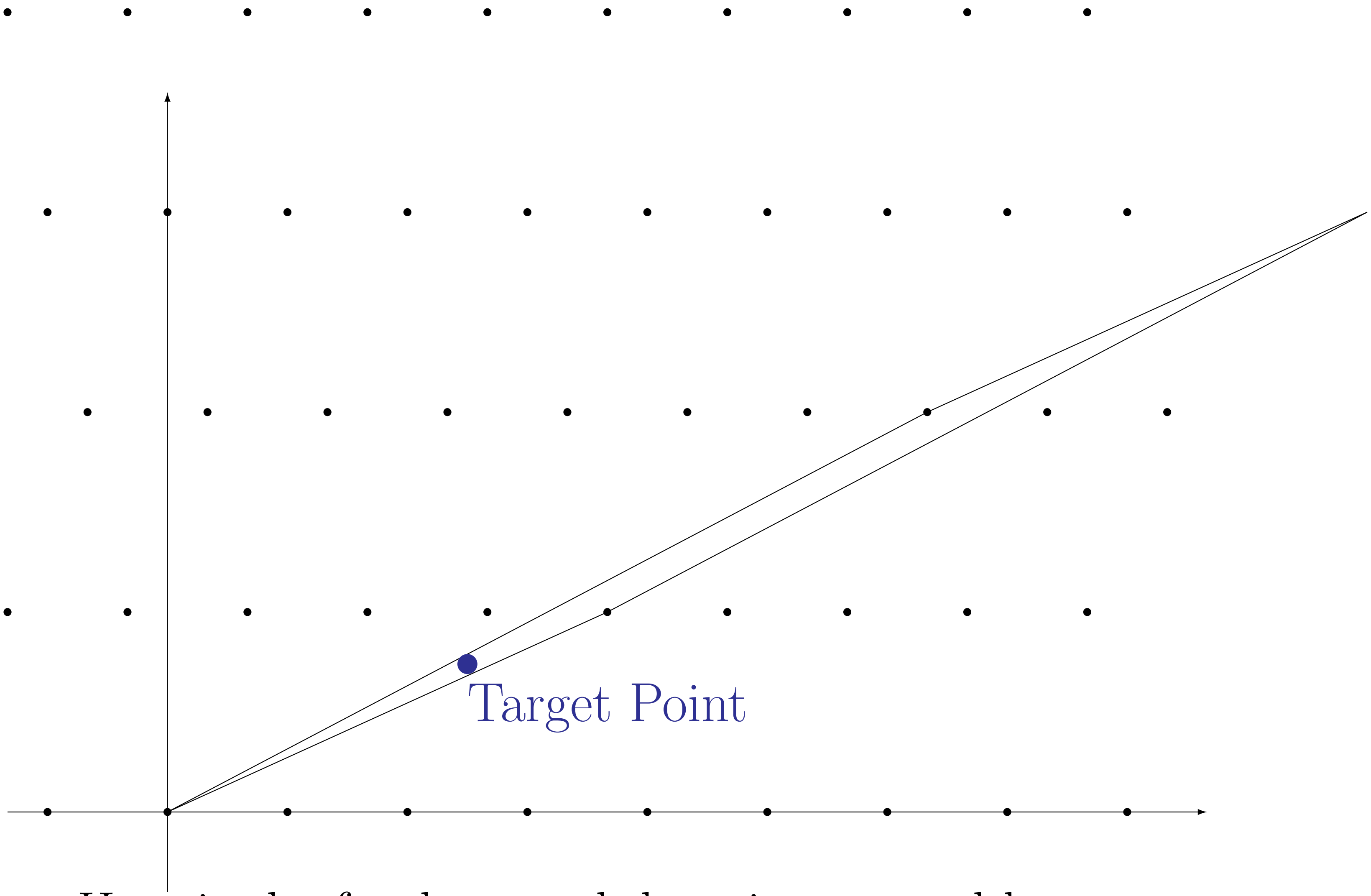
The vertex $\boldsymbol{v}$ that is closest to $\boldsymbol{t}$ is a candidate for (approximate) closest vector

The vertex $\boldsymbol{v}$ of the fundamental domain that is closest to $\boldsymbol{t}$ will be a close lattice point if the basis is “good”, meaning if the basis consists of vectors that are reasonably orthogonal to one another.

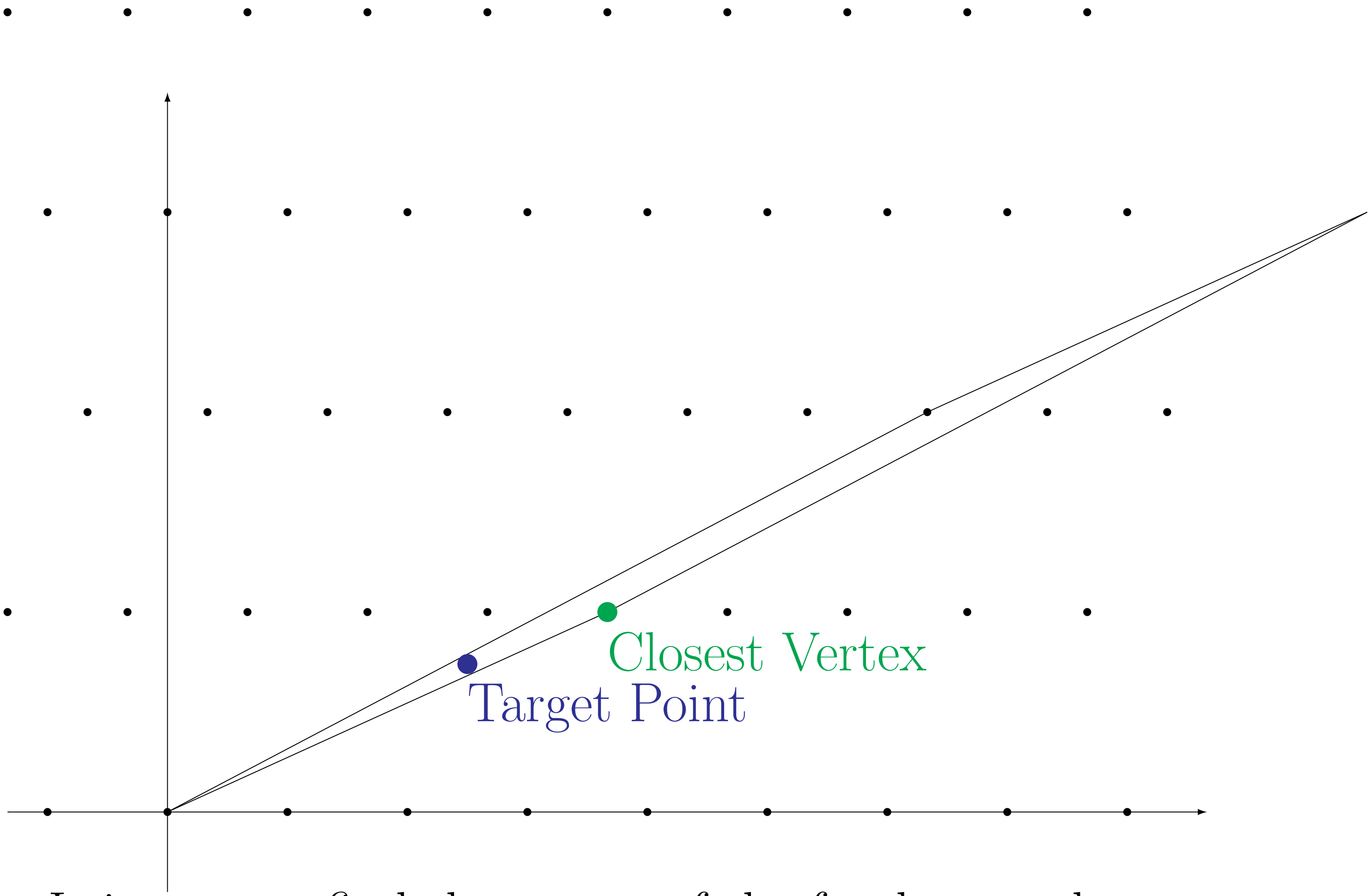
Good and Bad Bases



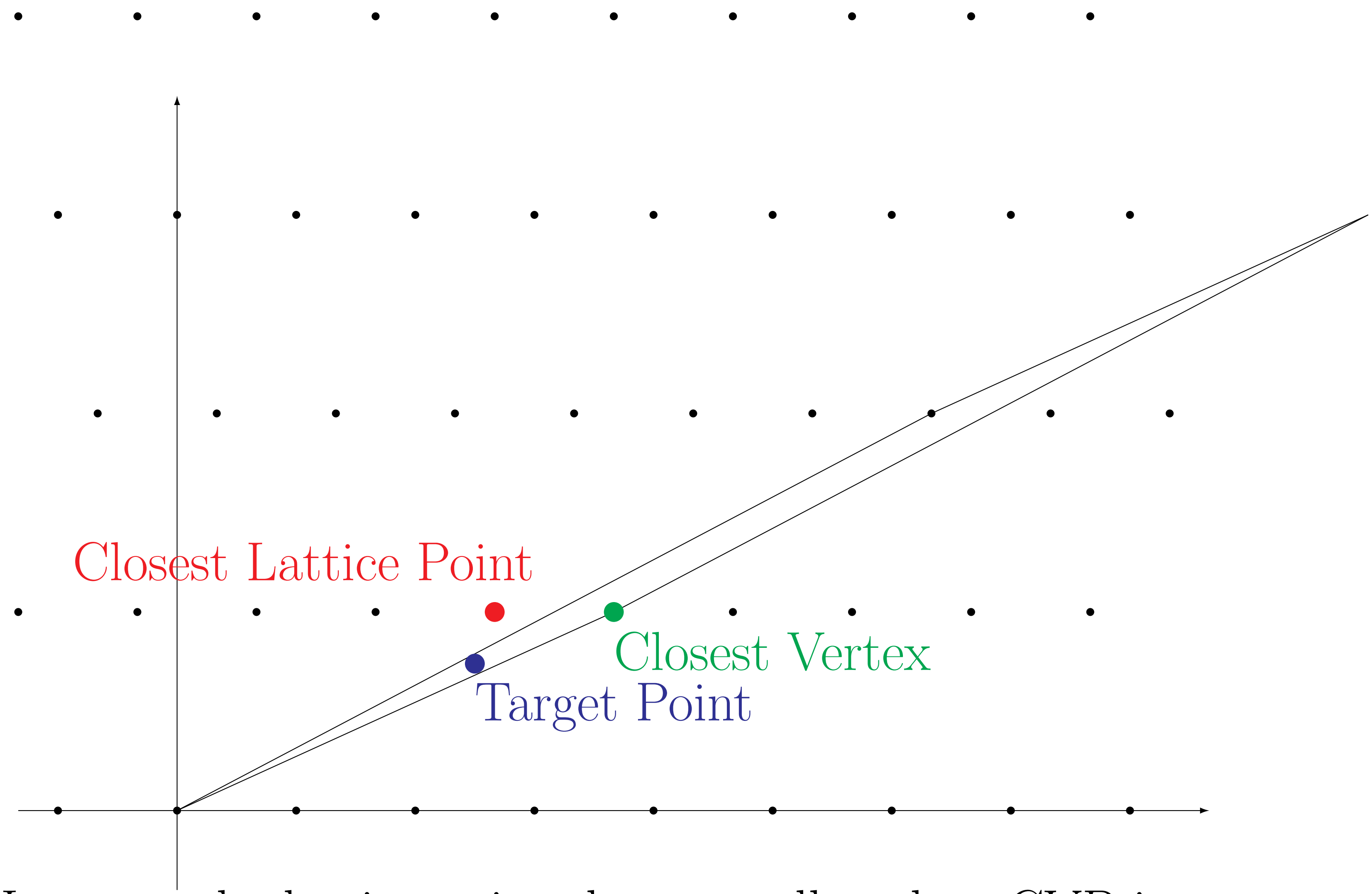
A "good" basis $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ and a "bad" basis $\{\boldsymbol{w}_1, \boldsymbol{w}_2\}$



Here is the fundamental domain spanned by a “bad” basis and a CVP target point



It is easy to find the vertex of the fundamental domain that is closest to the target point



However, the lattice point that actually solves CVP is much closer to the target than the closest vertex

Theory and Practice

Lattices, SVP and CVP, have been intensively studied for more than 100 years, both as intrinsic mathematical problems and for applications in pure and applied mathematics, physics and cryptography.

The theoretical study of lattices is often called the

Geometry of Numbers,

a name bestowed on it by Minkowski in his 1910 book *Geometrie der Zahlen*. That is our topic for today.

The practical process of finding short(est) or close(st) vectors in lattices is called **Lattice Reduction**. That will be tomorrow's topic .

Lattice reduction methods have been extensively developed for applications to number theory, computer algebra, discrete mathematics, applied mathematics, combinatorics, cryptography,. . .

How Orthogonal is a Basis of a Lattice?

Hademard's Inequality. Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be any basis for L. Then

$$\mathrm{Det}(L) \leq \|\boldsymbol{v}_1\| \cdot \|\boldsymbol{v}_2\| \cdots \|\boldsymbol{v}_n\|.$$

Hadamard's inequality is true because the volume of a parallelopiped is never greater than the product of the lengths of its sides.

Hadamard's inequality is an equality if and only if the basis vectors are orthogonal (perpendicular) to one another. The extent to which it is an inequality measures the extent to which the basis is non-orthogonal.

A famous theorem of Minkowski says that every lattice has a basis that is reasonably orthogonal, where the amount of non-orthogonality is bounded solely in terms of the dimension.

A Fundamental Lattice Theorem from the 19th Century

Theorem. (Minkowski): There is a constant γ_n so that for all lattices L of dimension n:

(a) There is a nonzero vector $\boldsymbol{v} \in L$ satisfying

$$\|\boldsymbol{v}\| \le \gamma_n \operatorname{Det}(L)^{1/n}.$$

(b) There is a basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ for L satisfying

$$\|\boldsymbol{v}_1\| \cdot \|\boldsymbol{v}_2\| \cdots \|\boldsymbol{v}_n\| \le \gamma_n^{n/2} \operatorname{Det}(L).$$

The constant γ_n is called **Hermite's constant**. It is known that for large n,

$$\boxed{\sqrt{\frac{n}{2\pi e}} \lesssim \gamma_n \lesssim \sqrt{\frac{n}{\pi e}},}$$

but the exact value of γ_n is known only for $n \le 8$ and $n = 24$.

Finding Points in Lattices — A Theoretical Result

I will start by sketching a proof of the following important resul. Minkowski's theorem will be an immediate consequence.

(See the lecture notes for an alternative proof using Voronoi cells.)

Lattice Point Lemma. (Minkowski): Let L be a lattice of dimension n. Then every compact convex symmetric region $\mathcal{R}$ of volume at least $2^n \operatorname{Det}(L)$ contains a nonzero lattice point.

The region $\mathcal{R}$ is assumed to have the following three properties:

Compact: closed and bounded

Convex: $\boldsymbol{v}, \boldsymbol{w} \in \mathcal{R} \implies$ line segment $\overline{\boldsymbol{v}\boldsymbol{w}} \subset \mathcal{R}$

Symmetric: $\boldsymbol{v} \in \mathcal{R} \implies -\boldsymbol{v} \in \mathcal{R}$

Proof of the Lattice Point Lemma

Let $\mathcal{R} \subset \mathbb{R}^n$ be a compact convex symmetric region with

$$\mathrm{Vol}(\mathcal{R}) > 2^n \,\mathrm{Det}(L).$$

Goal: Prove that $\mathcal{R}$ contains a nonzero lattice point.

Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be a basis for L and let

$$\mathcal{F} = \left\{ t_1 \boldsymbol{v}_1 + \cdots + t_n \boldsymbol{v}_n : 0 \le t_i < 1 \right\}$$

be the associated fundamental domain for L.

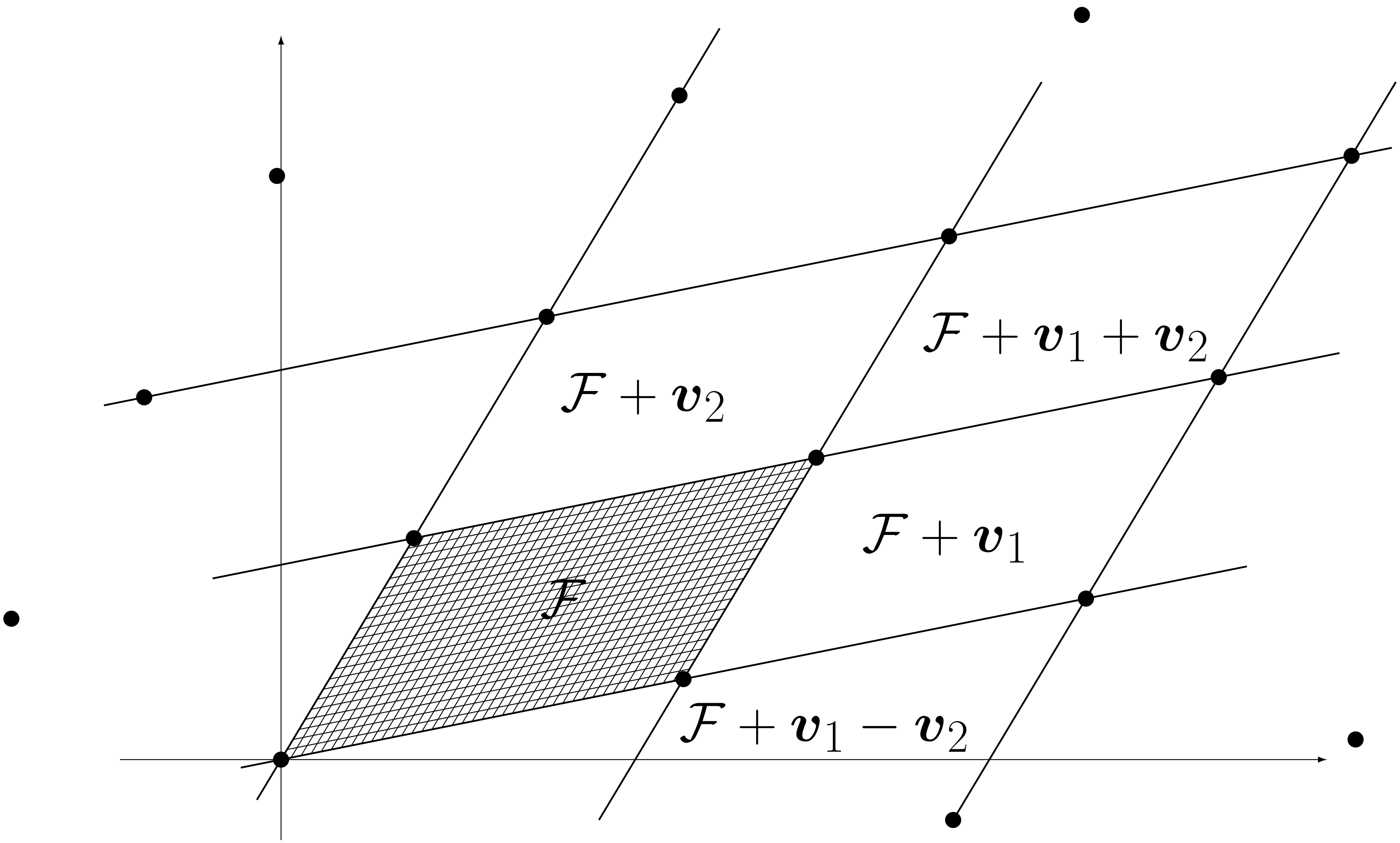
For each $\boldsymbol{v} \in L$, we look at the translation of $\mathcal{F}$,

$$\mathcal{F} + \boldsymbol{v} = \{ \boldsymbol{w} + \boldsymbol{v} : \boldsymbol{w} \in \mathcal{F} \}.$$

As $\boldsymbol{v}$ varies over L, the translates $\mathcal{F} + \boldsymbol{v}$ cover all of $\mathbb{R}^n$,

$$\bigcup_{\boldsymbol{v} \in L} (\mathcal{F} + \boldsymbol{v}) = \mathbb{R}^n.$$

Translations of $\mathcal{F}$ By Vectors in L


$\mathcal{F} + \boldsymbol{v}_1 + \boldsymbol{v}_2$
$\mathcal{F} + \boldsymbol{v}_2$
$\mathcal{F} + \boldsymbol{v}_1$
$\mathcal{F}$
$\mathcal{F} + \boldsymbol{v}_1 - \boldsymbol{v}_2$

Translating the fundamental domain $\mathcal{F}$ using the vectors in the lattice L covers all of $\mathbb{R}^n$.

Proof of the Lattice Point Lemma (continued)

In particular, each $\boldsymbol{r} \in \mathcal{R}$ can be written uniquely in the form

$$\boldsymbol{r} = \boldsymbol{v}_{\boldsymbol{r}} + \boldsymbol{w}_{\boldsymbol{r}} \quad \text{with } \boldsymbol{v}_{\boldsymbol{r}} \in L \text{ and } \boldsymbol{w}_{\boldsymbol{r}} \in \mathcal{F}.$$

In other words, take $\boldsymbol{r}$ and translate it by an element of L so that it lies in $\mathcal{F}$.

We dilate (shrink) $\mathcal{R}$ by a factor of 2,

$$\tfrac{1}{2}\mathcal{R} = \left\{\tfrac{1}{2}\boldsymbol{r} : \boldsymbol{r} \in \mathcal{R}\right\},$$

and consider the map

$$\tfrac{1}{2}\mathcal{R} \longrightarrow \mathcal{F}, \qquad \tfrac{1}{2}\boldsymbol{r} \longmapsto \boldsymbol{w}_{\frac{1}{2}\boldsymbol{r}}.$$

Shrinking by a factor of 2 changes volume by a factor of 2^n, so

$$\operatorname{Vol}\left(\tfrac{1}{2}\mathcal{R}\right) = \frac{1}{2^n}\operatorname{Vol}(\mathcal{R}) > \operatorname{Vol}(\mathcal{F}).$$

So there must be two *different* points $\frac{1}{2}\boldsymbol{r}_1$ and $\frac{1}{2}\boldsymbol{r}_2$ in $\frac{1}{2}\mathcal{R}$ with the same image in $\mathcal{F}$.

Proof of the Lattice Point Lemma (continued)

We have found two points in $\frac{1}{2}\mathcal{R}$ satisfying

$$\frac{1}{2}\boldsymbol{r}_1 = \boldsymbol{v}_1 + \boldsymbol{w} \quad \text{and} \quad \frac{1}{2}\boldsymbol{r}_2 = \boldsymbol{v}_2 + \boldsymbol{w}$$
$$\text{with} \quad \boldsymbol{v}_1, \boldsymbol{v}_2 \in L \quad \text{and} \quad \boldsymbol{w} \in \mathcal{F}.$$

Subtracting them yields a nonzero vector

$$\frac{1}{2}\boldsymbol{r}_1 - \frac{1}{2}\boldsymbol{r}_2 = \boldsymbol{v}_1 - \boldsymbol{v}_2 \in L.$$

We now observe that

$$\underbrace{\frac{1}{2}\boldsymbol{r}_1 + \overbrace{\left(-\frac{1}{2}\boldsymbol{r}_2\right)}^{\substack{\mathcal{R}\text{ is symmetric}\\ \text{so } -\boldsymbol{r}_2 \text{ is in } \mathcal{R}}}}_{\substack{\text{this is the midpoint of the line}\\ \text{segment from } \boldsymbol{r}_1 \text{ to } -\boldsymbol{r}_2,\\ \text{so it is in } \mathcal{R} \text{ by convexity}}}$$

Hence

$$\mathbf{0} \neq \boldsymbol{v}_1 - \boldsymbol{v}_2 \in \mathcal{R} \cap L.$$

Proof of the Lattice Point Lemma (finalé)

This completes the proof of the Lattice Point Lemma assuming

$$\mathrm{Vol}(\mathcal{R}) > 2^n \,\mathrm{Det}(L).$$

To deal with regions satisfying

$$\mathrm{Vol}(\mathcal{R}) = 2^n \,\mathrm{Det}(L)$$

we apply our result to find nonzero points

$$\mathbf{0} \neq \boldsymbol{v}_k \in \left(1 + \tfrac{1}{k}\right)\mathcal{R} \cap L \quad \text{for each } k = 1, 2, 3, \ldots.$$

The lattice points $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots$ are all in $2\mathcal{R}$, so there are only finitely many possibilities for them. Hence there is a nonzero lattice point $\boldsymbol{v} \in L$ in the intersection

$$\bigcap_{k=1}^{\infty} \left(1 + \tfrac{1}{k}\right)\mathcal{R} = \mathcal{R}.$$

Note that they are equal because $\mathcal{R}$ is compact. QED

Corollary. (Minkowski's Theorem Part (a)) A lattice L of dimension n always has a nonzero point $\boldsymbol{v} \in L$ of length at most

$$\|\boldsymbol{v}\| \lesssim \sqrt{\frac{2n}{\pi e}}\,\mathrm{Det}(L)^{1/n}$$

Proof. Let $\mathbb{B}_R^n \subset \mathbb{R}^n$ be a ball of radius R,

$$\bigl(\{\boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x}\| \le R\}\bigr).$$

If n is reasonably large, then $\mathbb{B}_R^n$ has volume

$$\mathrm{Vol}(\mathbb{B}_R^n) \approx \left(\frac{2\pi e}{n}\right)^{n/2} R^n.$$

Hence if we take $R \approx \sqrt{2n/\pi e}\,\mathrm{Det}(L)^{1/n}$, then we get

$$\mathrm{Vol}(\mathbb{B}_R^n) \gtrsim 2^n\,\mathrm{Det}(L).$$

the Lattice Point Lemma tells us that $\mathbb{B}_R^n$ contains a nonzero lattice point. QED

The Gaussian Heuristic

If $L \subset \mathbb{R}^n$ is a "random" lattice and $\boldsymbol{t} \in \mathbb{R}^n$ is a "random" target point, how far would we expect $\boldsymbol{t}$ to be from L? The following heuristic answer tends to work reasonably well in practice.

Gaussian Heuristic. For a random lattice $L \subset \mathbb{R}^n$ and random point $\boldsymbol{t} \in \mathbb{R}^n$, we expect

$$\min_{\boldsymbol{v} \in L} \|\boldsymbol{v} - \boldsymbol{t}\| \approx \sqrt{\frac{n}{2\pi e}}\,\mathrm{Det}(L)^{1/n}.$$

The Gaussian Heuristic

Gaussian Heuristic. For a random lattice $L \subset \mathbb{R}^n$ and random point $\boldsymbol{t} \in \mathbb{R}^n$, we expect

$$\min_{\boldsymbol{v} \in L} \|\boldsymbol{v} - \boldsymbol{t}\| \approx \sqrt{\frac{n}{2\pi e}}\, \mathrm{Det}(L)^{1/n}.$$

Justification: The volume of the ball $\mathbb{B}_R^n(\boldsymbol{t})$ of radius R centered at $\boldsymbol{t}$ has volume

$$\mathrm{Vol}\big(\mathbb{B}_R^n(\boldsymbol{t})\big) = \mathrm{Vol}\big(\mathbb{B}_1(\mathbf{0})\big) R^n \approx \left(\frac{2\pi e}{n}\right)^{n/2} R^n.$$

A fundamental domain $\mathcal{F}$ for L has volume $\mathrm{Det}(L)$, and the tranlated fundamental domains $\mathcal{F} + \boldsymbol{v}$ cover $\mathbb{R}^n$. So we expect $\mathbb{B}_R^n(\boldsymbol{t})$ to contain a point of L if its volume (significantly) exceeds $\mathrm{Det}(L)$. Setting

$$\mathrm{Vol}\big(\mathbb{B}_R^n(\boldsymbol{t})\big) = \mathrm{Det}(L)$$

and solving for R gives the Gaussian heuristic.

The Successive Minima of a Lattice

The *first minimum of* L, denoted $\lambda_1(L)$, is the length of shortest non-zero vector in L,

$$\lambda_1(L) = \inf_{\boldsymbol{v}\in L\smallsetminus\mathbf{0}} \|\boldsymbol{v}\|.$$

More generally, the *k'th successive minimum of* L, denoted $\lambda_k(L)$, is the smallest number such that L contains k vectors that are linearly independent, i.e.,

$$\lambda_k(L) = \inf\Bigl\{\lambda > 0 : \dim \operatorname{Span}\bigl\{\boldsymbol{v} \in L : \|\boldsymbol{v}\| \le \lambda\bigr\} \ge k\Bigr\}.$$

With this notation, a general version of Minkowski's Theorem says that

$$\lambda_1\lambda_2\cdots\lambda_k \le \gamma^{k/2}\operatorname{Det}(L)^{k/n}.$$

An Introduction to Lattices, Lattice Reduction, and Lattice-Based Cryptography

Joseph H. Silverman

Brown University

PCMI Lecture Series

July 6–10, 2020