Random Lattices as Sphere Packings

Presentation by

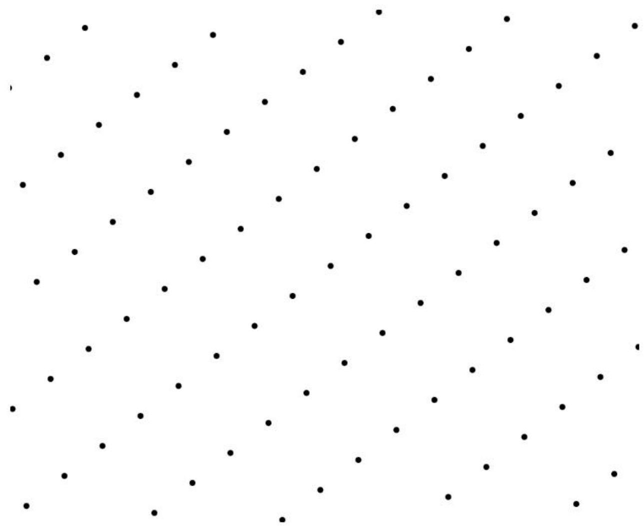
Nihar P. Gargava

Doctoral student,
Chair of Number Theory,
Section of Mathematics,
École Polytechnique Fédérale de Lausanne

29th November 2022

What is a lattice packing?

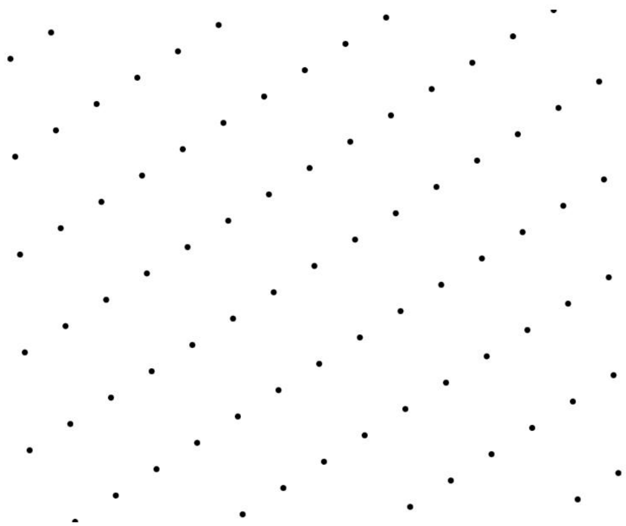
Visualizing in $\mathbb{R}^2$



What is a lattice packing?

Consider $\mathbb{R}^d$ with the standard inner product. A lattice $\Lambda \subseteq \mathbb{R}^d$ is a discrete subgroup such that the quotient space $\mathbb{R}^d / \Lambda$ has a finite induced volume.

Visualizing in $\mathbb{R}^2$

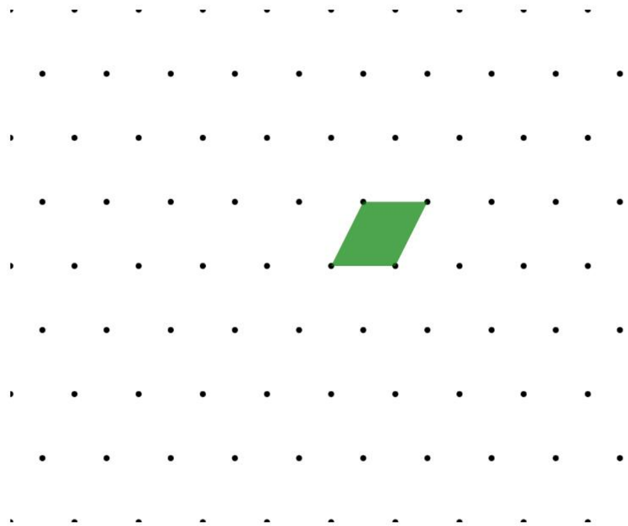


What is a lattice packing?

Consider $\mathbb{R}^d$ with the standard inner product. A lattice $\Lambda \subseteq \mathbb{R}^d$ is a discrete subgroup such that the quotient space $\mathbb{R}^d / \Lambda$ has a finite induced volume.

Given a lattice Λ, choose $r > 0$ and consider the open balls $\{B_r(v)\}_{v \in \Lambda}$ such for any $v_1, v_2 \in \Lambda$, $B_r(v_1) \cap B_r(v_2) \neq \emptyset \Rightarrow v_1 = v_2$.

Visualizing in $\mathbb{R}^2$

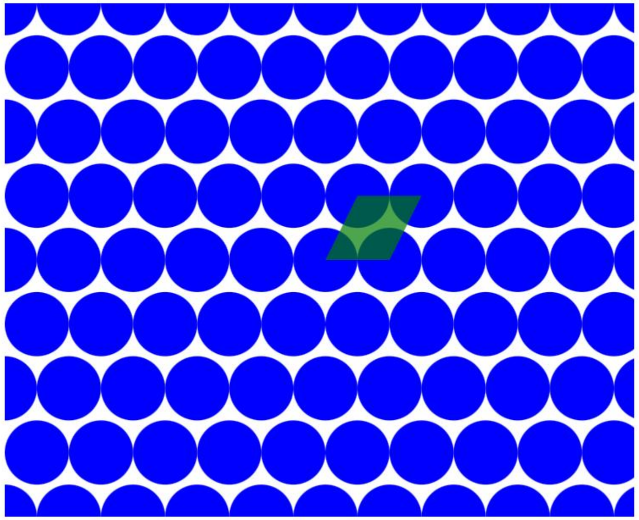


What is a lattice packing?

Consider $\mathbb{R}^d$ with the standard inner product. A lattice $\Lambda \subseteq \mathbb{R}^d$ is a discrete subgroup such that the quotient space $\mathbb{R}^d / \Lambda$ has a finite induced volume.

Given a lattice Λ, choose $r > 0$ and consider the open balls $\{B_r(v)\}_{v \in \Lambda}$ such for any $v_1, v_2 \in \Lambda$, $B_r(v_1) \cap B_r(v_2) \neq \emptyset \Rightarrow v_1 = v_2$.

Visualizing in $\mathbb{R}^2$



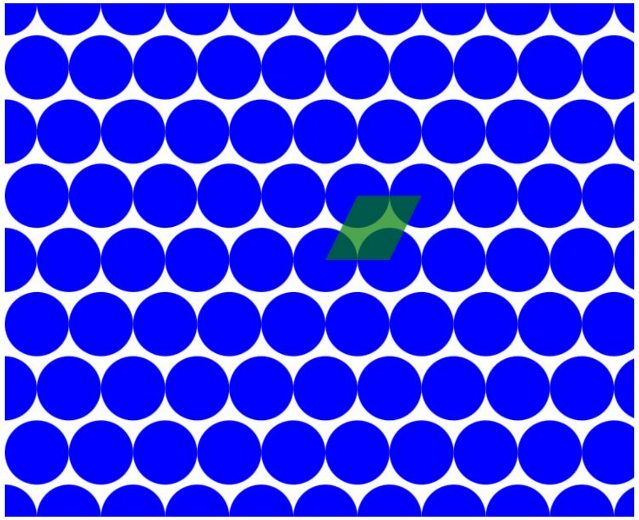
What is a lattice packing?

Consider $\mathbb{R}^d$ with the standard inner product. A lattice $\Lambda \subseteq \mathbb{R}^d$ is a discrete subgroup such that the quotient space $\mathbb{R}^d / \Lambda$ has a finite induced volume.

Given a lattice Λ, choose $r > 0$ and consider the open balls $\{B_r(v)\}_{v \in \Lambda}$ such for any $v_1, v_2 \in \Lambda$, $B_r(v_1) \cap B_r(v_2) \neq \emptyset \Rightarrow v_1 = v_2$.

Then (Λ, r) is called a lattice sphere packing, or simply lattice packing inside $(\mathbb{R}^d, \langle \, , \, \rangle)$.

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

Consider $\mathbb{R}^d$ with the standard inner product. A lattice $\Lambda \subseteq \mathbb{R}^d$ is a discrete subgroup such that the quotient space $\mathbb{R}^d / \Lambda$ has a finite induced volume.

Given a lattice Λ, choose $r > 0$ and consider the open balls $\{B_r(v)\}_{v \in \Lambda}$ such for any $v_1, v_2 \in \Lambda$, $B_r(v_1) \cap B_r(v_2) \neq \emptyset \Rightarrow v_1 = v_2$.

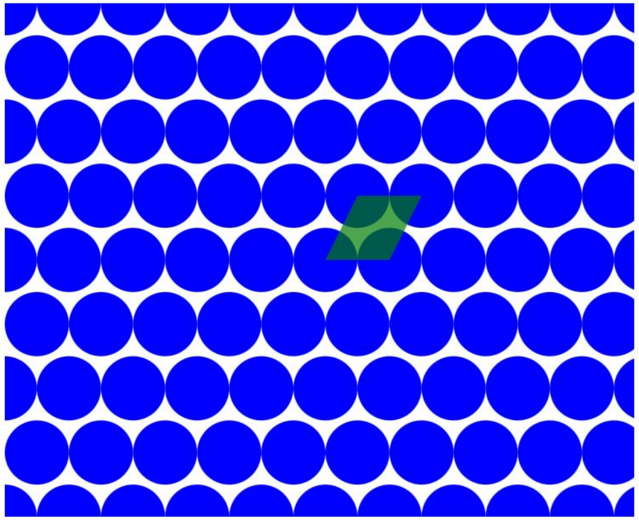
Then (Λ, r) is called a lattice sphere packing, or simply lattice packing inside $(\mathbb{R}^d, \langle\ ,\ \rangle)$.

Packing density of a lattice packing is:

$$\lim_{R \to \infty} \frac{\mu\left(B_R(0) \cap \left(\bigsqcup_{v \in \Lambda} B_r(v)\right)\right)}{\mu\left(B_R(0)\right)} = \frac{\mu(B_r(0))}{\mu(\mathbb{R}^d / \Lambda)}$$

It is always in the interval $[0, 1]$.

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

Consider $\mathbb{R}^d$ with the standard inner product. A lattice $\Lambda \subseteq \mathbb{R}^d$ is a discrete subgroup such that the quotient space $\mathbb{R}^d/\Lambda$ has a finite induced volume.

Given a lattice Λ, choose $r > 0$ and consider the open balls $\{B_r(v)\}_{v\in\Lambda}$ such for any $v_1, v_2 \in \Lambda$, $B_r(v_1) \cap B_r(v_2) \neq \emptyset \Rightarrow v_1 = v_2$.

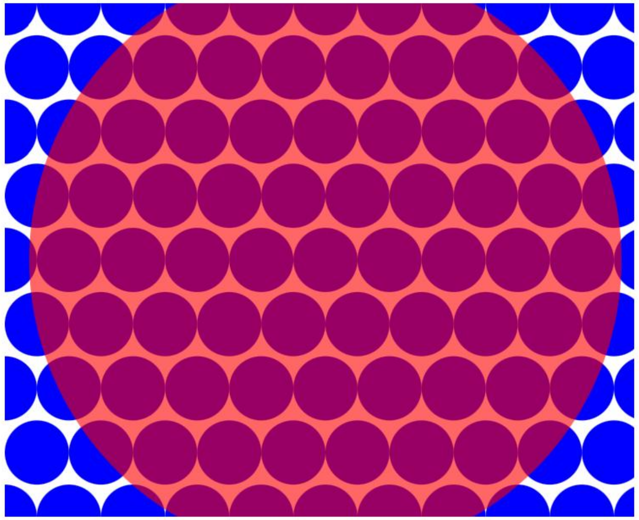
Then (Λ, r) is called a lattice sphere packing, or simply lattice packing inside $(\mathbb{R}^d, \langle\ ,\ \rangle)$.

Packing density of a lattice packing is:

$$\lim_{R\to\infty} \frac{\mu\left(B_R(0) \cap \left(\bigsqcup_{v\in\Lambda} B_r(v)\right)\right)}{\mu\left(B_R(0)\right)} = \frac{\mu(B_r(0))}{\mu(\mathbb{R}^d/\Lambda)}$$

It is always in the interval $[0,1]$.

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

Consider $\mathbb{R}^d$ with the standard inner product. A lattice $\Lambda \subseteq \mathbb{R}^d$ is a discrete subgroup such that the quotient space $\mathbb{R}^d / \Lambda$ has a finite induced volume.

Given a lattice Λ, choose $r > 0$ and consider the open balls $\{B_r(v)\}_{v \in \Lambda}$ such for any $v_1, v_2 \in \Lambda$, $B_r(v_1) \cap B_r(v_2) \neq \emptyset \Rightarrow v_1 = v_2$.

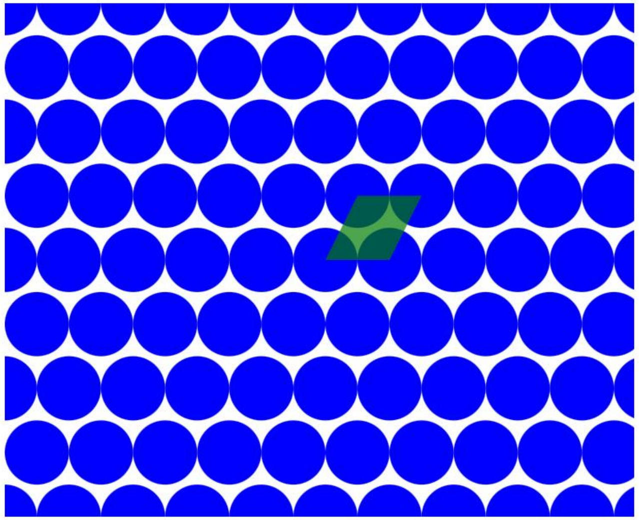
Then (Λ, r) is called a lattice sphere packing, or simply lattice packing inside $(\mathbb{R}^d, \langle \, , \, \rangle)$.

Packing density of a lattice packing is:

$$\lim_{R \to \infty} \frac{\mu\left(B_R(0) \cap \left(\bigsqcup_{v \in \Lambda} B_r(v)\right)\right)}{\mu\left(B_R(0)\right)} = \frac{\mu(B_r(0))}{\mu(\mathbb{R}^d / \Lambda)}$$

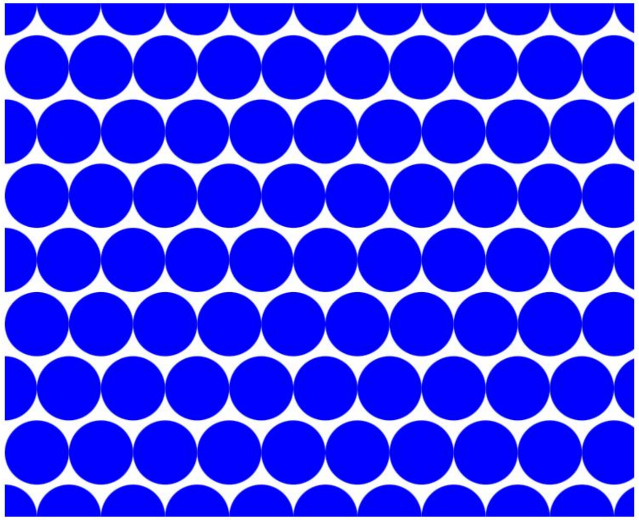
It is always in the interval $[0, 1]$.

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

Visualizing in $\mathbb{R}^2$



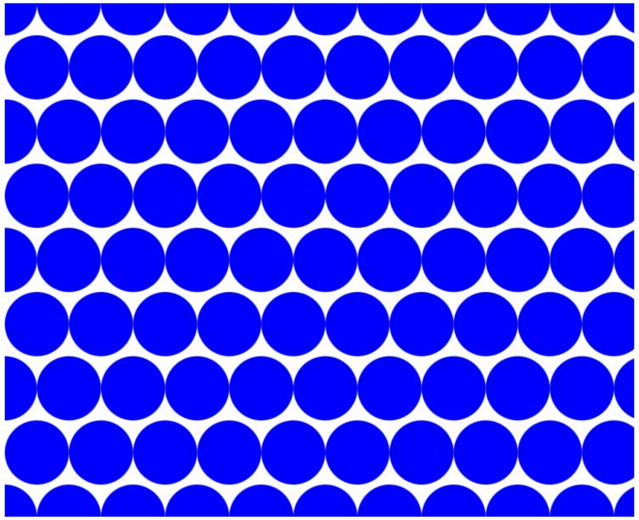
What is a lattice packing?

However, note that $2r$ can be at most

$$m(\Lambda) = \min_{v \in \Lambda \setminus \{0\}} ||v||,$$

otherwise some balls will begin to intersect.

Visualizing in $\mathbb{R}^2$



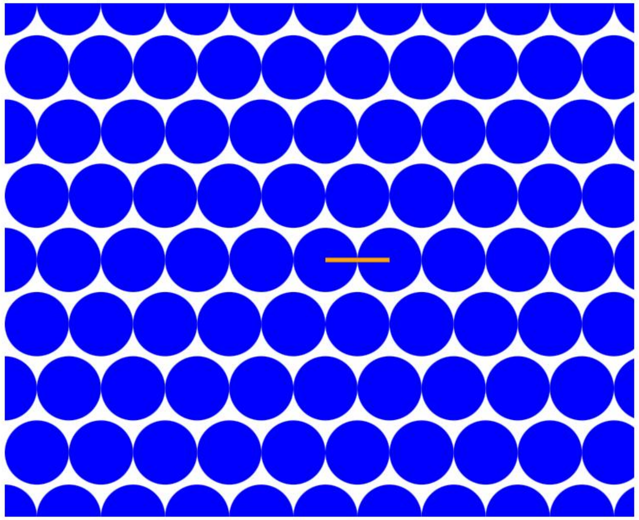
What is a lattice packing?

However, note that $2r$ can be at most

$$m(\Lambda) = \min_{v \in \Lambda \setminus \{0\}} ||v||,$$

otherwise some balls will begin to intersect.

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

However, note that $2r$ can be at most

$$m(\Lambda) = \min_{v \in \Lambda \setminus \{0\}} ||v||,$$

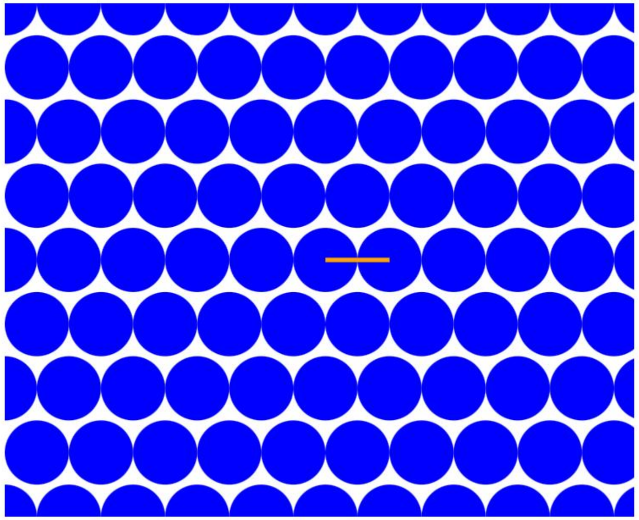
otherwise some balls will begin to intersect.

The goal is to maximize packing density. So take $r = \frac{1}{2} m(\Lambda)$. In that case packing density will be equal to

$$\frac{\mu(B_{m(\Lambda)/2}(0))}{\mu(\mathbb{R}^d\,/\Lambda)},$$

and is independent of scaling.

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

However, note that $2r$ can be at most

$$m(\Lambda) = \min_{v \in \Lambda \setminus \{0\}} ||v||,$$

otherwise some balls will begin to intersect.

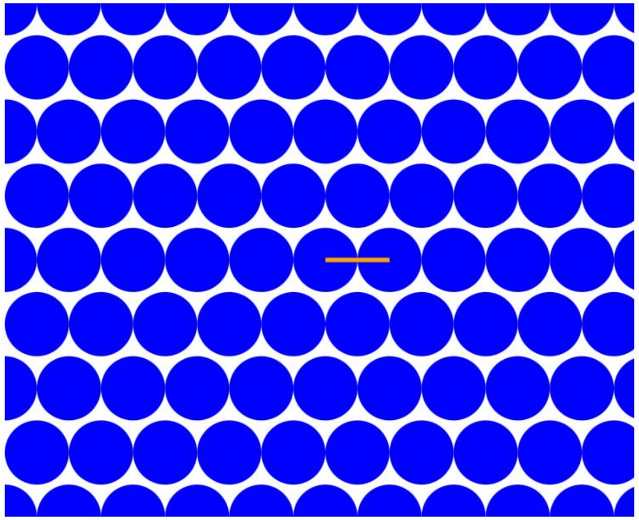
The goal is to maximize packing density. So take $r = \frac{1}{2} m(\Lambda)$. In that case packing density will be equal to

$$\frac{\mu(B_{m(\Lambda)/2}(0))}{\mu(\mathbb{R}^d \,/ \Lambda)},$$

and is independent of scaling.

To maximize this over all Λ, it is sufficient to maximize over unit covolume lattices (i.e. $\mu(\mathbb{R}^d \,/ \Lambda) = 1$)

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

However, note that $2r$ can be at most

$$m(\Lambda) = \min_{v \in \Lambda \setminus \{0\}} ||v||,$$

otherwise some balls will begin to intersect.

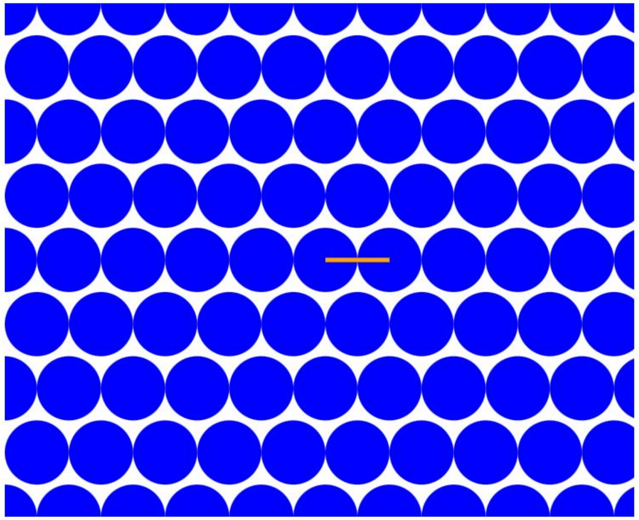
The goal is to maximize packing density. So take $r = \frac{1}{2}m(\Lambda)$. In that case packing density will be equal to

$$\frac{\mu(B_{m(\Lambda)/2}(0))}{\mu(\mathbb{R}^d / \Lambda)},$$

and is independent of scaling.

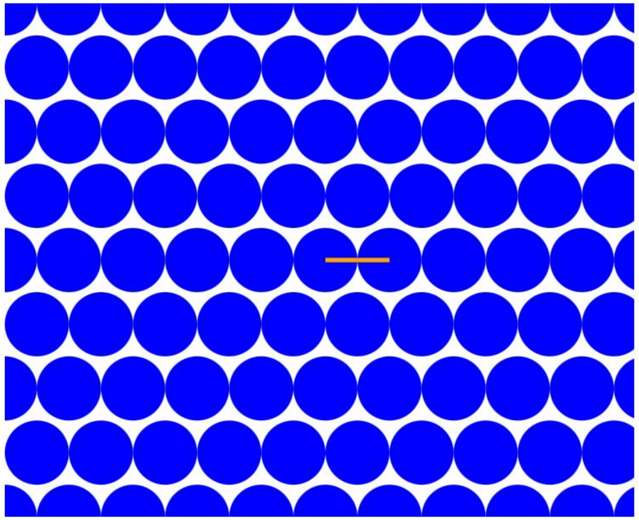
To maximize this over all Λ, it is sufficient to maximize over unit covolume lattices (i.e. $\mu(\mathbb{R}^d / \Lambda) = 1$)

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

Visualizing in $\mathbb{R}^2$

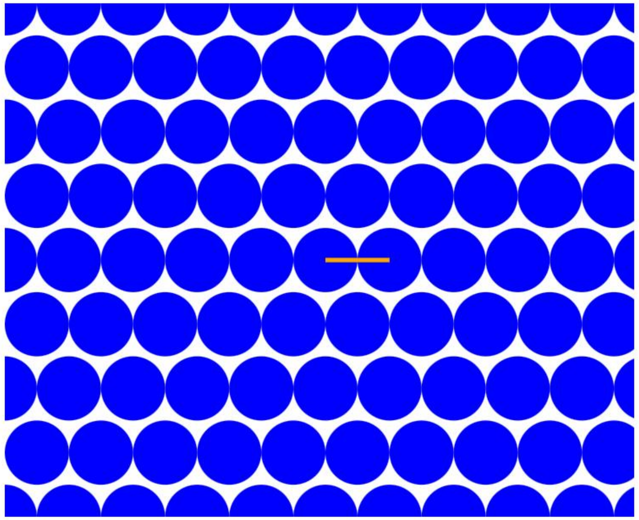


What is a lattice packing?

So we somehow find

$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

Visualizing in $\mathbb{R}^2$



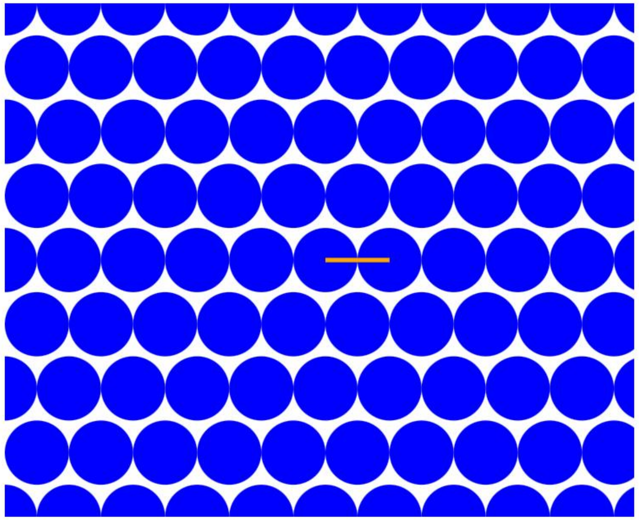
What is a lattice packing?

So we somehow find

$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

$$= \sup_{g \in SL_d(\mathbb{R})} \frac{1}{2^d} \mu\left(B_{m(g\mathbb{Z}^d)}(0)\right)$$

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

So we somehow find

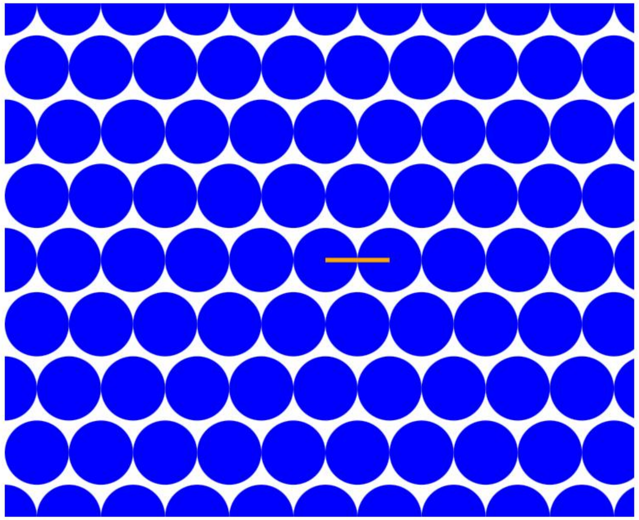
$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

$$= \sup_{g \in SL_d(\mathbb{R})} \frac{1}{2^d} \mu\left(B_{m(g\mathbb{Z}^d)}(0)\right)$$

which we use to define our dimensional constant c_d

$$:= \frac{1}{2^d} c_d$$

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

So we somehow find

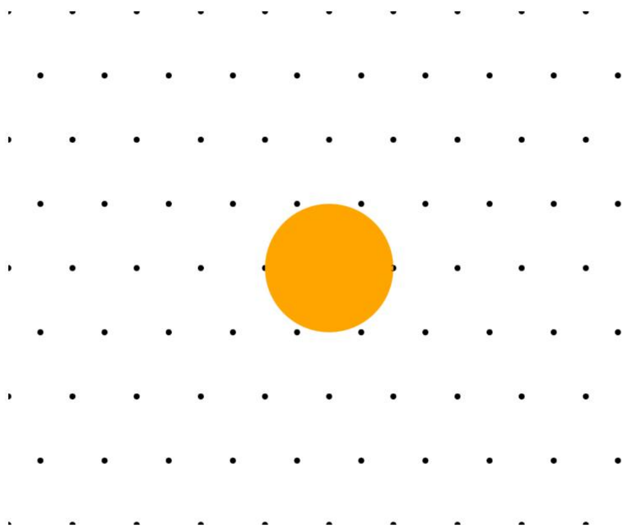
$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

$$= \sup_{g \in SL_d(\mathbb{R})} \frac{1}{2^d} \mu\left(B_{m(g\mathbb{Z}^d)}(0)\right)$$

which we use to define our dimensional constant c_d

$$:= \frac{1}{2^d} c_d$$

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

So we somehow find

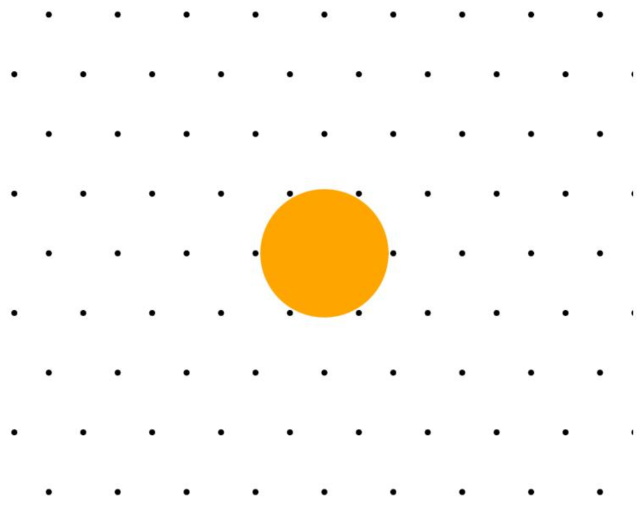
$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

$$= \sup_{g \in SL_d(\mathbb{R})} \frac{1}{2^d}\mu\left(B_{m(g\mathbb{Z}^d)}(0)\right)$$

which we use to define our dimensional constant c_d

$$:= \frac{1}{2^d}c_d$$

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

So we somehow find

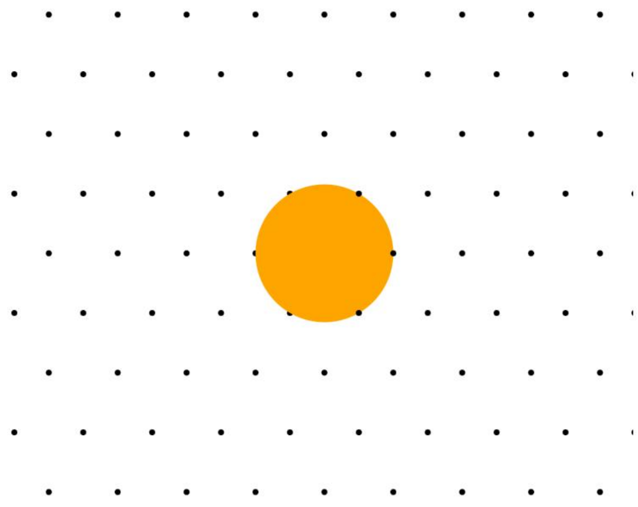
$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

$$= \sup_{g \in SL_d(\mathbb{R})} \frac{1}{2^d} \mu\left(B_{m(g\mathbb{Z}^d)}(0)\right)$$

which we use to define our dimensional constant c_d

$$:= \frac{1}{2^d} c_d$$

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

So we somehow find

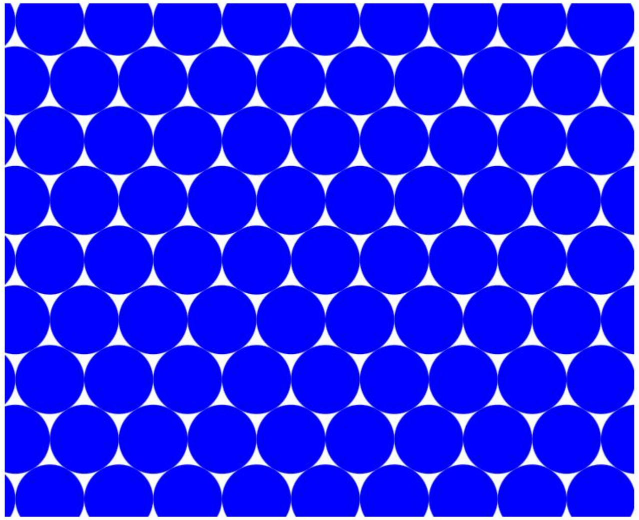
$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

$$= \sup_{g \in SL_d(\mathbb{R})} \frac{1}{2^d} \mu\left(B_{m(g\mathbb{Z}^d)}(0)\right)$$

which we use to define our dimensional constant c_d

$$:= \frac{1}{2^d} c_d$$

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

So we somehow find

$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

$$= \sup_{g \in SL_d(\mathbb{R})} \frac{1}{2^d} \mu\left(B_{m(g\mathbb{Z}^d)}(0)\right)$$

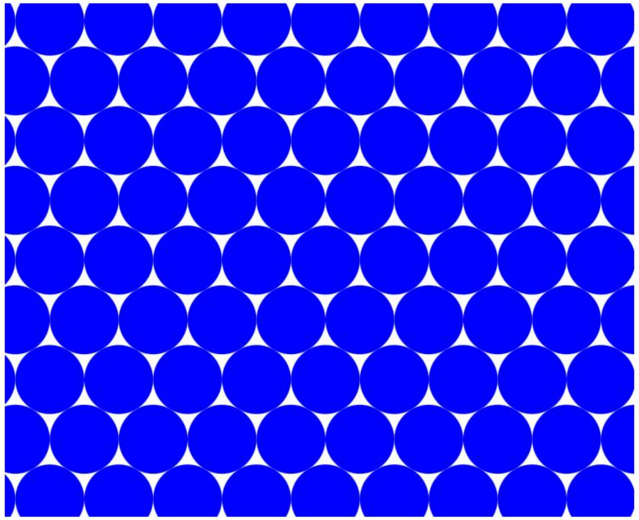
which we use to define our dimensional constant c_d

$$:= \frac{1}{2^d} c_d$$

Putting it together, we have

$$c_d = \sup\left\{\mu\left(B_r(0)\right) \mid r > 0, \exists\, g \in SL_d(\mathbb{R}) \text{ and } B_r(0) \cap g\mathbb{Z}^d = \{0\}\right\}.$$

Visualizing in $\mathbb{R}^2$



What is a lattice packing?

So we somehow find

$$\sup_{\substack{\Lambda \subseteq \mathbb{R}^d \\ \mu(\mathbb{R}^d/\Lambda)=1}} \mu\left(B_{m(\Lambda)/2}(0)\right)$$

$$= \sup_{g \in SL_d(\mathbb{R})} \frac{1}{2^d} \mu\left(B_{m(g\mathbb{Z}^d)}(0)\right)$$

which we use to define our dimensional constant c_d

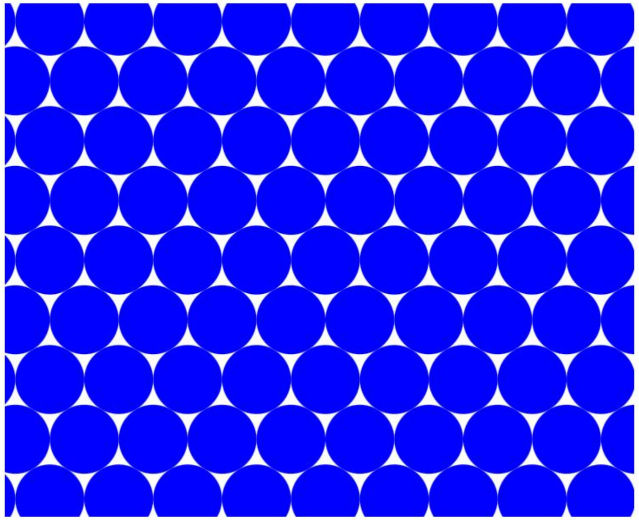
$$:= \frac{1}{2^d} c_d$$

Putting it together, we have

$$c_d = \sup\left\{\mu\left(B_r(0)\right) \mid r > 0, \exists\, g \in SL_d(\mathbb{R}) \text{ and } B_r(0) \cap g\mathbb{Z}^d = \{0\}\right\}.$$

Clearly, $c_d \in [0, 2^d]$, so supremum exists!

Visualizing in $\mathbb{R}^2$



What is known about c_d?

What is known about c_d?

The exact value of the constant c_d is known only for $d = \{1, 2, 3, 4, 5, 6, 7, 8, 24\}$. For other d, we want to understand the asymptotic behaviour. In this talk, we will only focus on lower bounds.

What is known about c_d?

The exact value of the constant c_d is known only for $d = \{1, 2, 3, 4, 5, 6, 7, 8, 24\}$. For other d, we want to understand the asymptotic behaviour. In this talk, we will only focus on lower bounds.

Some asymptotic lower bounds for large dimensions

Lower bound	Contribution of	Dimensions covered
$c_d \geq 1$	Minkowksi (1896)	$\forall\, d \geq 1$
$c_d \geq 2(d-1)$	Ball (1992)	$\forall\, d \geq 1$
$c_{4n} \geq 8.8n$	Vance (2011)	$d = 4n, n \geq 1$
$c_{2\varphi(n)} \geq n$	Venkatesh (2013)	$d = 2\varphi(k)$ for some k

What is known about c_d?

The exact value of the constant c_d is known only for $d = \{1, 2, 3, 4, 5, 6, 7, 8, 24\}$. For other d, we want to understand the asymptotic behaviour. In this talk, we will only focus on lower bounds.

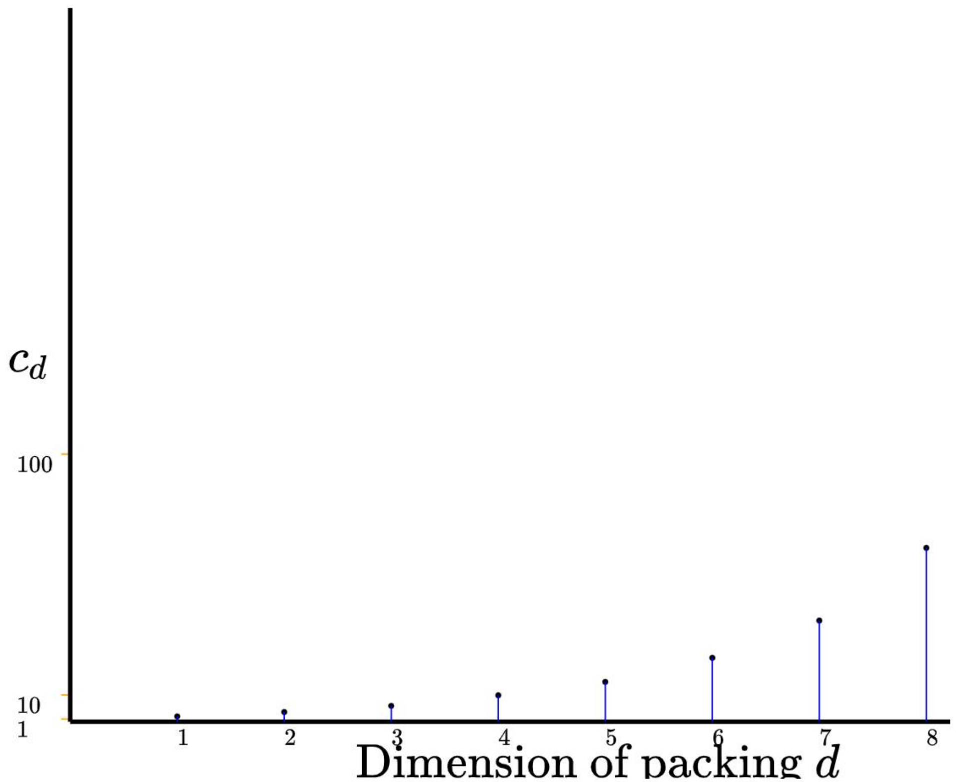
Some asymptotic lower bounds for large dimensions

Lower bound	Contribution of	Dimensions covered
$c_d \geq 1$	Minkowksi (1896)	$\forall\, d \geq 1$
$c_d \geq 2(d-1)$	Ball (1992)	$\forall\, d \geq 1$
$c_{4n} \geq 8.8n$	Vance (2011)	$d = 4n, n \geq 1$
$c_{2\varphi(n)} \geq n$	Venkatesh (2013)	$d = 2\varphi(k)$ for some k

Since $\liminf \left(\frac{\varphi(n)}{n} \log \log n \right) = e^{-\gamma}$, the last bound is the best lower bound (among these, and overall) on c_d in infinitely many dimensions. The first dimension where it outperforms all others in this list is $d = 960$.

What is known about c_d?

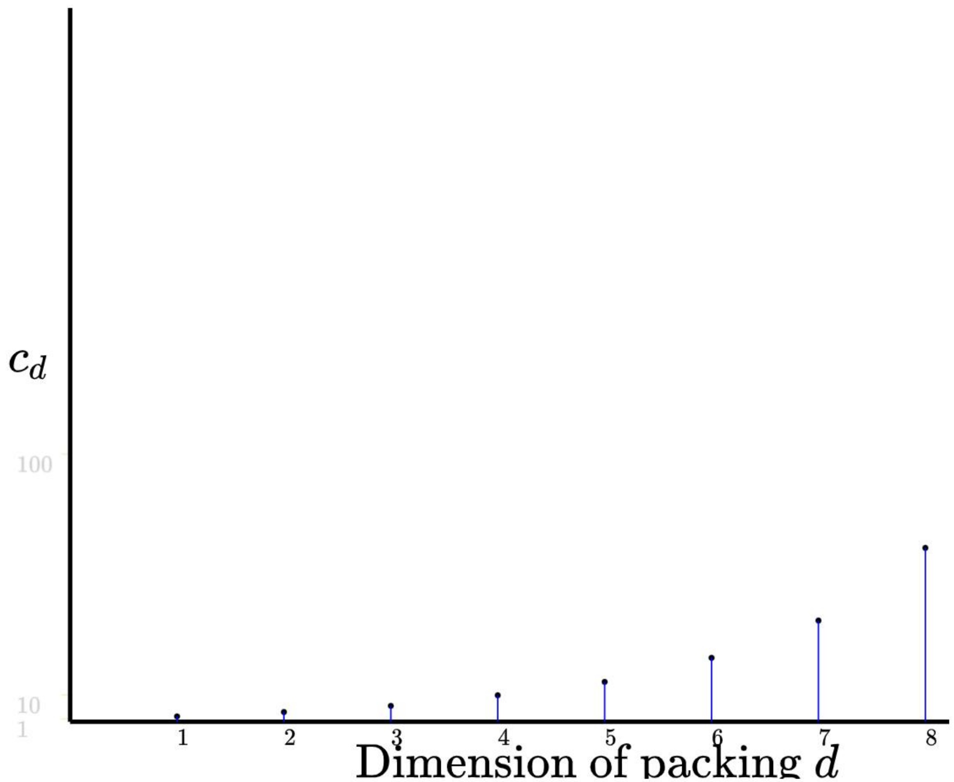
Comparison of bounds



What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

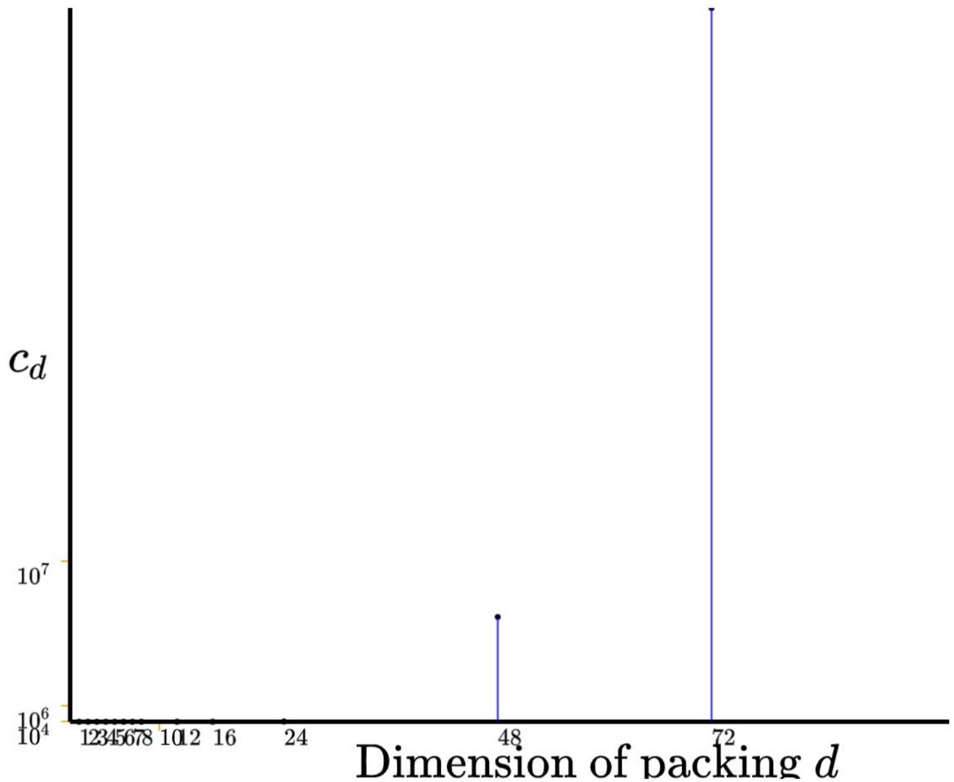
Comparison of bounds



What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

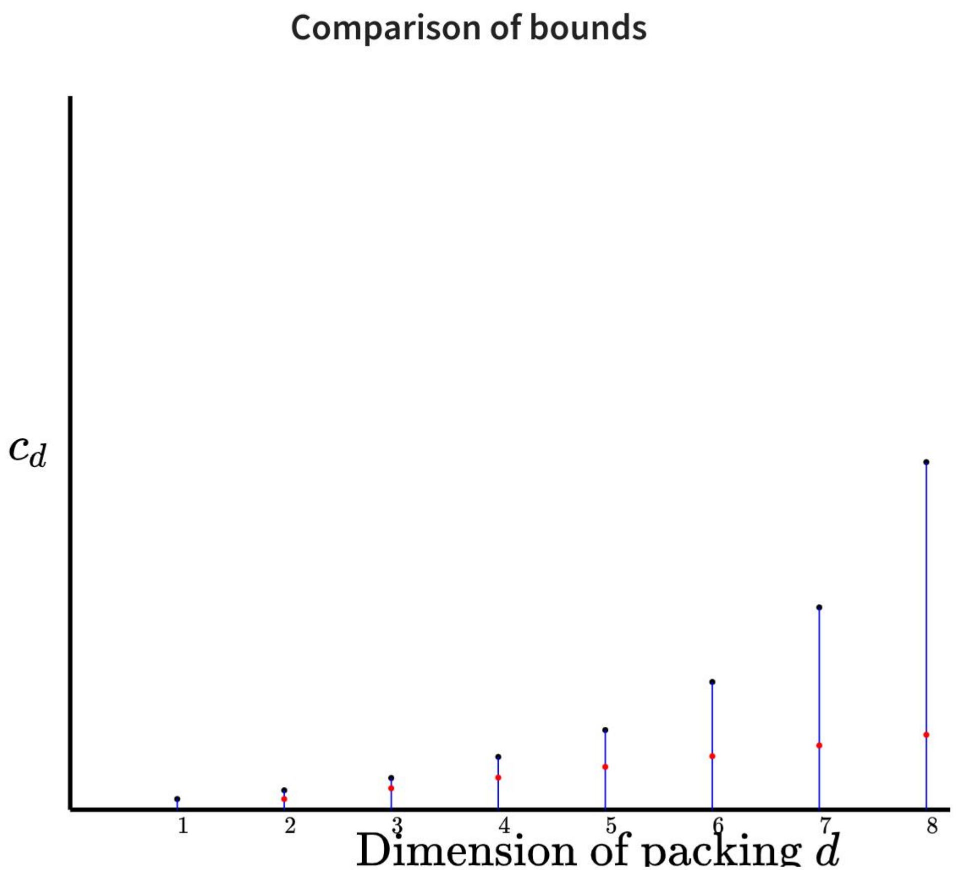
Comparison of bounds



What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

(Ball, 1992) , the lower bound is as indicated.



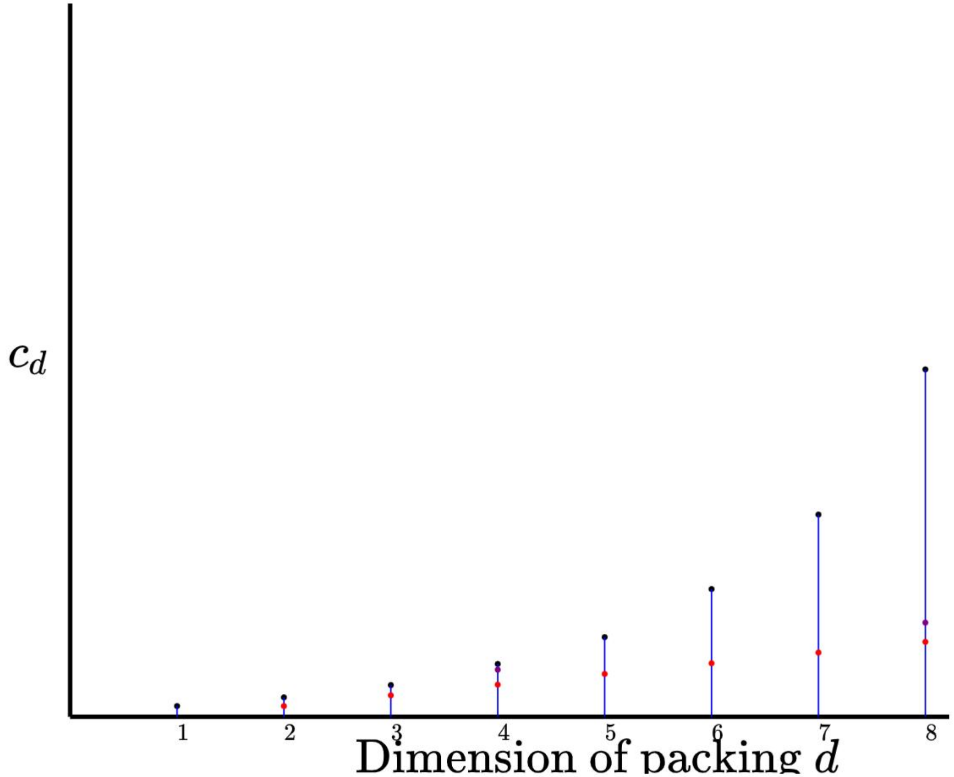
What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

(Ball, 1992) , the lower bound is as indicated.

(Vance, 2011) , using a probabilistic argument on lattices that lie in vector-space over quaternion division algebra. Works only when $4 \mid d$.

Comparison of bounds



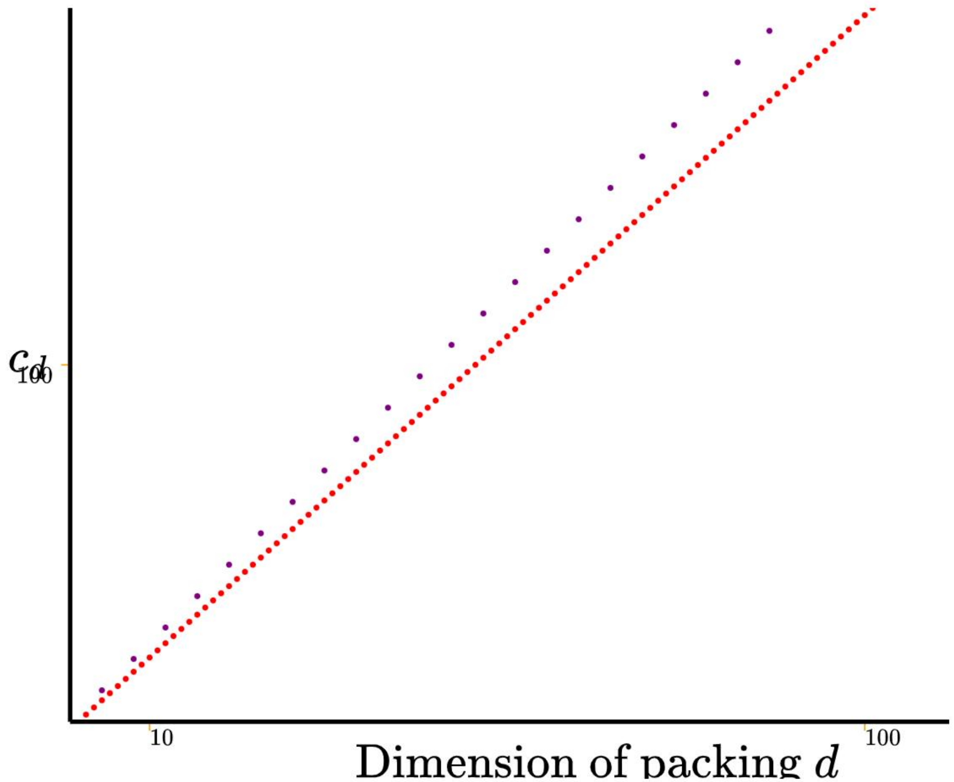
What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

(Ball, 1992) , the lower bound is as indicated.

(Vance, 2011) , using a probabilistic argument on lattices that lie in vector-space over quaternion division algebra. Works only when $4 \mid d$.

Comparison of bounds



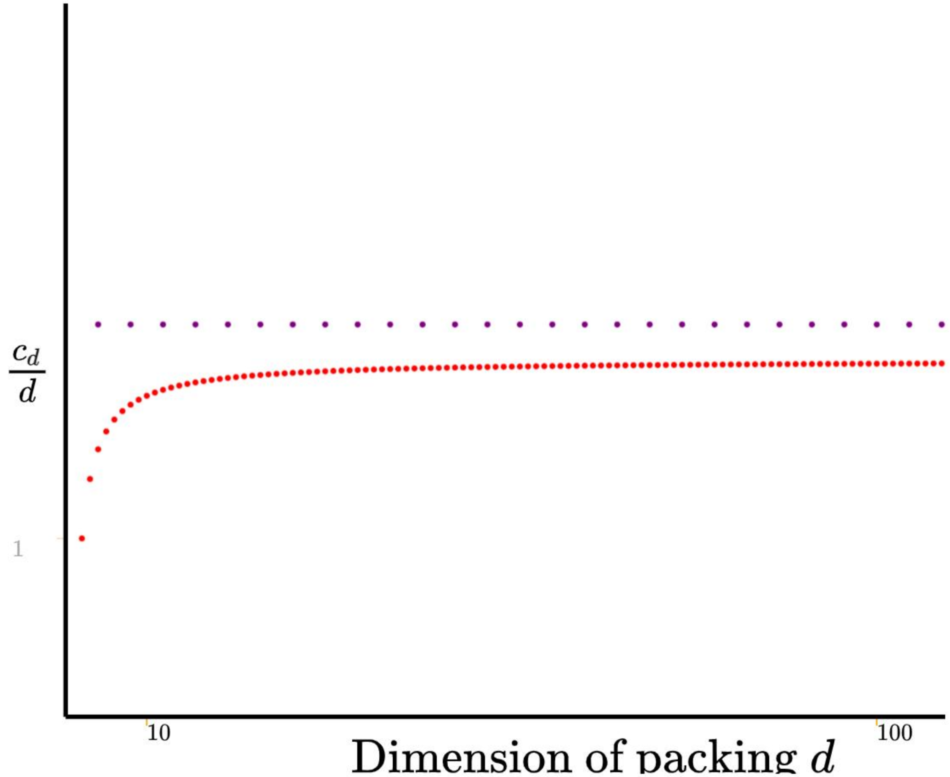
What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

(Ball, 1992) , the lower bound is as indicated.

(Vance, 2011) , using a probabilistic argument on lattices that lie in vector-space over quaternion division algebra. Works only when $4 \mid d$.

Comparison of bounds



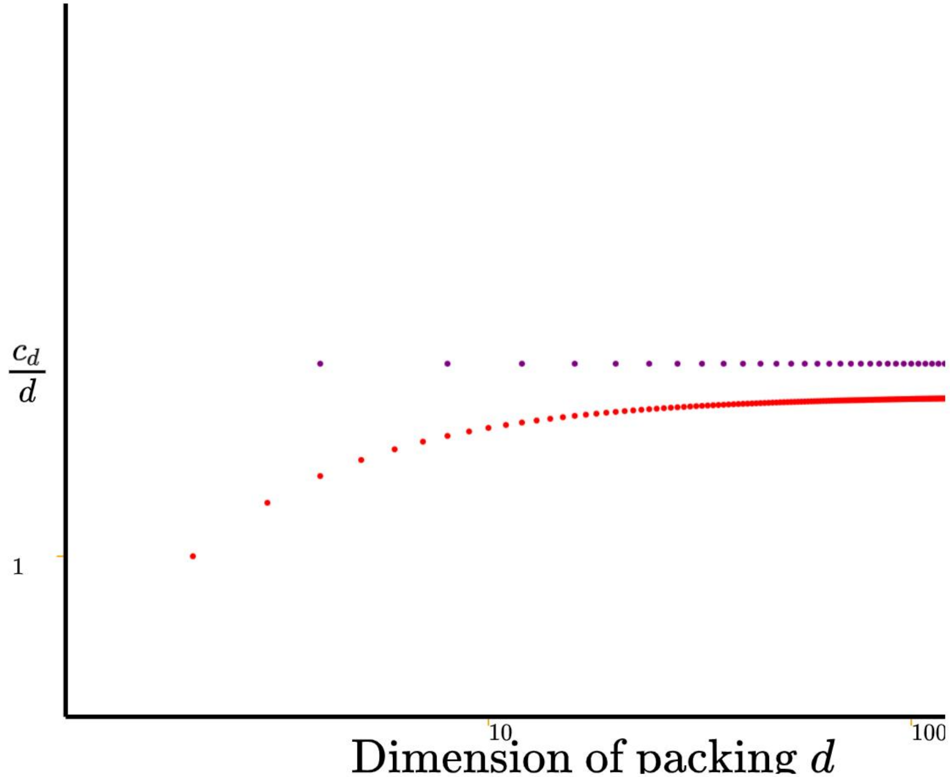
What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

(Ball, 1992) , the lower bound is as indicated.

(Vance, 2011) , using a probabilistic argument on lattices that lie in vector-space over quaternion division algebra. Works only when $4 \mid d$.

Comparison of bounds



What is known about c_d?

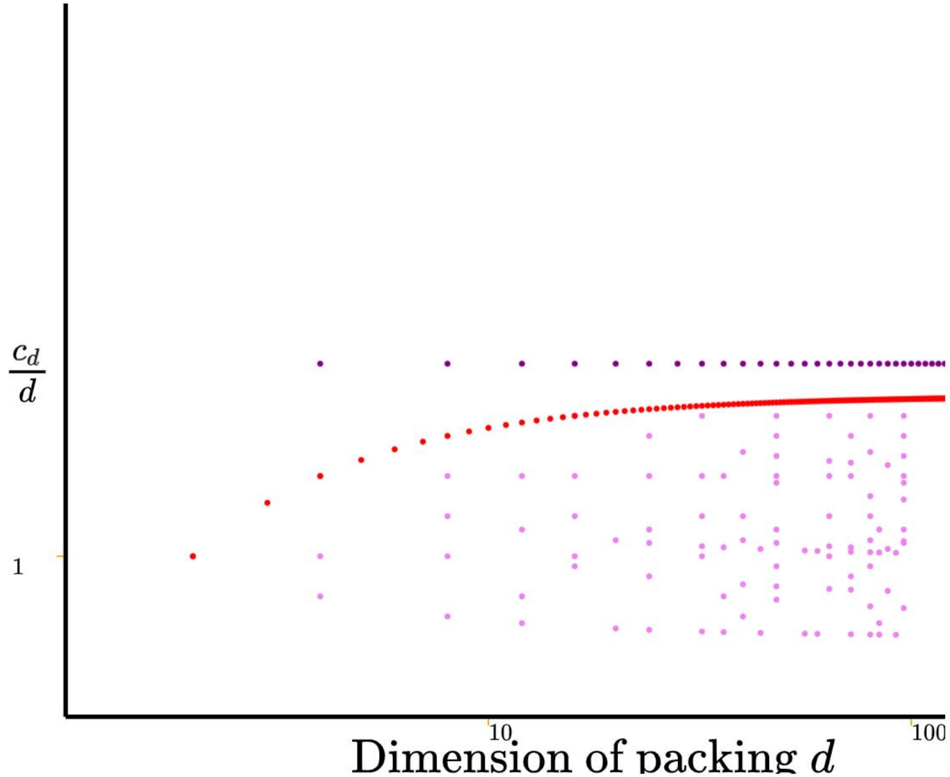
Explicit lattice constructions can help us only upto $d \leq 300$.

(Ball, 1992) , the lower bound is as indicated.

(Vance, 2011) , using a probabilistic argument on lattices that lie in vector-space over quaternion division algebra. Works only when $4 \mid d$.

(Venkatesh, 2013) , using a probabilistic argument on lattices that lie in $(K \otimes_{\mathbb{Q}} \mathbb{R})^2$, K is a cyclotomic field.

Comparison of bounds



What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

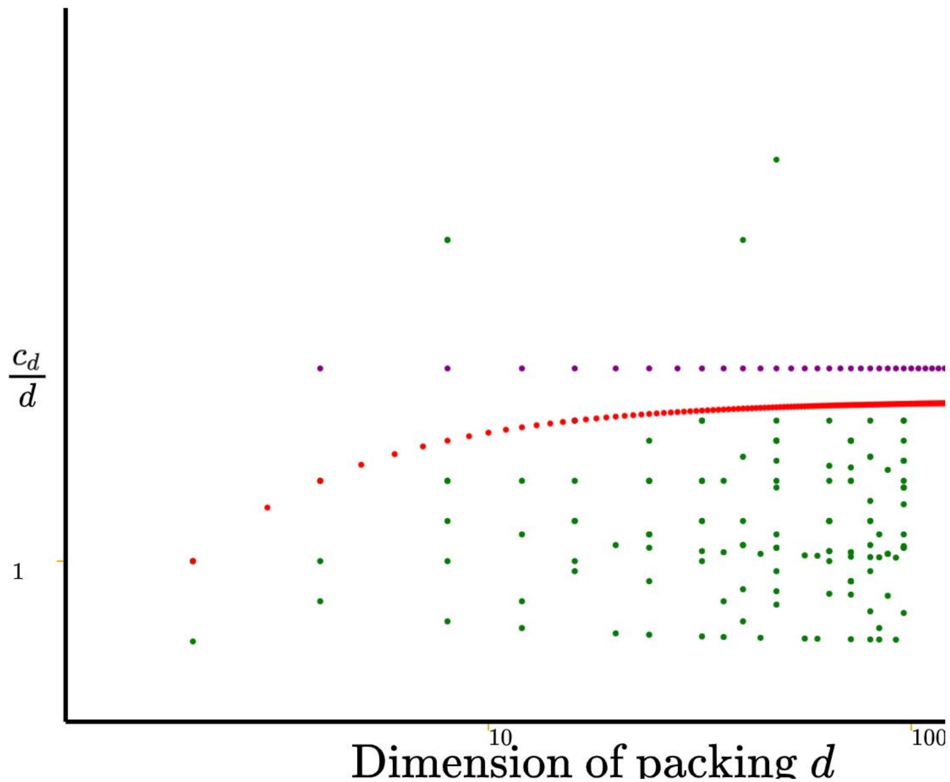
(Ball, 1992) , the lower bound is as indicated.

(Vance, 2011) , using a probabilistic argument on lattices that lie in vector-space over quaternion division algebra. Works only when $4 \mid d$.

(Venkatesh, 2013) , using a probabilistic argument on lattices that lie in $(K \otimes_{\mathbb{Q}} \mathbb{R})^2$, K is a cyclotomic field.

(G., 2021) , using a probabilistic argument on lattices that lie in $(D \otimes_{\mathbb{Q}} \mathbb{R})^2$, D is a division algebra over $\mathbb{Q}$.

Comparison of bounds



What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

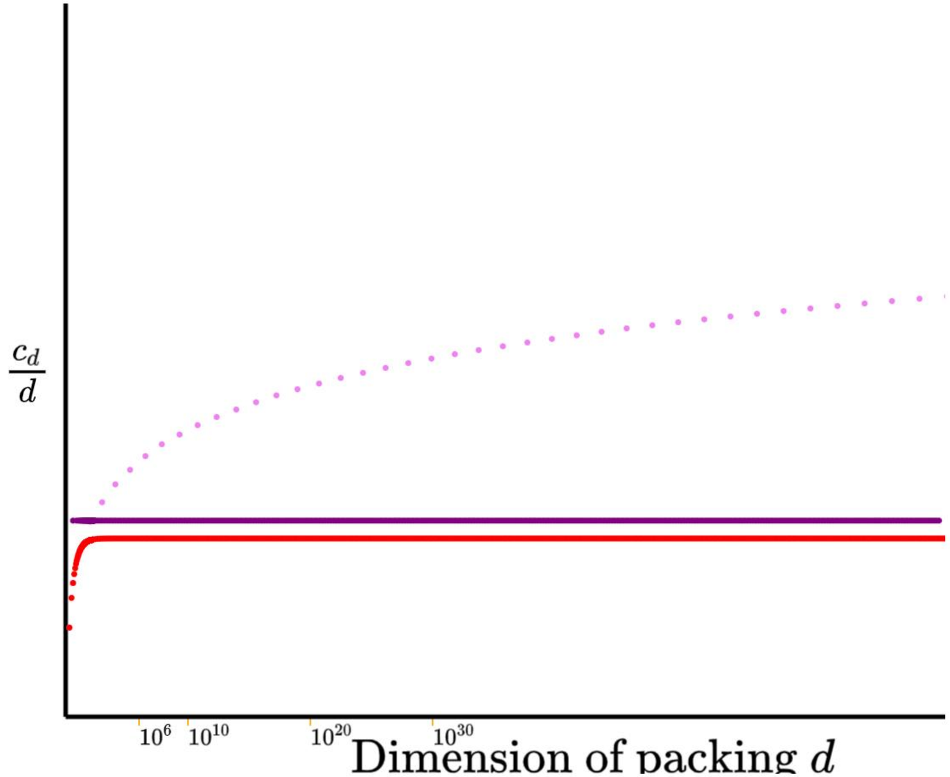
(Ball, 1992) , the lower bound is as indicated.

(Vance, 2011) , using a probabilistic argument on lattices that lie in vector-space over quaternion division algebra. Works only when $4 \mid d$.

(Venkatesh, 2013) , using a probabilistic argument on lattices that lie in $(K \otimes_{\mathbb{Q}} \mathbb{R})^2, K$ is a cyclotomic field.

(G., 2021) , using a probabilistic argument on lattices that lie in $(D \otimes_{\mathbb{Q}} \mathbb{R})^2, D$ is a division algebra over $\mathbb{Q}$.

Comparison of bounds



What is known about c_d?

Explicit lattice constructions can help us only upto $d \leq 300$.

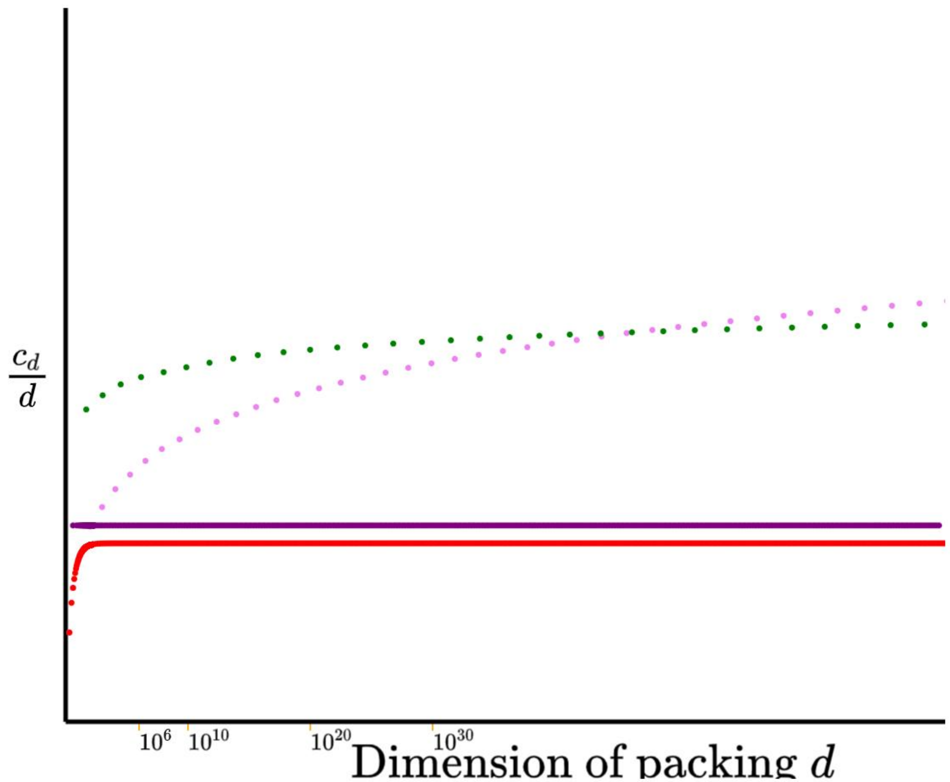
(Ball, 1992) , the lower bound is as indicated.

(Vance, 2011) , using a probabilistic argument on lattices that lie in vector-space over quaternion division algebra. Works only when $4 \mid d$.

(Venkatesh, 2013) , using a probabilistic argument on lattices that lie in $(K \otimes_{\mathbb{Q}} \mathbb{R})^2, K$ is a cyclotomic field.

(G., 2021) , using a probabilistic argument on lattices that lie in $(D \otimes_{\mathbb{Q}} \mathbb{R})^2, D$ is a division algebra over $\mathbb{Q}$.

Comparison of bounds



What is known about c_d?

What is known about c_d?

Theorem *(G. 2021)*

Let D be a finite-dimensional division algebra over $\mathbb{Q}$. Let $\mathcal{O} \subseteq D$ be an order in D and $G_0 \subseteq \mathcal{O}$ be a finite group embedded in the multiplicative group of D. Then if $d = 2\dim_{\mathbb{Q}} D$, then

$$c_d \geq \#G_0.$$

What is known about c_d?

Theorem *(G. 2021)*

Let D be a finite-dimensional division algebra over $\mathbb{Q}$. Let $\mathcal{O} \subseteq D$ be an order in D and $G_0 \subseteq \mathcal{O}$ be a finite group embedded in the multiplicative group of D. Then if $d = 2\dim_{\mathbb{Q}} D$, then

$$c_d \geq \#G_0.$$

To recover Venkatesh's result, set $D = \mathbb{Q}(\mu_n)$, $\mathcal{O} = \mathbb{Z}[\mu_n]$ and $G_0 = \langle \mu_n \rangle$. Hence, this gives

$$c_{2\varphi(n)} \geq n$$

What is known about c_d?

Theorem *(G. 2021)*

Let D be a finite-dimensional division algebra over $\mathbb{Q}$. Let $\mathcal{O} \subseteq D$ be an order in D and $G_0 \subseteq \mathcal{O}$ be a finite group embedded in the multiplicative group of D. Then if $d = 2\dim_{\mathbb{Q}} D$, then

$$c_d \geq \# G_0.$$

To recover Venkatesh's result, set $D = \mathbb{Q}(\mu_n)$, $\mathcal{O} = \mathbb{Z}[\mu_n]$ and $G_0 = \langle \mu_n \rangle$. Hence, this gives

$$c_{2\varphi(n)} \geq n$$

The cherrypicked sequence of Venkatesh achieves an asymptotic growth of $O(d \log\log d)$. This is achieved by setting K as the nth cyclotomic field where $n = \prod_{p<N} p$.

What is known about c_d?

Theorem *(G. 2021)*

Let D be a finite-dimensional division algebra over $\mathbb{Q}$. Let $\mathcal{O} \subseteq D$ be an order in D and $G_0 \subseteq \mathcal{O}$ be a finite group embedded in the multiplicative group of D. Then if $d = 2\dim_{\mathbb{Q}} D$, then

$$c_d \geq \#G_0.$$

To recover Venkatesh's result, set $D = \mathbb{Q}(\mu_n)$, $\mathcal{O} = \mathbb{Z}[\mu_n]$ and $G_0 = \langle \mu_n \rangle$. Hence, this gives

$$c_{2\varphi(n)} \geq n$$

The cherrypicked sequence of Venkatesh achieves an asymptotic growth of $O(d \log\log d)$. This is achieved by setting K as the nth cyclotomic field where $n = \prod_{p<N} p$.

The division algbera construction gives more freedom to cherrypick sequences. Instead of choosing a sequence of cyclotomic fields, we can now choose sequences of $\mathbb{Q}$-divison algebras. However, no such sequence will be able to give an asymptotic result strictly better than $O(d \log\log d)$. Improvements in individual dimensions is still possible, as shown before.

The probabilistic method

The probabilistic method

To show $c_d \geq K$, we must prove the existence of $g \in SL_d(\mathbb{R})$ such that the origin centered ball B with $\mu(B) = K$ has $g\mathbb{Z}^d \cap B = \{0\}$

The probabilistic method

To show $c_d \geq K$, we must prove the existence of $g \in SL_d(\mathbb{R})$ such that the origin centered ball B with $\mu(B) = K$ has $g\mathbb{Z}^d \cap B = \{0\}$

This is an optimization problem on the space

$$X_d := \{\Lambda \subset \mathbb{R}^d | \ \mu(\mathbb{R}^d/\Lambda) = 1\} = \{g\,\mathbb{Z}^d \ \mid g \in SL_d(\mathbb{R})\}$$

The probabilistic method

To show $c_d \geq K$, we must prove the existence of $g \in SL_d(\mathbb{R})$ such that the origin centered ball B with $\mu(B) = K$ has $g\mathbb{Z}^d \cap B = \{0\}$

This is an optimization problem on the space

$$X_d := \{\Lambda \subset \mathbb{R}^d | \ \mu(\mathbb{R}^d/\Lambda) = 1\} = \{g\,\mathbb{Z}^d \ | \ g \in SL_d(\mathbb{R})\}$$

$$\simeq SL_d(\mathbb{R})/SL_d(\mathbb{Z}).$$

The probabilistic method

To show $c_d \geq K$, we must prove the existence of $g \in SL_d(\mathbb{R})$ such that the origin centered ball B with $\mu(B) = K$ has $g\mathbb{Z}^d \cap B = \{0\}$

This is an optimization problem on the space

$$X_d := \{\Lambda \subset \mathbb{R}^d | \, \mu(\mathbb{R}^d/\Lambda) = 1\} = \{g\,\mathbb{Z}^d \mid g \in SL_d(\mathbb{R})\}$$
$$\simeq SL_d(\mathbb{R})/SL_d(\mathbb{Z}).$$

A priori, this is a bijection of sets. But now we can pull back the topology and the measure from $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$.

The probabilistic method

To show $c_d \geq K$, we must prove the existence of $g \in SL_d(\mathbb{R})$ such that the origin centered ball B with $\mu(B) = K$ has $g\mathbb{Z}^d \cap B = \{0\}$

This is an optimization problem on the space

$$X_d := \{\Lambda \subset \mathbb{R}^d | \mu(\mathbb{R}^d/\Lambda) = 1\} = \{g\mathbb{Z}^d \mid g \in SL_d(\mathbb{R})\}$$
$$\simeq SL_d(\mathbb{R})/SL_d(\mathbb{Z}).$$

A priori, this is a bijection of sets. But now we can pull back the topology and the measure from $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$.

$SL_d(\mathbb{R})$ has the topology of a locally compact group.

The probabilistic method

To show $c_d \geq K$, we must prove the existence of $g \in SL_d(\mathbb{R})$ such that the origin centered ball B with $\mu(B) = K$ has $g\mathbb{Z}^d \cap B = \{0\}$

This is an optimization problem on the space

$$X_d := \{\Lambda \subset \mathbb{R}^d \mid \mu(\mathbb{R}^d/\Lambda) = 1\} = \{g\mathbb{Z}^d \mid g \in SL_d(\mathbb{R})\}$$
$$\simeq SL_d(\mathbb{R})/SL_d(\mathbb{Z}).$$

A priori, this is a bijection of sets. But now we can pull back the topology and the measure from $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$.

$SL_d(\mathbb{R})$ has the topology of a locally compact group.

$SL_d(\mathbb{R})$ is unimodular. $SL_d(\mathbb{Z})$ is a discrete subgroup inside $SL_d(\mathbb{R})$ and therefore there is a unique left $SL_d(\mathbb{R})$-invariant measure on $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$.

The probabilistic method

The probabilistic method

Proposition

There exists a unique (upto scaling) natural measure on $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$, left-invariant under $SL_d(\mathbb{R})$ action on cosets.
Furthermore, $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$ under this has a **bounded** total measure.

The probabilistic method

Proposition

There exists a unique (upto scaling) natural measure on $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$, left-invariant under $SL_d(\mathbb{R})$ action on cosets.
Furthermore, $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$ under this has a **bounded** total measure.

This gives us a probability space. Hence we can talk about random unit covolume lattices.

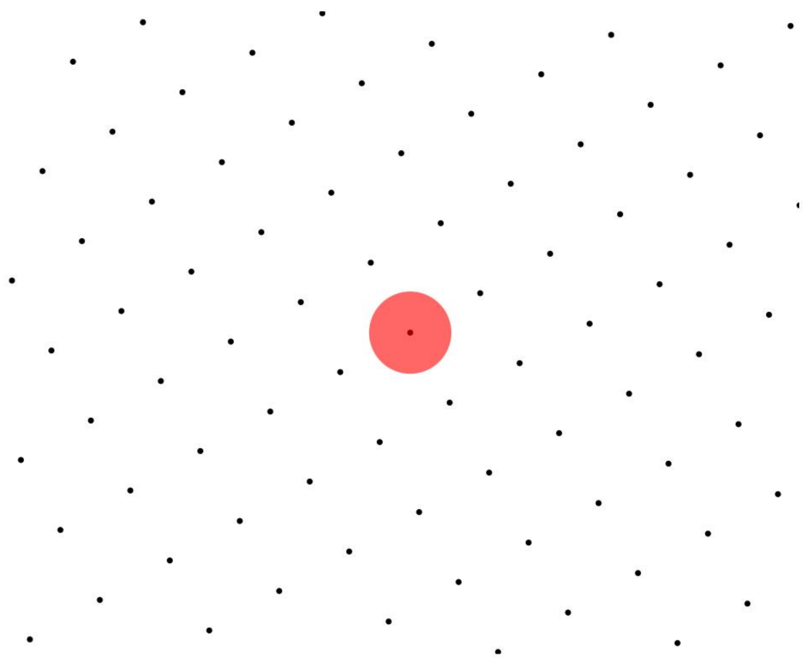
Lattice-sum function

Visualizing in $\mathbb{R}^2$

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

Visualizing in $\mathbb{R}^2$

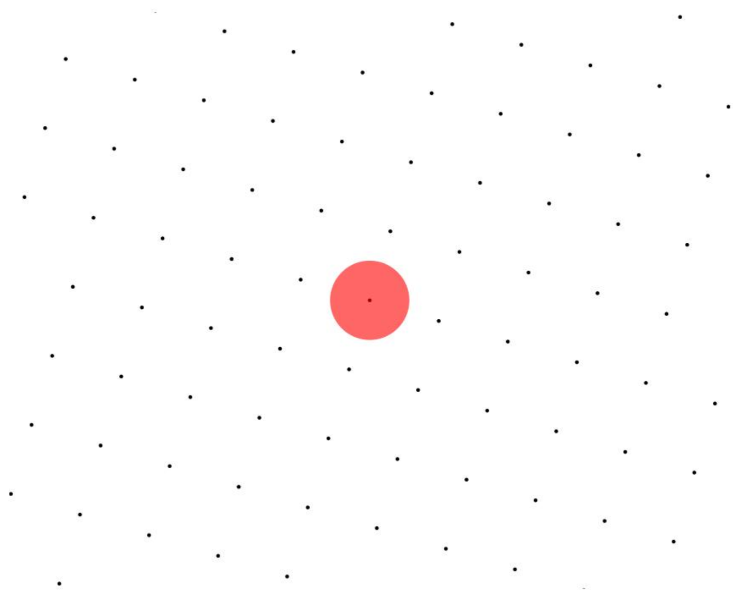


$\int_{\mathbb{R}^2} f(x)dx$ 0.950

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

Visualizing in $\mathbb{R}^2$



$\int_{\mathbb{R}^2} f(x)dx =$ 0.950

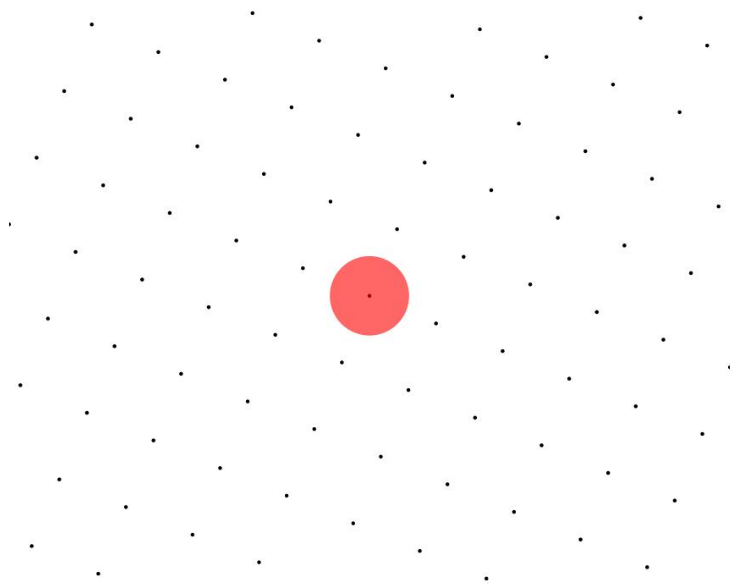
Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Visualizing in $\mathbb{R}^2$



$\int_{\mathbb{R}^2} f(x)dx =$ 0.950

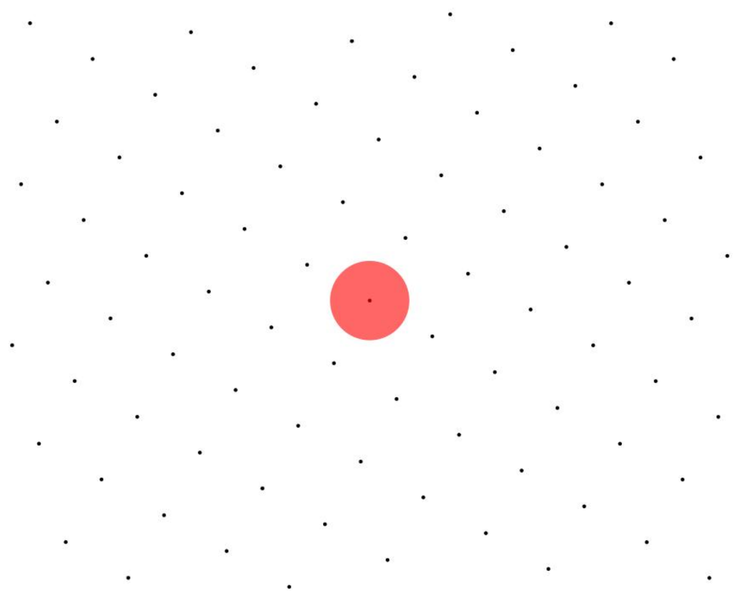
Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 0

$\int_{\mathbb{R}^2} f(x)dx =$ 0.950

Lattice-sum function

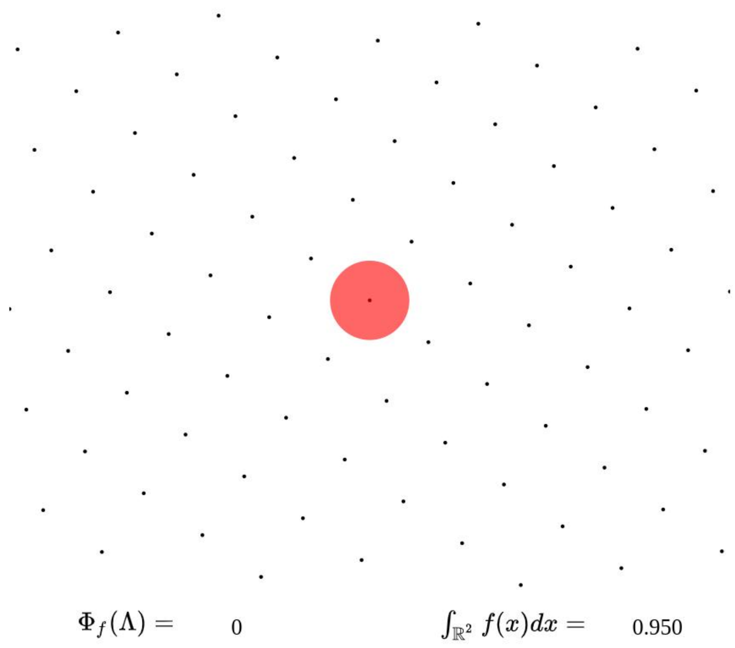
Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Visualizing in $\mathbb{R}^2$



Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

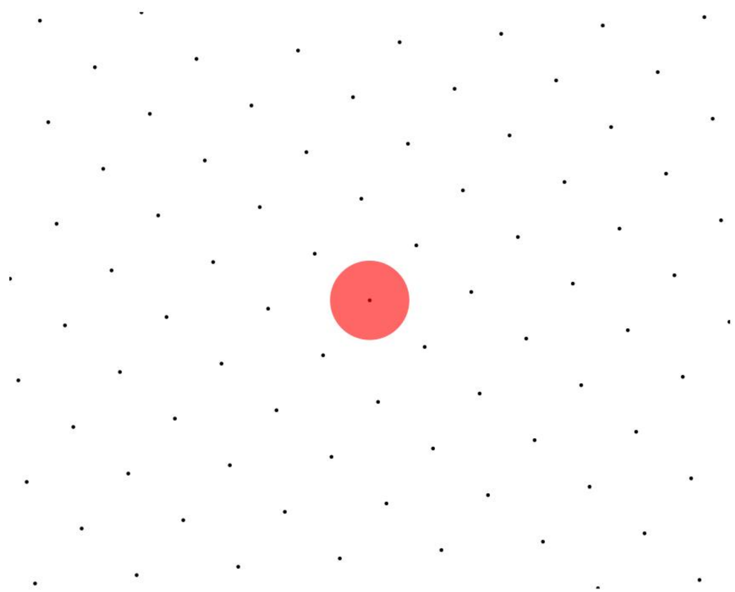
With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 0

$\int_{\mathbb{R}^2} f(x)dx =$ 0.950

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

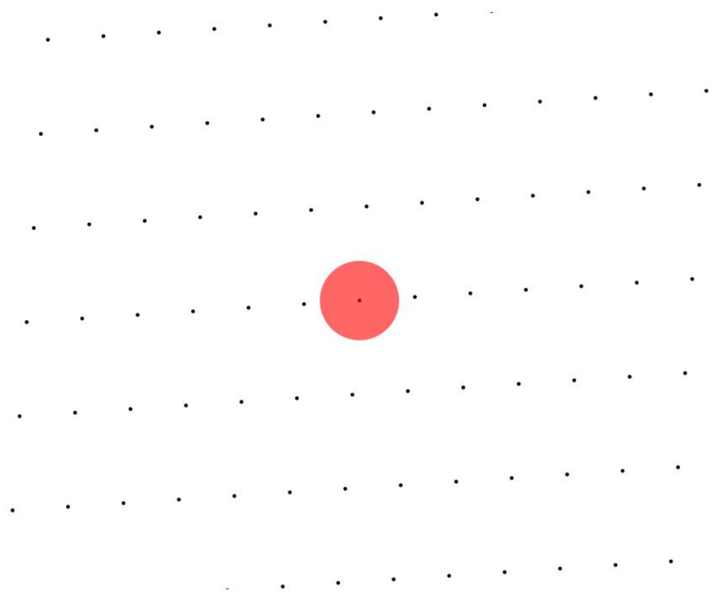
With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 0

$\int_{\mathbb{R}^2} f(x)dx =$ 0.950

$\frac{\sum_{\Lambda \in S} \Phi_f(\Lambda)}{\#S} = \frac{0}{1}$

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

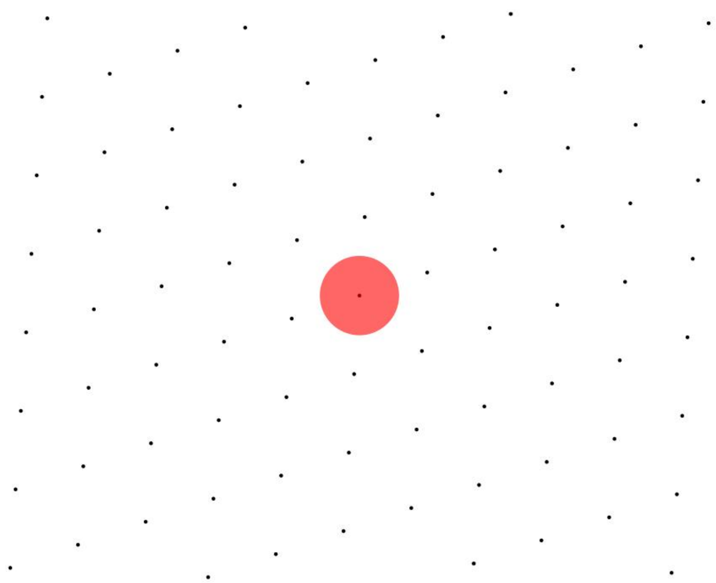
With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 0 $\qquad \int_{\mathbb{R}^2} f(x)dx =$ 0.950

$\frac{\sum_{\Lambda \in S} \Phi_f(\Lambda)}{\#S} = \frac{0}{2} =$ 0.00

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

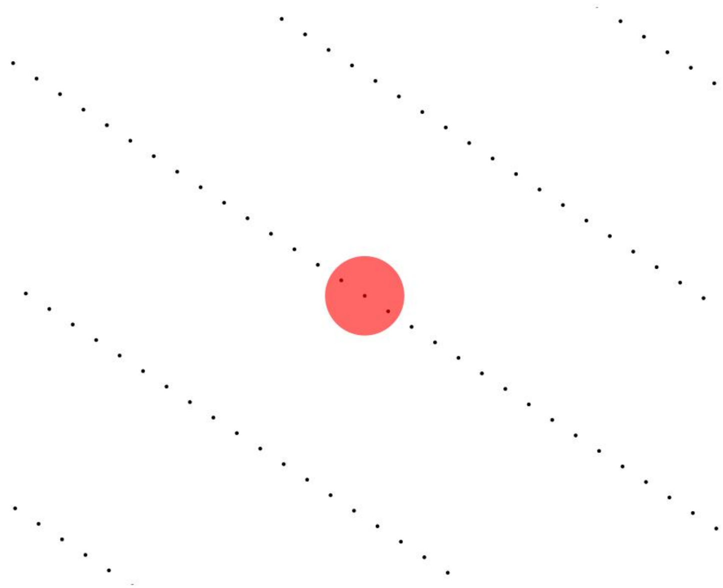
With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 2 $\quad$ $\int_{\mathbb{R}^2} f(x)dx =$ 0.950

$\frac{\sum_{\Lambda \in S} \Phi_f(\Lambda)}{\#S} = \frac{2}{3} =$ 0.667

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

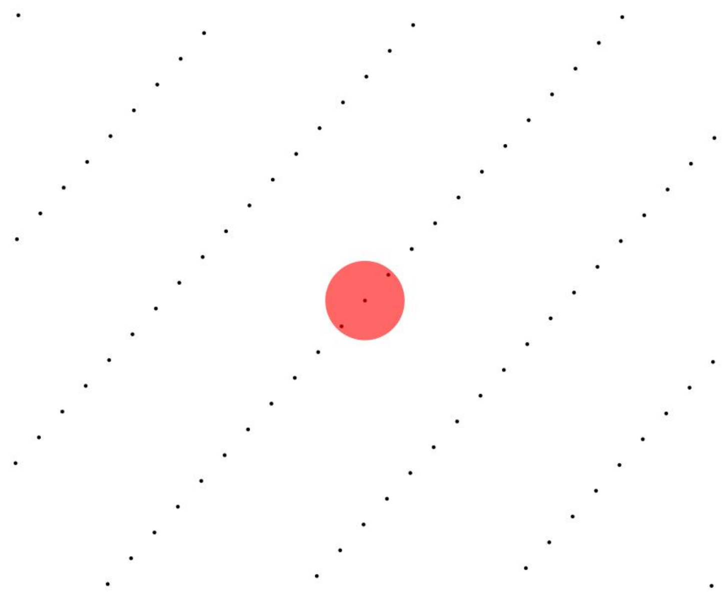
With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 2 $\int_{\mathbb{R}^2} f(x)dx =$ 0.950

$\frac{\sum_{\Lambda \in S} \Phi_f(\Lambda)}{\# S} = \frac{4}{4} =$ 1.00

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

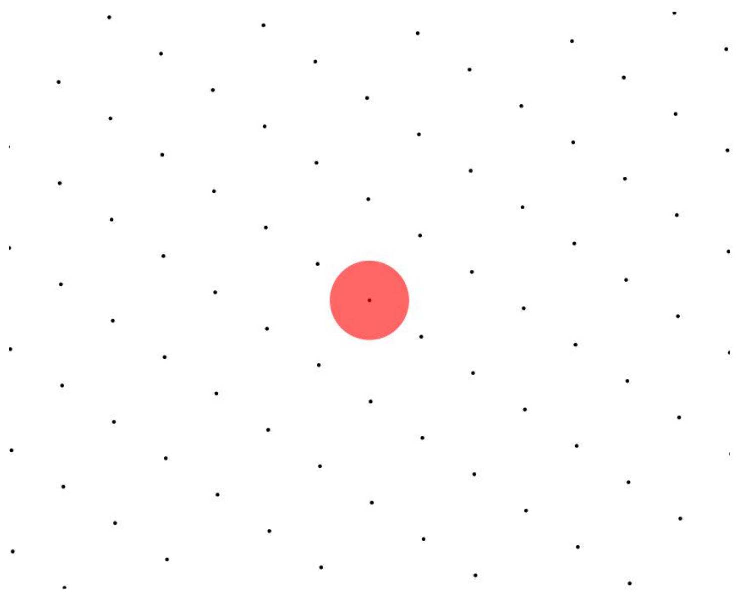
With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 0 $\int_{\mathbb{R}^2} f(x)dx =$ 0.950

$\frac{\sum_{\Lambda \in S} \Phi_f(\Lambda)}{\# S} = \frac{4}{5} =$ 0.800

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

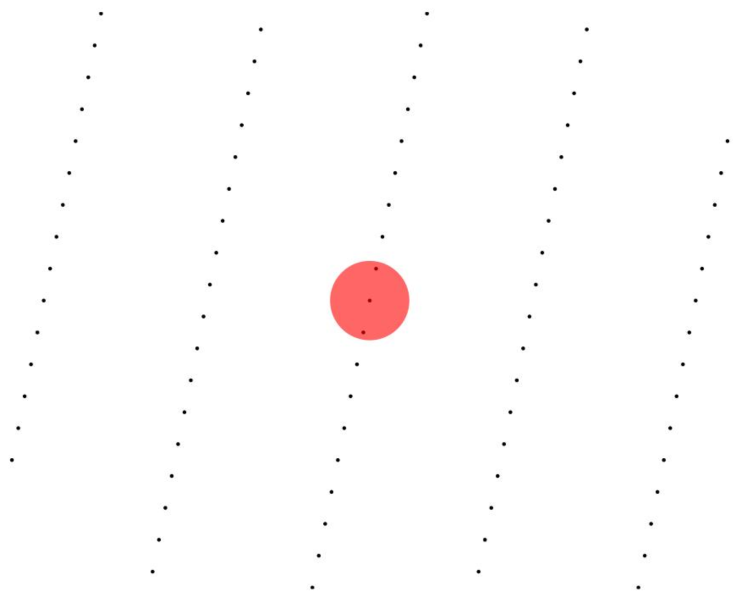
With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 2

$\int_{\mathbb{R}^2} f(x)dx =$ 0.950

$\frac{\sum_{\Lambda \in S} \Phi_f(\Lambda)}{\# S} = \frac{68}{100} =$ 0.680

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

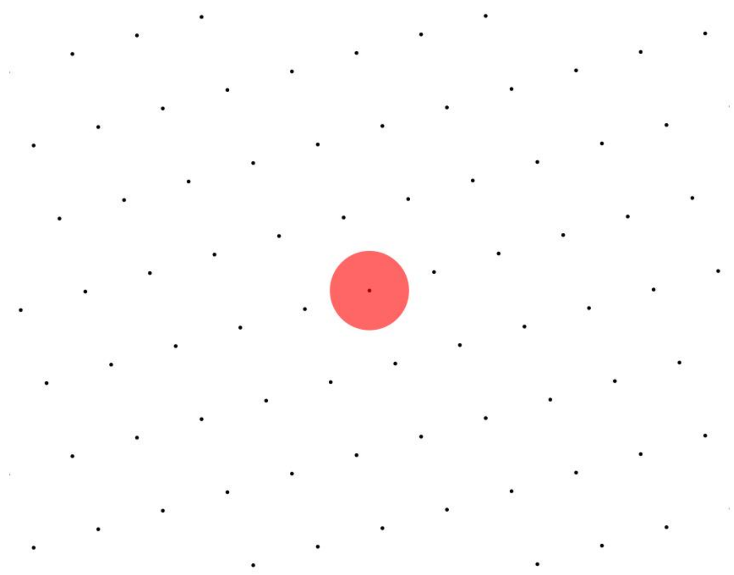
$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

So we see that it is almost the integral.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 0 $\qquad \int_{\mathbb{R}^2} f(x)dx =$ 0.950

$\frac{\sum_{\Lambda \in S} \Phi_f(\Lambda)}{\#S} = \frac{242}{257} =$ 0.942

Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

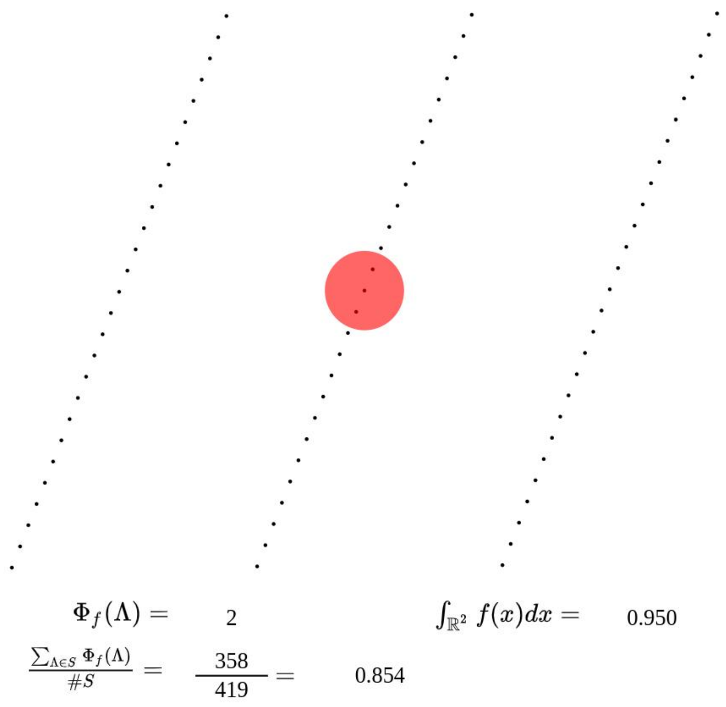
$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

So we see that it is almost the integral.

Visualizing in $\mathbb{R}^2$



Lattice-sum function

Consider a bounded measurable function with compact support $f : \mathbb{R}^d \to \mathbb{R}$.
e.g. the indicator function of a ball.

With this, we can now construct the lattice-sum function $\Phi_f(\Lambda) : X_d \to \mathbb{R}$, given as

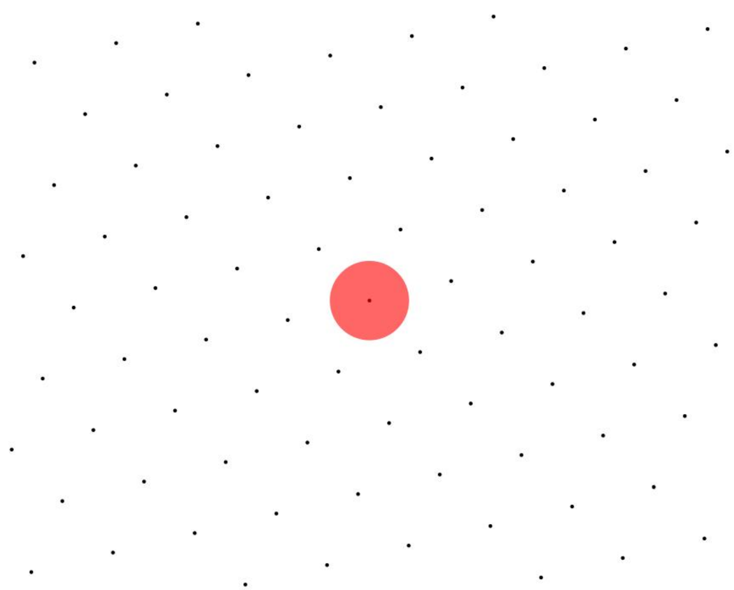
$$\Phi_f(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} f(v).$$

Since we can generate random lattices, we can talk about the expected value of $\Phi_f(\Lambda)$.

Let us try to do this experimentally! Let us sample over a set $S \subseteq X_d$ of lattices.

So we see that it is almost the integral.

Visualizing in $\mathbb{R}^2$



$\Phi_f(\Lambda) =$ 0

$\int_{\mathbb{R}^2} f(x)dx =$ 0.950

$\frac{\sum_{\Lambda \in S} \Phi_f(\Lambda)}{\#S} = \frac{462}{500} =$ 0.924

Lattice-sum function

What we are empirically confirming is the following.

Lattice-sum function

What we are empirically confirming is the following.

Theorem *(Siegel, 1945)*

Suppose $f : \mathbb{R}^d \to \mathbb{R}$ is a compactly supported bounded measurable function. Then, the following holds.

$$\int_{X_d} \Phi_f = \int_{SL_d(\mathbb{R})/SL_d(\mathbb{Z})} \left(\sum_{v \in g\mathbb{Z}^d \setminus \{0\}} f(v) \right) dg = \int_{\mathbb{R}^d} f(x) dx,$$

where the dx on the right-hand side is the usual Lebesgue measure on $\mathbb{R}^d$ and dg is the unique $SL_d(\mathbb{R})$-invariant probability measure on $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$.

Lattice-sum function

But as you saw that for any $\Lambda \in X_d$, when f is the indicator of a ball, we must have $\Phi_f(\Lambda) \in \{0, 2, 4, 6, \dots\}$. That's because balls are symmetric.

$$v \in \operatorname{supp}(f) \cap (\Lambda \setminus \{0\}) \Rightarrow -v \in \operatorname{supp}(f) \cap (\Lambda \setminus \{0\}).$$

Lattice-sum function

But as you saw that for any $\Lambda \in X_d$, when f is the indicator of a ball, we must have $\Phi_f(\Lambda) \in \{0, 2, 4, 6, \dots\}$. That's because balls are symmetric.

$$v \in \mathrm{supp}(f) \cap (\Lambda \setminus \{0\}) \Rightarrow -v \in \mathrm{supp}(f) \cap (\Lambda \setminus \{0\}).$$

If f is the indicator function of a ball of volume $2 - \varepsilon$, then this tells us that for any dimension d

$$\int_{X_d} \Phi_f = 2 - \varepsilon$$

Lattice-sum function

But as you saw that for any $\Lambda \in X_d$, when f is the indicator of a ball, we must have $\Phi_f(\Lambda) \in \{0, 2, 4, 6, \ldots\}$. That's because balls are symmetric.

$$v \in \text{supp}(f) \cap (\Lambda \setminus \{0\}) \Rightarrow -v \in \text{supp}(f) \cap (\Lambda \setminus \{0\}).$$

If f is the indicator function of a ball of volume $2 - \varepsilon$, then this tells us that for any dimension d

$$\int_{X_d} \Phi_f = 2 - \varepsilon$$

Conclusion: There exists some lattice $\Lambda \in X_d$ such that $\Phi_f(\Lambda) = 0$. That is, there is some lattice of unit covolume that intersects trivially with an origin centered ball of volume $2 - \varepsilon$.

Lattice-sum function

But as you saw that for any $\Lambda \in X_d$, when f is the indicator of a ball, we must have $\Phi_f(\Lambda) \in \{0, 2, 4, 6, \dots\}$. That's because balls are symmetric.

$$v \in \operatorname{supp}(f) \cap (\Lambda \setminus \{0\}) \Rightarrow -v \in \operatorname{supp}(f) \cap (\Lambda \setminus \{0\}).$$

If f is the indicator function of a ball of volume $2 - \varepsilon$, then this tells us that for any dimension d

$$\int_{X_d} \Phi_f = 2 - \varepsilon$$

Conclusion: There exists some lattice $\Lambda \in X_d$ such that $\Phi_f(\Lambda) = 0$. That is, there is some lattice of unit covolume that intersects trivially with an origin centered ball of volume $2 - \varepsilon$.

Another conclusion: $c_d \geq 2$ for all dimensions d!

Lattice-sum function

But as you saw that for any $\Lambda \in X_d$, when f is the indicator of a ball, we must have $\Phi_f(\Lambda) \in \{0, 2, 4, 6, \ldots\}$. That's because balls are symmetric.

$$v \in \operatorname{supp}(f) \cap (\Lambda \setminus \{0\}) \Rightarrow -v \in \operatorname{supp}(f) \cap (\Lambda \setminus \{0\}).$$

If f is the indicator function of a ball of volume $2 - \varepsilon$, then this tells us that for any dimension d

$$\int_{X_d} \Phi_f = 2 - \varepsilon$$

Conclusion: There exists some lattice $\Lambda \in X_d$ such that $\Phi_f(\Lambda) = 0$. That is, there is some lattice of unit covolume that intersects trivially with an origin centered ball of volume $2 - \varepsilon$.

Another conclusion: $c_d \geq 2$ for all dimensions d!

Both Venkatesh and the division algebra lattices use this idea. What we want is to find expectation of the lattice sum over a smaller subset of lattices that have a larger group of symmetries.

Lattice-sum function

But as you saw that for any $\Lambda \in X_d$, when f is the indicator of a ball, we must have $\Phi_f(\Lambda) \in \{0, 2, 4, 6, \dots\}$. That's because balls are symmetric.

$$v \in \operatorname{supp}(f) \cap (\Lambda \setminus \{0\}) \Rightarrow -v \in \operatorname{supp}(f) \cap (\Lambda \setminus \{0\}).$$

If f is the indicator function of a ball of volume $2 - \varepsilon$, then this tells us that for any dimension d

$$\int_{X_d} \Phi_f = 2 - \varepsilon$$

Conclusion: There exists some lattice $\Lambda \in X_d$ such that $\Phi_f(\Lambda) = 0$. That is, there is some lattice of unit covolume that intersects trivially with an origin centered ball of volume $2 - \varepsilon$.

Another conclusion: $c_d \geq 2$ for all dimensions d!

Both Venkatesh and the division algebra lattices use this idea. What we want is to find expectation of the lattice sum over a smaller subset of lattices that have a larger group of symmetries.

For Venkatesh, the group of symmetries is always a cyclic group. For the new result, the symmetries are non-commutative.

Venkatesh's lower bound

Venkatesh's lower bound

The idea is to take a **nice** enough subcollection $Y_d \subseteq X_d$ of lattices and average the lattice-sum function Φ_f over them.

Venkatesh's lower bound

The idea is to take a **nice** enough subcollection $Y_d \subseteq X_d$ of lattices and average the lattice-sum function Φ_f over them.

Define the set Y_d as

$$Y_d = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mathcal{O}_K^2 \mid a, b, c, d \in K_{\mathbb{R}} = K \otimes \mathbb{R}, ad - bc = 1_{K_{\mathbb{R}}} \right\}.$$

Venkatesh's lower bound

The idea is to take a **nice** enough subcollection $Y_d \subseteq X_d$ of lattices and average the lattice-sum function Φ_f over them.

Define the set Y_d as

$$Y_d = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mathcal{O}_K^2 \mid a, b, c, d \in K_{\mathbb{R}} = K \otimes \mathbb{R}, ad - bc = 1_{K_{\mathbb{R}}} \right\}.$$

In conventional notation, this is just

$$Y_d = \{g(\mathcal{O}_K^{\oplus 2}) \mid g \in SL_2(K_{\mathbb{R}})\} \simeq SL_2(K_{\mathbb{R}})/SL_2(\mathcal{O}_K).$$

Venkatesh's lower bound

The idea is to take a **nice** enough subcollection $Y_d \subseteq X_d$ of lattices and average the lattice-sum function Φ_f over them.

Define the set Y_d as

$$Y_d = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mathcal{O}_K^2 \mid a, b, c, d \in K_{\mathbb{R}} = K \otimes \mathbb{R}, ad - bc = 1_{K_{\mathbb{R}}} \right\}.$$

In conventional notation, this is just

$$Y_d = \{g(\mathcal{O}_K^{\oplus 2}) \mid g \in SL_2(K_{\mathbb{R}})\} \simeq SL_2(K_{\mathbb{R}})/SL_2(\mathcal{O}_K).$$

Y_d can be given probability measure.

Venkatesh's lower bound

The idea is to take a **nice** enough subcollection $Y_d \subseteq X_d$ of lattices and average the lattice-sum function Φ_f over them.

Define the set Y_d as

$$Y_d = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mathcal{O}_K^2 \mid a, b, c, d \in K_{\mathbb{R}} = K \otimes \mathbb{R}, ad - bc = 1_{K_{\mathbb{R}}} \right\}.$$

In conventional notation, this is just

$$Y_d = \{g(\mathcal{O}_K^{\oplus 2}) \mid g \in SL_2(K_{\mathbb{R}})\} \simeq SL_2(K_{\mathbb{R}})/SL_2(\mathcal{O}_K).$$

Y_d can be given probability measure.

So if f is the indicator function of an origin-centered ball with respect to a quadratic form that is invariant under $\langle \mu_n \rangle$, we have that $\Phi_f(\Lambda) \in \{0, n, 2n, 3n, 4n, \ldots\}$ for $\Lambda \in Y_d$. Such a quadratic form always exists by averaging!

Venkatesh's lower bound

Venkatesh, then proves the following analogue of Siegel's theorem.

Venkatesh's lower bound

Venkatesh, then proves the following analogue of Siegel's theorem.

Theorem *(Venkatesh 2013)*

Let $d = 2\varphi(n)$ Suppose $f : K_{\mathbb{R}}^2 \to \mathbb{R}$ is a compactly supported bounded measurable function. Then, the following holds.

$$\int_{Y_d} \Phi_f = \int_{SL_2(K_{\mathbb{R}})/SL_2(\mathcal{O}_K)} \left(\sum_{v \in g\mathcal{O}_K^{\oplus 2} \setminus \{0\}} f(v) \right) dg = \int_{\mathbb{R}^d} f(x)dx,$$

where the dx on the right-hand side is that lebesgue measure on $\mathbb{R}^d$ that makes $\mathcal{O}_K^{\oplus 2}$ of unit covolume and dg is the unique $SL_2(K_{\mathbb{R}})$-invariant probability measure on Y_d.

Venkatesh's lower bound

Venkatesh, then proves the following analogue of Siegel's theorem.

Theorem *(Venkatesh 2013)*

Let $d = 2\varphi(n)$ Suppose $f : K_{\mathbb{R}}^2 \to \mathbb{R}$ is a compactly supported bounded measurable function. Then, the following holds.

$$\int_{Y_d} \Phi_f = \int_{SL_2(K_{\mathbb{R}})/SL_2(\mathcal{O}_K)} \left(\sum_{v \in g\mathcal{O}_K^{\oplus 2} \setminus \{0\}} f(v) \right) dg = \int_{\mathbb{R}^d} f(x) dx,$$

where the dx on the right-hand side is that lebesgue measure on $\mathbb{R}^d$ that makes $\mathcal{O}_K^{\oplus 2}$ of unit covolume and dg is the unique $SL_2(K_{\mathbb{R}})$-invariant probability measure on Y_d.

Conclusion: By setting f as the indicator function of a ball in a suitable quadratic form, we conclude that there exists some lattice $\Lambda \in Y_d$ such that $\Phi_f(\Lambda) = 0$. That is, there is some lattice of unit covolume that intersects trivially with an origin centered ball of volume $n - \varepsilon$.

Venkatesh's lower bound

Venkatesh, then proves the following analogue of Siegel's theorem.

Theorem *(Venkatesh 2013)*

Let $d = 2\varphi(n)$ Suppose $f : K_{\mathbb{R}}^2 \to \mathbb{R}$ is a compactly supported bounded measurable function. Then, the following holds.

$$\int_{Y_d} \Phi_f = \int_{SL_2(K_{\mathbb{R}})/SL_2(\mathcal{O}_K)} \left(\sum_{v \in g\mathcal{O}_K^{\oplus 2} \setminus \{0\}} f(v) \right) dg = \int_{\mathbb{R}^d} f(x)dx,$$

where the dx on the right-hand side is that lebesgue measure on $\mathbb{R}^d$ that makes $\mathcal{O}_K^{\oplus 2}$ of unit covolume and dg is the unique $SL_2(K_{\mathbb{R}})$-invariant probability measure on Y_d.

Conclusion: By setting f as the indicator function of a ball in a suitable quadratic form, we conclude that there exists some lattice $\Lambda \in Y_d$ such that $\Phi_f(\Lambda) = 0$. That is, there is some lattice of unit covolume that intersects trivially with an origin centered ball of volume $n - \varepsilon$.

Another conclusion: $c_{2\varphi(n)} \geq n$ for all n!

Towards division algebra

The division algebra case is also very similar. Let D be a finite-dimensional division algebra over $\mathbb{Q}$. Let $\mathcal{O} \subseteq D$ be an order in D. We work in $d = 2\dim_{\mathbb{Q}} D$ dimensions. Define $D_{\mathbb{R}} = D \otimes_{\mathbb{Q}} \mathbb{R}$.

$$Y_d = \{g(\mathcal{O}^{\oplus 2}) \mid g \in SL_2(D_{\mathbb{R}})\} \simeq SL_2(D_{\mathbb{R}})/SL_2(\mathcal{O}).$$

Here

$$SL_2(D_{\mathbb{R}}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix} \text{ is a measure preserving map on } D_{\mathbb{R}}^{\oplus 2} \right\}$$

Towards division algebra

The division algebra case is also very similar. Let D be a finite-dimensional division algebra over $\mathbb{Q}$. Let $\mathcal{O} \subseteq D$ be an order in D. We work in $d = 2\dim_{\mathbb{Q}} D$ dimensions. Define $D_{\mathbb{R}} = D \otimes_{\mathbb{Q}} \mathbb{R}$.

$$Y_d = \{g(\mathcal{O}^{\oplus 2}) \mid g \in SL_2(D_{\mathbb{R}})\} \simeq SL_2(D_{\mathbb{R}})/SL_2(\mathcal{O}).$$

Here

$$SL_2(D_{\mathbb{R}}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix} \text{ is a measure preserving map on } D_{\mathbb{R}}^{\oplus 2} \right\}$$

Y_d consists of lattices that are invariant under diagonal right-multiplication by units in $\mathcal{O}$

$$g(\mathcal{O}^{\oplus 2}) = g(\mathcal{O}^{\oplus 2}) \begin{bmatrix} \mu & 0 \\ 0 & \mu \end{bmatrix}, \text{ for any } \mu \in \mathcal{O}^*$$

Towards division algebra

Theorem *(G. 2021)*

Let $d = 2[D : \mathbb{Q}]$. Suppose $f : D_{\mathbb{R}}^2 \to \mathbb{R}$ is a compactly supported bounded measurable function. Then, the following holds.

$$\int_{Y_d} \Phi_f = \int_{SL_2(D_{\mathbb{R}})/SL_2(\mathcal{O})} \left(\sum_{v \in g\mathcal{O}^{\oplus 2} \setminus \{0\}} f(v) \right) dg = \int_{\mathbb{R}^d} f(x) dx,$$

where the dx on the right-hand side is that Lebesgue measure on $\mathbb{R}^d$ that makes $\mathcal{O}^{\oplus 2}$ of unit covolume and dg is the unique $SL_2(D_{\mathbb{R}})$-invariant probability measure on Y_d.

Towards division algebra

Theorem *(G. 2021)*

Let $d = 2[D : \mathbb{Q}]$. Suppose $f : D_{\mathbb{R}}^2 \to \mathbb{R}$ is a compactly supported bounded measurable function. Then, the following holds.

$$\int_{Y_d} \Phi_f = \int_{SL_2(D_{\mathbb{R}})/SL_2(\mathcal{O})} \left(\sum_{v \in g\mathcal{O}^{\oplus 2} \setminus \{0\}} f(v) \right) dg = \int_{\mathbb{R}^d} f(x) dx,$$

where the dx on the right-hand side is that Lebesgue measure on $\mathbb{R}^d$ that makes $\mathcal{O}^{\oplus 2}$ of unit covolume and dg is the unique $SL_2(D_{\mathbb{R}})$-invariant probability measure on Y_d.

To get packing bounds, fix a finite subgroup $G_0 \subseteq \mathcal{O}^*$ to act diagonally on the right of $\mathcal{O}^{\oplus 2}$. We get the bounds

$$c_{2 \dim_{\mathbb{Q}} D} \geq \# G_0.$$

Towards division algebra

In fact we only need to find finite subgroups that live in $\mathbb{Q}$-division algebras. The order $\mathcal{O}$ can be aligned according to the finite group. Fortunately, there exists a complete classification of such finite subgroups due to Amitsur, 1955.

Towards division algebra

FINITE SUBGROUPS OF DIVISION RINGS

BY

S. A. AMITSUR

1. **Introduction.** The problem of determining all finite groups which can be embedded in the multiplicative group of the nonzero elements of division rings was first proposed and partially solved in [6] by I. N. Herstein. It was shown there that the only finite subgroup of division rings of finite characteristic are cyclic, and that the subgroups of odd order of division rings of characteristic zero are of a very special type [6, Theorem 5]. In particular, the odd subgroups of the real quaternions are all cyclic. This brought I. N. Herstein to the conjecture that all odd subgroups of division rings are cyclic.

The purpose of the present paper is to determine completely all subgroups (of even and odd order) of division rings. These groups are classified in five classes connected in some way to the finite groups of rotations of the 3-Euclidean sphere. Among others we disprove the conjecture of Herstein and exhibit infinitely many finite subgroups of division rings of odd order. In particular the minimal order of an odd noncyclic group contained in a division ring is 63.

Towards division algebra

FINITE SUBGROUPS OF DIVISION RINGS

BY

S. A. AMITSUR

1. **Introduction.** The problem of determining all finite groups which can be embedded in the multiplicative group of the nonzero elements of division rings was first proposed and partially solved in [6] by I. N. Herstein. It was shown there that the only finite subgroup of division rings of finite characteristic are cyclic, and that the subgroups of odd order of division rings of characteristic zero are of a very special type [6, Theorem 5]. In particular, the odd subgroups of the real quaternions are all cyclic. This brought I. N. Herstein to the conjecture that all odd subgroups of division rings are cyclic.

The purpose of the present paper is to determine completely all subgroups (of even and odd order) of division rings. These groups are classified in five classes connected in some way to the finite groups of rotations of the 3-Euclidean sphere. Among others we disprove the conjecture of Herstein and exhibit infinitely many finite subgroups of division rings of odd order. In particular the minimal order of an odd noncyclic group contained in a division ring is 63.

LEMMA 7. *Let x, y be two integers and let $\beta=\beta(q,\ x-1)\geqq 1$* (i.e., $x\equiv 1 \pmod q$)) *and $\beta_\nu=(q,\ y)\geqq 0$ for a prime q. Then:* (1) *if* $q\neq 2$ or $\beta\geqq 2$ (*i.e.,* $x\equiv 1 \pmod 4$) *in case* $q=2$) *then* $\beta(q,\ x^\nu-1)=\beta+\beta_\nu$. (2) *If $q=2$ and $\beta=1$ then: $\beta_\nu=0$ implies that $\beta(2,\ x^\nu-1)=1$, and $\beta_\nu\geqq 1$ implies that $\beta(2,\ x^\nu-1)=\beta_\nu+i+1$ where $x=1+2+\cdots+2^i+2^{i+2}x_1$, $i\geqq 1$.*

The proof is by induction on β_ν. If $\beta_\nu=0$, let $x=1+q^\beta z$, $(z,\ q)=1$. Then, $(1+q^\beta z)^\nu=1+q^\beta yz+$terms with higher powers of q, and this case is proved since $(yz,\ q)=1$. Let $y=qy'=q^{\beta_\nu}y''$, $(y'',\ q)=1$, and $\beta_\nu\geqq 1$. By induction it follows that $x^{\nu'}=1+q^{\beta+\beta_\nu-1}u$, $(u,\ q)=1$. Hence,

$$x^\nu=(1+q^{\beta+\beta_\nu-1}u)^q=1+q^{\beta+\beta_\nu}u+\cdots+C_{q,\nu}\,q^{\nu(\beta+\beta_\nu-1)}u^{q-\nu}+\cdots.$$

The highest power of q dividing

$$C_{q,\nu}\,q^{\nu(\beta+\beta_\nu-1)}\ u^{q-\nu}$$

is $\nu(\beta+\beta_\nu-1)+1$ if $1\leqq\nu<q$ and it is $q(\beta+\beta_\nu-1)$ if $\nu=q$. Hence, the exceptional case to the proof of this lemma may occur if $q(\beta+\beta_\nu-1)=1\cdot(\beta+\beta_\nu-1)+1$. Equivalently, $(q-1)(\beta+\beta_\nu)=q$. This may happen only if $q=2$ and $\beta+\beta_\nu=2$. This proves the first part of the lemma.

To prove the second part it suffices to show it only for $y=2$. For, if x is

THEOREM 5. *A necessary and sufficient condition that $\mathfrak{A}_{m,r}$ is a division algebra is that* (3C) *or* (3D) *holds and either:*

(1) $n=s=2$ *and* $r\equiv -1 \pmod m$ *or,*

(2) *For every prime $q\mid n$ there exists a prime $p\mid m$ such that $q\nmid n_p$ and that one of the following holds:*

(2a) $p\equiv 1 \pmod 4$ *or* $q\neq 2$ *and* $\beta(q,\ s)\geqq\beta(q,\ p-1)+\mathrm{Max}_i\,\beta(q,\ \gamma_i)$.

(2b) $p\equiv 1+2+\cdots+2^i \pmod{2^{i+2}}$, $i\geqq 1$ *and* $q=2$, (3C) *holds; and* $\beta(2,\ s)\geqq i+1+\mathrm{Max}\,\{1,\ \beta(2,\ \gamma_i)\}$ *if* $s\equiv 0 \pmod 4$, *but if* $s\not\equiv 0 \pmod 4$ *then all* $\beta(2,\ \gamma_i)=0$; i.e., *all γ_i are odd integers.*

(2c) $p=q=2$, (3D) *holds, $m/4$ and all γ_i are odd integers.*

Proof. Evidently, (1) of Theorem 4 and condition (1) of the present theorem are equivalent. The proof of this theorem will be achieved by showing that the condition (2a) is equivalent to (I_1), (2b) is equivalent to (II_2) and that (2c) and (b) of Theorem 4 are equivalent. This will prove the theorem since it was shown that (I_1) and (I_2) together are equivalent to (a) of Theorem 4.

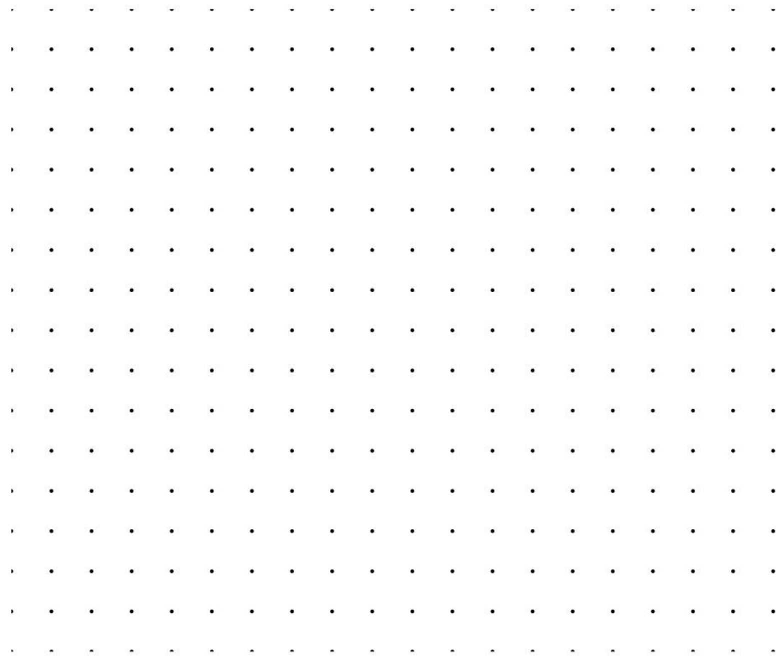
Substituting (III_1) in (II) we obtain by (IV) that (I_1) is equivalent to the

Towards division algebra

For brewity, we will not discuss classification of of finite subgroups ofdivision rings. Instead, let us talk about effectiveness of these results.

Controlled randomness

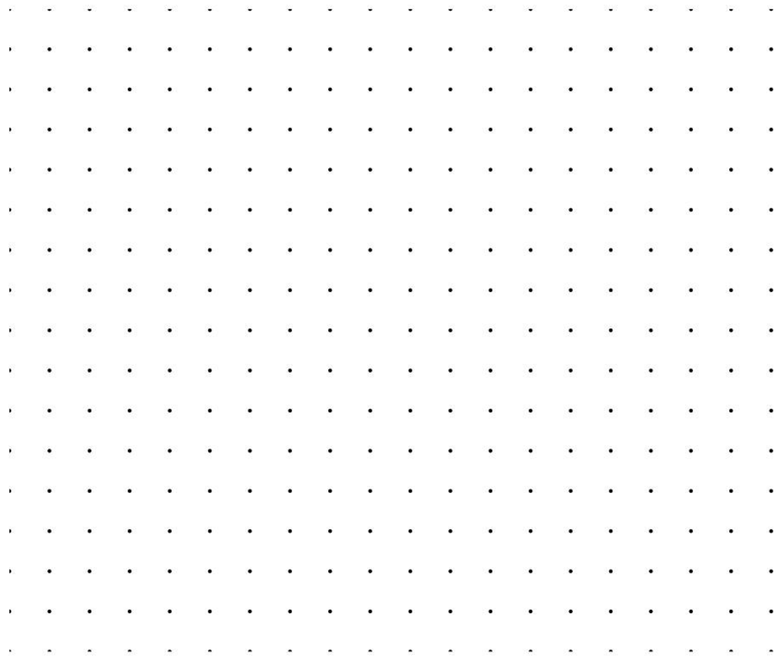
Visualizing in $\mathbb{R}^2$



Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

Visualizing in $\mathbb{R}^2$



$p = 5$

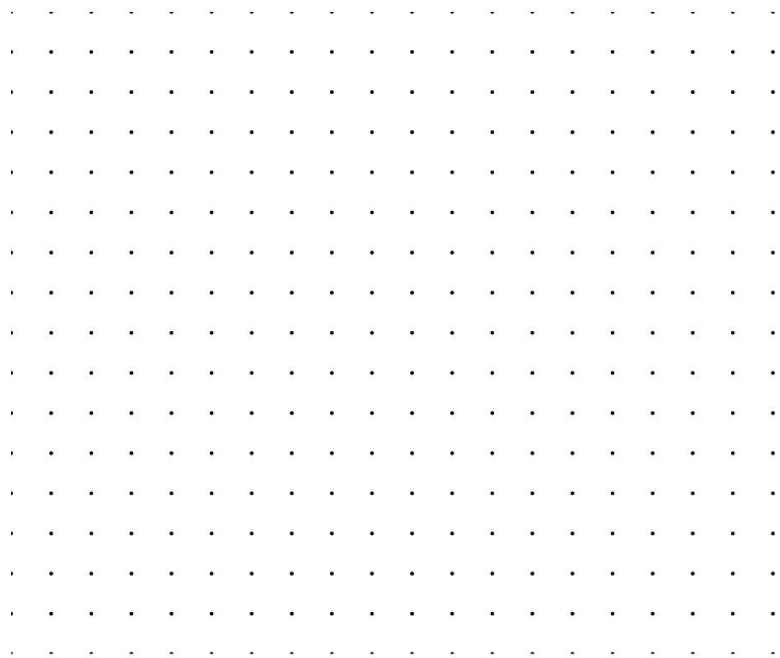
Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p \, v \setminus \{0\})$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

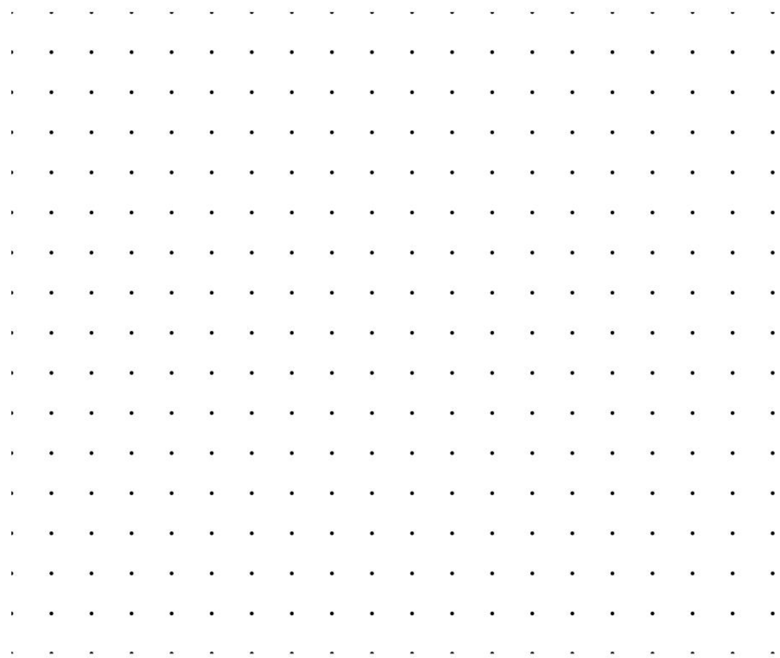
$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

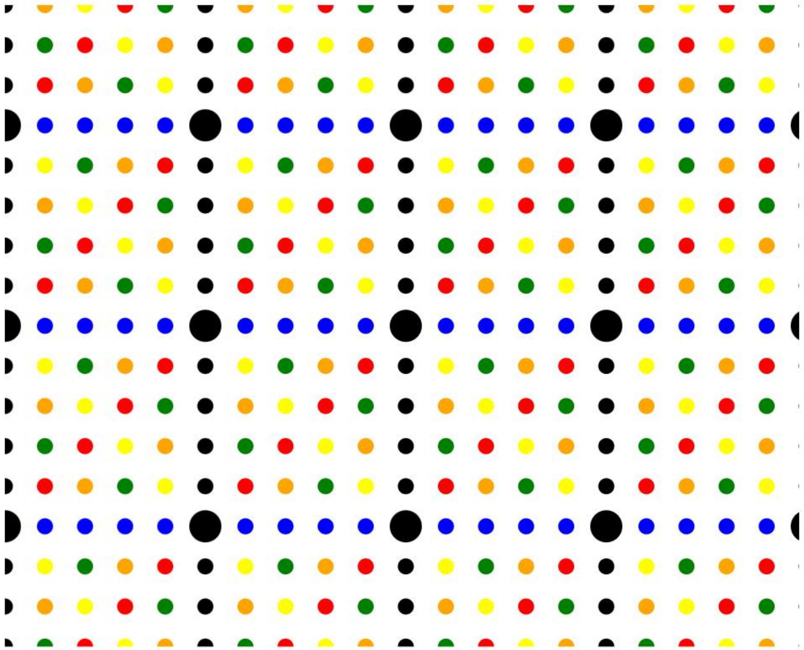
$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

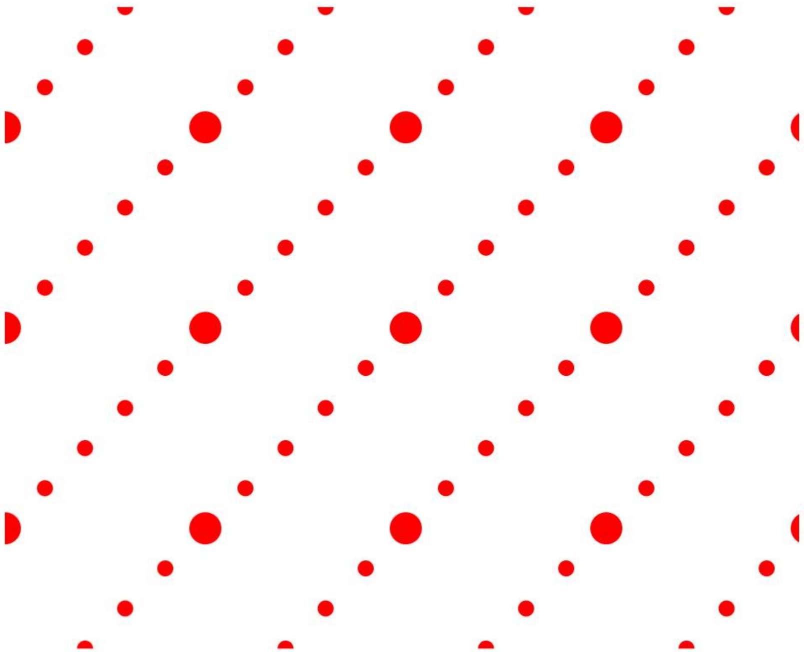
$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

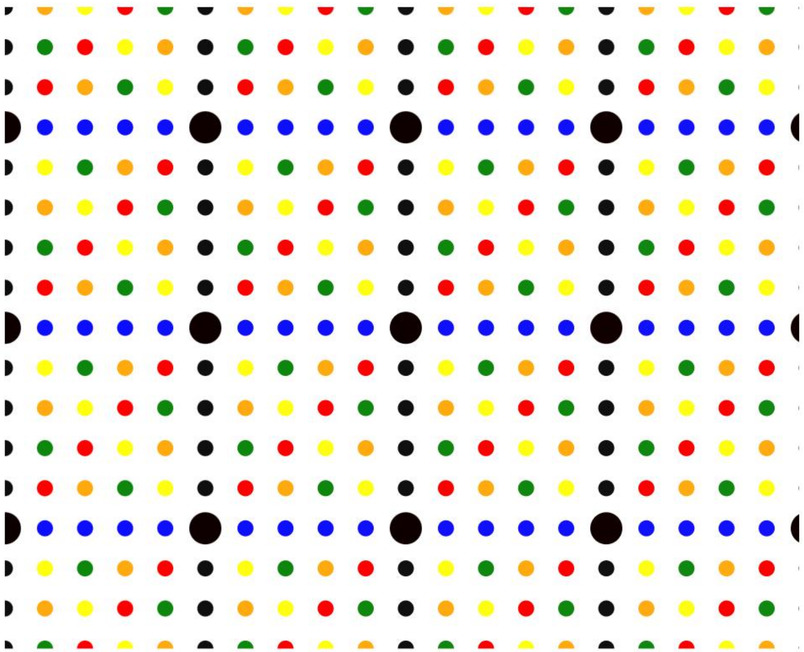
$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

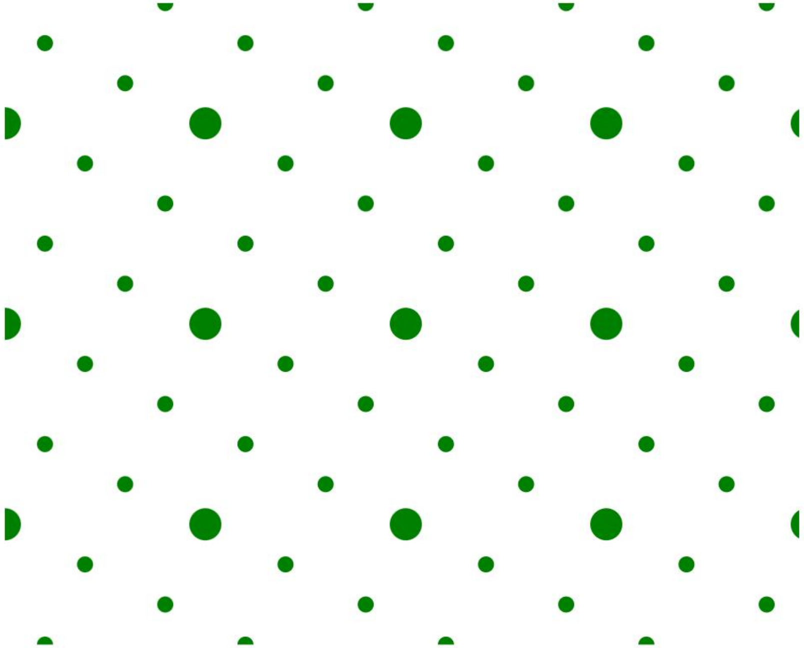
$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

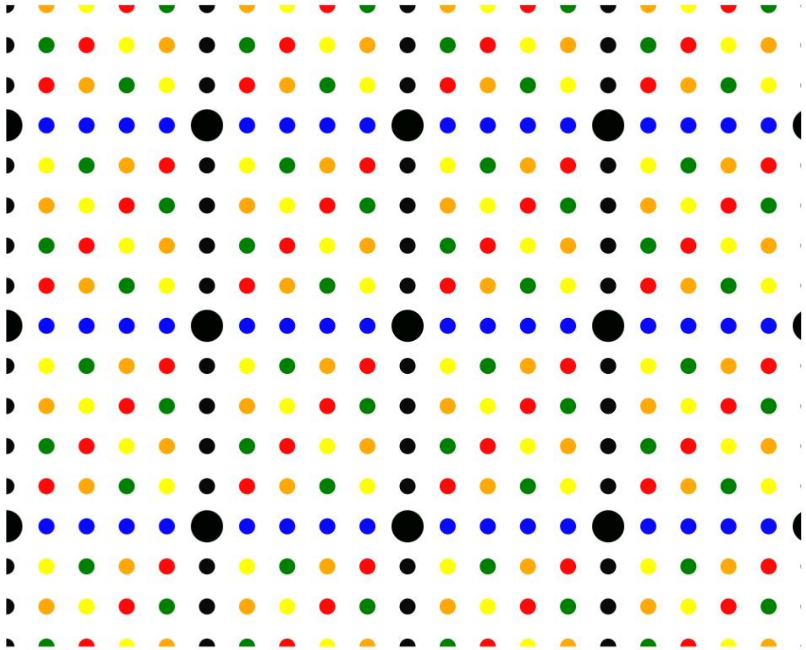
$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p v \setminus \{0\})$$

This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p v \setminus \{0\})$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

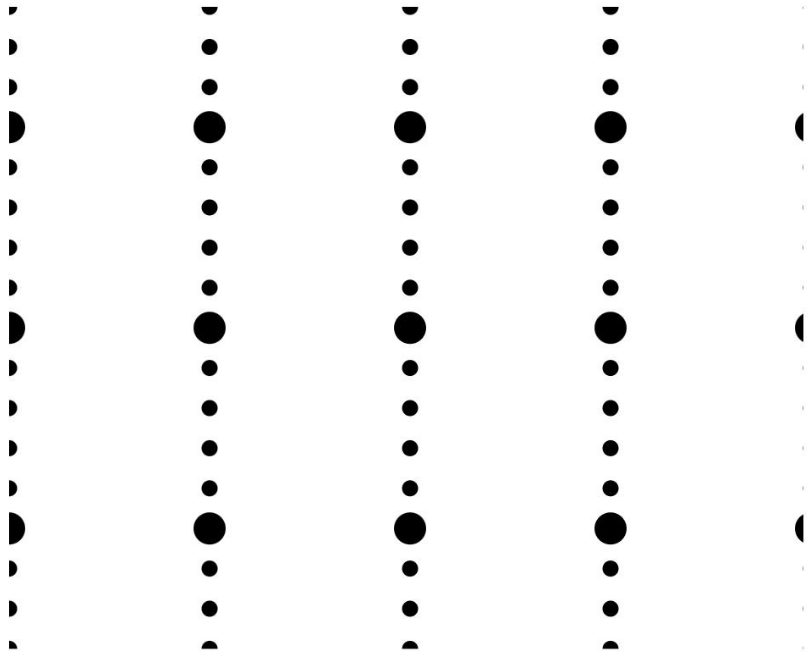
$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

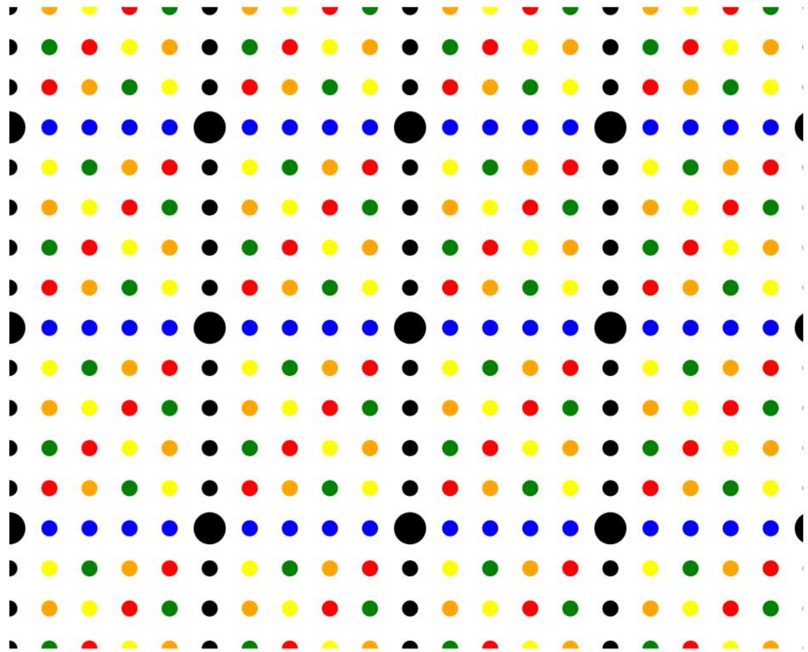
This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Let us put all these sub-lattices in one set

$$\mathcal{L}_p' = \{\pi_p^{-1}(\mathbb{F}_p\, v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\}.$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

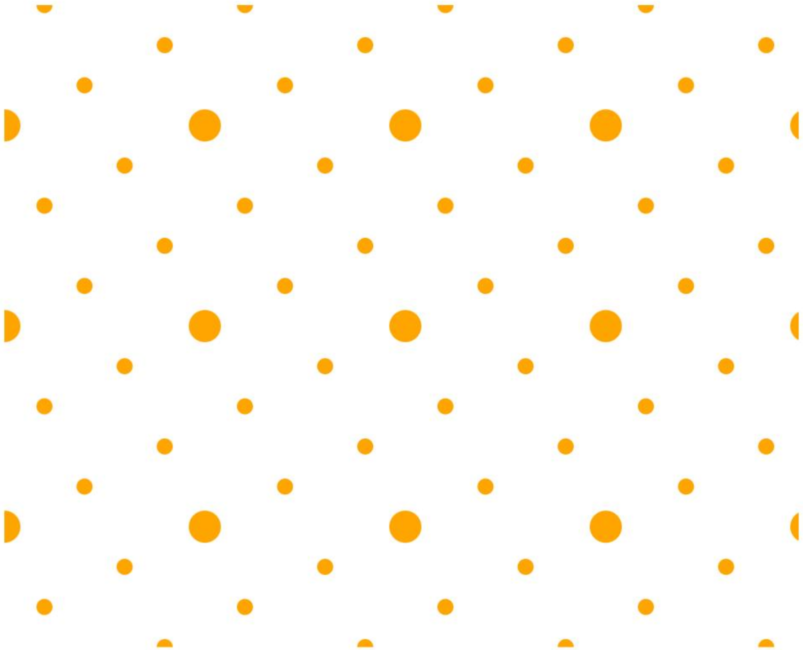
This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Let us put all these sub-lattices in one set

$$\mathcal{L}'_p = \{\pi_p^{-1}(\mathbb{F}_p\, v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\}.$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

Choose a prime number p. Consider the map $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$.

$\mathbb{F}_p^d \setminus \{0\}$ is a disjoint union of lines.

$$\mathbb{F}_p^d \setminus \{0\} = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} (\mathbb{F}_p\, v \setminus \{0\})$$

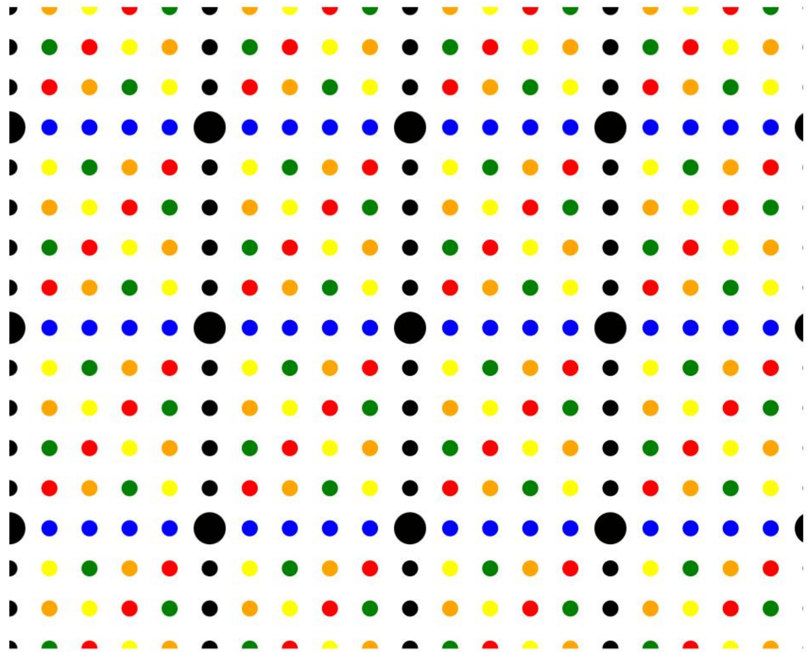
This implies that

$$\mathbb{Z}^d \setminus p\mathbb{Z}^d = \bigsqcup_{v \in (\mathbb{F}_p^d \setminus \{0\})/\mathbb{F}_p^*} \pi_p^{-1}(\mathbb{F}_p\, v \setminus \{0\})$$

Let us put all these sub-lattices in one set

$$\mathcal{L}_p' = \{\pi_p^{-1}(\mathbb{F}_p\, v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\}.$$

Visualizing in $\mathbb{R}^2$



$p = 5$

Controlled randomness

However the lattices in $\mathcal{L}'_p$ are not unit covolume. But each one of them has a covolume of p^{d-1}.

Controlled randomness

However the lattices in $\mathcal{L}_p'$ are not unit covolume. But each one of them has a covolume of p^{d-1}.

So appropriately normalizing, elements of this set become unit covolume lattices.

$$\mathcal{L}_p = \{C_p \pi_p^{-1}(\mathbb{F}_p v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\},$$

when $C_p = p^{-\left(1-\frac{1}{d}\right)}$.

Controlled randomness

However the lattices in $\mathcal{L}'_p$ are not unit covolume. But each one of them has a covolume of p^{d-1}.

So appropriately normalizing, elements of this set become unit covolume lattices.

$$\mathcal{L}_p = \{C_p \pi_p^{-1}(\mathbb{F}_p v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\},$$

when $C_p = p^{-\left(1-\frac{1}{d}\right)}$.

So $\mathcal{L}_p \subseteq X_d$ is a set of unit covolume lattices, with $\#\mathcal{L}_p \to \infty$ as $p \to \infty$.

Controlled randomness

However the lattices in $\mathcal{L}'_p$ are not unit covolume. But each one of them has a covolume of p^{d-1}.

So appropriately normalizing, elements of this set become unit covolume lattices.

$$\mathcal{L}_p = \{C_p \pi_p^{-1}(\mathbb{F}_p v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\},$$

when $C_p = p^{-\left(1-\frac{1}{d}\right)}$.

So $\mathcal{L}_p \subseteq X_d$ is a set of unit covolume lattices, with $\#\mathcal{L}_p \to \infty$ as $p \to \infty$.

Now as before let $f : \mathbb{R}^d \to \mathbb{R}$ be a compactly supported Riemann integrable function. Let $\Phi_f : X_d \to \mathbb{R}$ again be the lattice-sums of f.

Controlled randomness

However the lattices in $\mathcal{L}'_p$ are not unit covolume. But each one of them has a covolume of p^{d-1}.

So appropriately normalizing, elements of this set become unit covolume lattices.

$$\mathcal{L}_p = \{C_p \pi_p^{-1}(\mathbb{F}_p v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\},$$

when $C_p = p^{-\left(1-\frac{1}{d}\right)}$.

So $\mathcal{L}_p \subseteq X_d$ is a set of unit covolume lattices, with $\#\mathcal{L}_p \to \infty$ as $p \to \infty$.

Now as before let $f : \mathbb{R}^d \to \mathbb{R}$ be a compactly supported Riemann integrable function. Let $\Phi_f : X_d \to \mathbb{R}$ again be the lattice-sums of f.

What do you expect this quantity to be as $p \to \infty$?

$$\frac{1}{\#\mathcal{L}_p} \sum_{\Lambda \in \mathcal{L}_p} \Phi_f(\Lambda) = \frac{1}{\#\mathcal{L}_p} \sum_{\Lambda \in \mathcal{L}_p} \left(\sum_{v \in \Lambda \setminus \{0\}} f(v) \right)$$

Controlled randomness

The answer to this question is very classical.

Controlled randomness

The answer to this question is very classical.

Theorem *(Rogers, 1947)*

Let p be an arbitrary prime, $\mathbb{F}_p$ be the field with p elements and let $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$ be the natural coordinate-wise projection map. Let $\mathcal{L}_p$ be the set of sub-lattices of $\mathbb{Z}^d$ that are pre-images of one-dimensional subspaces in this projection map scaled to become unit covolume, i.e.

$$\mathcal{L}_p = \{C_p \pi_p^{-1}(\mathbb{F}_p v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\}, C_p = p^{-\left(1-\frac{1}{d}\right)}.$$

Consider a compactly supported continuous function $f : \mathbb{R}^d \to \mathbb{R}$ and the lattice-sum function $\Phi_f : X_d \to \mathbb{R}$. Then the following holds.

$$\lim_{p\to\infty} \left[\frac{1}{\#\mathcal{L}_p} \sum_{\Lambda\in\mathcal{L}_p} \Phi_f(\Lambda)\right] = \int_{\mathbb{R}^d} f(x)dx.$$

Controlled randomness

The answer to this question is very classical.

Theorem *(Rogers, 1947)*

Let p be an arbitrary prime, $\mathbb{F}_p$ be the field with p elements and let $\pi_p : \mathbb{Z}^d \to \mathbb{F}_p^d$ be the natural coordinate-wise projection map. Let $\mathcal{L}_p$ be the set of sub-lattices of $\mathbb{Z}^d$ that are pre-images of one-dimensional subspaces in this projection map scaled to become unit covolume, i.e.

$$\mathcal{L}_p = \{C_p \pi_p^{-1}(\mathbb{F}_p v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\}, C_p = p^{-\left(1-\frac{1}{d}\right)}.$$

Consider a compactly supported continuous function $f : \mathbb{R}^d \to \mathbb{R}$ and the lattice-sum function $\Phi_f : X_d \to \mathbb{R}$. Then the following holds.

$$\lim_{p\to\infty} \left[\frac{1}{\#\mathcal{L}_p} \sum_{\Lambda\in\mathcal{L}_p} \Phi_f(\Lambda)\right] = \int_{\mathbb{R}^d} f(x)dx.$$

After using the integrality gap lemma, this is a constructive proof of $c_d \geq 2$.

Controlled randomness

Since we are working with finitely many lattices, we can use this procedure to obtain a probabilistic algorithm that randomly generates lattices with good packing efficiency

Controlled randomness

Since we are working with finitely many lattices, we can use this procedure to obtain a probabilistic algorithm that randomly generates lattices with good packing efficiency

This idea can be generalized to number fields, as was shown by (Moustrou, 2016).

Controlled randomness

Since we are working with finitely many lattices, we can use this procedure to obtain a probabilistic algorithm that randomly generates lattices with good packing efficiency

This idea can be generalized to number fields, as was shown by (Moustrou, 2016).

We can also generalize the proof for division rings. But what are analogue of prime ideals for division rings?

Controlled randomness

Since we are working with finitely many lattices, we can use this procedure to obtain a probabilistic algorithm that randomly generates lattices with good packing efficiency

This idea can be generalized to number fields, as was shown by (Moustrou, 2016).

We can also generalize the proof for division rings. But what are analogue of prime ideals for division rings?

Suppose D is a $\mathbb{Q}$-division ring, K be the center of the ring and $\mathcal{O}$ be an $\mathcal{O}_K$-order in D. Let $[D:K]=n^2$.

A prime ideal of an $\mathcal{O}$ is a proper two-sided ideal $\mathfrak{p}$ in $\mathcal{O}$ such that $K \cdot \mathfrak{p} = D$ and such that for every pair of two sided ideals S, T in $\mathcal{O}$, we have that $S \cdot T \subset \mathfrak{p}$ implies $S \subset \mathfrak{p}$ or $T \subset \mathfrak{p}$.

Controlled randomness

Since we are working with finitely many lattices, we can use this procedure to obtain a probabilistic algorithm that randomly generates lattices with good packing efficiency

This idea can be generalized to number fields, as was shown by (Moustrou, 2016).

We can also generalize the proof for division rings. But what are analogue of prime ideals for division rings?

Suppose D is a $\mathbb{Q}$-division ring, K be the center of the ring and $\mathcal{O}$ be an $\mathcal{O}_K$-order in D. Let $[D : K] = n^2$.

A prime ideal of an $\mathcal{O}$ is a proper two-sided ideal $\mathfrak{p}$ in $\mathcal{O}$ such that $K \cdot \mathfrak{p} = D$ and such that for every pair of two sided ideals S, T in $\mathcal{O}$, we have that $S \cdot T \subset \mathfrak{p}$ implies $S \subset \mathfrak{p}$ or $T \subset \mathfrak{p}$.

Important property: For all but finitely many primes $\mathfrak{p}$ of $\mathcal{O}$, the quotient $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is isomorphic to $M_n(\mathbb{F}_q)$, where $\mathcal{O}_K/\mathcal{O}_K \cap \mathfrak{p} \cong \mathbb{F}_q$.

Controlled randomness

Since we are working with finitely many lattices, we can use this procedure to obtain a probabilistic algorithm that randomly generates lattices with good packing efficiency

This idea can be generalized to number fields, as was shown by (Moustrou, 2016).

We can also generalize the proof for division rings. But what are analogue of prime ideals for division rings?

Suppose D is a $\mathbb{Q}$-division ring, K be the center of the ring and $\mathcal{O}$ be an $\mathcal{O}_K$-order in D. Let $[D : K] = n^2$.

A prime ideal of an $\mathcal{O}$ is a proper two-sided ideal $\mathfrak{p}$ in $\mathcal{O}$ such that $K \cdot \mathfrak{p} = D$ and such that for every pair of two sided ideals S, T in $\mathcal{O}$, we have that $S \cdot T \subset \mathfrak{p}$ implies $S \subset \mathfrak{p}$ or $T \subset \mathfrak{p}$.

Important property: For all but finitely many primes $\mathfrak{p}$ of $\mathcal{O}$, the quotient $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is isomorphic to $M_n(\mathbb{F}_q)$, where $\mathcal{O}_K/\mathcal{O}_K \cap \mathfrak{p} \cong \mathbb{F}_q$.

Hence we get countably many projection maps $\pi_{\mathfrak{p}} : \mathcal{O} \to M_n(\mathbb{F}_q)$.

Controlled randomness

Theorem *(G., Serban, 2021)*

Let $d = 2[D:\mathbb{Q}]$. Let $\mathfrak{p} \subseteq \mathcal{O}$ be a prime as above and let $\pi_{\mathfrak{p}} : \mathcal{O}^t \to M_n(\mathbb{F}_q)^2$ be the projection map as above (on two copies of $\mathcal{O}$). Consider the set of sub-lattices of $\mathcal{O}^2$ that are pre-images of $M_n(\mathbb{F}_q)$-submodules of $\mathbb{F}_q$-dimension $n(2n-1)$, i.e.

$$\begin{aligned} \mathcal{C}_{\mathfrak{p}} &= \{C \subseteq M_n(\mathbb{F}_q)^2 \mid C \text{ is a } M_n(\mathbb{F}_q)\text{-submodule } \simeq (\mathbb{F}_q^n)^{\oplus(2n-1)}\}, \\ \mathcal{L}_{\mathfrak{p}} &= \{\beta_{\mathfrak{p}} \pi_{\mathfrak{p}}^{-1}(C) \mid C \in \mathcal{C}_{\mathfrak{p}}\}, \quad \beta_{\mathfrak{p}} = q^{-1/nmt} \end{aligned}$$

Consider a compactly supported continuous function $f : \mathbb{R}^d \to \mathbb{R}$ and the lattice-sum function $\Phi_f : X_d \to \mathbb{R}$. Then the following holds.

$$\lim_{\#\mathbb{F}_q \to \infty} \left[\frac{1}{\#\mathcal{L}_{\mathfrak{p}}} \sum_{\Lambda \in \mathcal{L}_{\mathfrak{p}}} \Phi_f(\Lambda) \right] = \int_{\mathbb{R}^d} f(x) dx.$$

where the dx on the right-hand side is that Lebesgue measure on $\mathbb{R}^d$ that makes $\mathcal{O}^2 \subseteq (D \otimes \mathbb{R})^2 \simeq \mathbb{R}^d$ of unit covolume.

Controlled randomness

We can therefore prove the following from above.

Controlled randomness

We can therefore prove the following from above.

Theorem *(G., Serban, 2021)*

Let $m_k = \prod_{\substack{p \leq k \text{ prime} \\ 2 \nmid \text{ord}_2 p}} p$ and set $n_k := 8\varphi(m_k)$. Then for any $\varepsilon > 0$ there is an effective constant c_ε such that for $k > c_\varepsilon$ a lattice Λ in dimension n_k with density

$$\Delta(\Lambda) \geq (1 - \varepsilon)\frac{24 \cdot m_k}{2^{n_k}}$$

can be constructed in $e^{4.5 \cdot n_k \log(n_k)(1+o(1))}$ binary operations. This construction leads to the asymptotic density of $\Delta(\Lambda) \geq (1 - e^{-n_k})\frac{3 \cdot n_k (\log\log n_k)^{7/24}}{2^{n_k}}$.

Controlled randomness

We can therefore prove the following from above.

Theorem *(G., Serban, 2021)*

Let $m_k = \prod_{\substack{p \leq k \text{ prime} \\ 2 \nmid \text{ord}_2 p}} p$ and set $n_k := 8\varphi(m_k)$. Then for any $\varepsilon > 0$ there is an effective constant c_ε such that for $k > c_\varepsilon$ a lattice Λ in dimension n_k with density

$$\Delta(\Lambda) \geq (1 - \varepsilon)\frac{24 \cdot m_k}{2^{n_k}}$$

can be constructed in $e^{4.5 \cdot n_k \log(n_k)(1+o(1))}$ binary operations. This construction leads to the asymptotic density of $\Delta(\Lambda) \geq (1 - e^{-n_k})\frac{3 \cdot n_k (\log \log n_k)^{7/24}}{2^{n_k}}$.

The sequence above is actually the sequence of green points mentioned before. This theorem shows that the construction is also effective.

Controlled randomness

We can therefore prove the following from above.

Theorem *(G., Serban, 2021)*

Let $m_k = \prod_{\substack{p \le k \text{ prime} \\ 2 \nmid \mathrm{ord}_2 p}} p$ and set $n_k := 8\varphi(m_k)$. Then for any $\varepsilon > 0$ there is an effective constant c_ε such that for $k > c_\varepsilon$ a lattice Λ in dimension n_k with density

$$\Delta(\Lambda) \ge (1-\varepsilon)\frac{24 \cdot m_k}{2^{n_k}}$$

can be constructed in $e^{4.5 \cdot n_k \log(n_k)(1+o(1))}$ binary operations. This construction leads to the asymptotic density of $\Delta(\Lambda) \ge (1-e^{-n_k})\frac{3 \cdot n_k (\log\log n_k)^{7/24}}{2^{n_k}}$.

The sequence above is actually the sequence of green points mentioned before. This theorem shows that the construction is also effective.

The condition of $2 \nmid \mathrm{ord}_p 2$ has to do with division ring contructions. Details can be given on request!

Open questions and ongoing work

Open questions and ongoing work

Open problem:

What are explicit descriptions of lattices that prove at least Minkowski's lower bounds as $d \to \infty$? That is, what are the lattices that have the most optimal packing density in large dimensions?

In terms of coding theory, this problem is to find explicitly lattices that achieve "goodness"

$$\Delta(\Lambda^{(d)})^{\frac{1}{d}} = \frac{r_{\text{pack}}(\Lambda^{(d)})}{r_{\text{eff}}(\Lambda^{(d)})} \geq \frac{1}{2},$$

for a subsequence of lattices $\Lambda^{(d)} \subseteq \mathbb{R}^d$ as $d \to \infty$.

Open questions and ongoing work

Open problem:

What are explicit descriptions of lattices that prove at least Minkowski's lower bounds as $d \to \infty$? That is, what are the lattices that have the most optimal packing density in large dimensions?

In terms of coding theory, this problem is to find explicitly lattices that achieve "goodness"

$$\Delta(\Lambda^{(d)})^{\frac{1}{d}} = \frac{r_{\text{pack}}(\Lambda^{(d)})}{r_{\text{eff}}(\Lambda^{(d)})} \geq \frac{1}{2},$$

for a subsequence of lattices $\Lambda^{(d)} \subseteq \mathbb{R}^d$ as $d \to \infty$.

This is like the problem of finding **hay** in a haystack!

Open questions and ongoing work

Open problem:

What are explicit descriptions of lattices that prove at least Minkowski's lower bounds as $d \to \infty$? That is, what are the lattices that have the most optimal packing density in large dimensions?

In terms of coding theory, this problem is to find explicitly lattices that achieve "goodness"

$$\Delta(\Lambda^{(d)})^{\frac{1}{d}} = \frac{r_{\text{pack}}(\Lambda^{(d)})}{r_{\text{eff}}(\Lambda^{(d)})} \geq \frac{1}{2},$$

for a subsequence of lattices $\Lambda^{(d)} \subseteq \mathbb{R}^d$ as $d \to \infty$.

This is like the problem of finding **hay** in a haystack!

Need to decrease the search space to get smaller running times.

Open questions and ongoing work

Open problem:

Explicitly describe the higher moments of these random lattices.
That is, give a mean value formula for $\left(\sum_{v\in\Lambda} f(v)\right)^2, \left(\sum_{v\in\Lambda} f(v)\right)^3, \ldots$ for any of these random sets of lattices.

Open questions and ongoing work

Open problem:

Explicitly describe the higher moments of these random lattices.
That is, give a mean value formula for $\left(\sum_{v\in\Lambda} f(v)\right)^2, \left(\sum_{v\in\Lambda} f(v)\right)^3, \ldots$ for any of these random sets of lattices.

For the $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$ case, we have (Rogers, 1955-56) papers. This created a lower bound of $c_d \geq \frac{1}{3}\sqrt{d}$, which was the best back then.

Open questions and ongoing work

Open problem:

Explicitly describe the higher moments of these random lattices.
That is, give a mean value formula for $\left(\sum_{v\in\Lambda} f(v)\right)^2, \left(\sum_{v\in\Lambda} f(v)\right)^3, \ldots$ for any of these random sets of lattices.

For the $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$ case, we have (Rogers, 1955-56) papers. This created a lower bound of $c_d \geq \frac{1}{3}\sqrt{d}$, which was the best back then.

Such work has not been satisfactorily generalized to $SL_t(K)/SL_t(\mathcal{O}_K)$. This is an ongoing project jointly with V. Serban and M. Viazovska.

Open questions and ongoing work

Question:

Do the effective families of lattices equidistribute in the moduli space of lattices? This is a question of arithmetic dynamics.

Open questions and ongoing work

Question:

Do the effective families of lattices equidistribute in the moduli space of lattices? This is a question of arithmetic dynamics.

For $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$ and $SL_d(K)/SL_d(\mathcal{O}_K)$, this is known due to the work of Eskin, Oh, Ullmo.

Open questions and ongoing work

Question:

Do the effective families of lattices equidistribute in the moduli space of lattices? This is a question of arithmetic dynamics.

For $SL_d(\mathbb{R})/SL_d(\mathbb{Z})$ and $SL_d(K)/SL_d(\mathcal{O}_K)$, this is known due to the work of Eskin, Oh, Ullmo.

For division rings, this is still open.

Thank you for your attention!

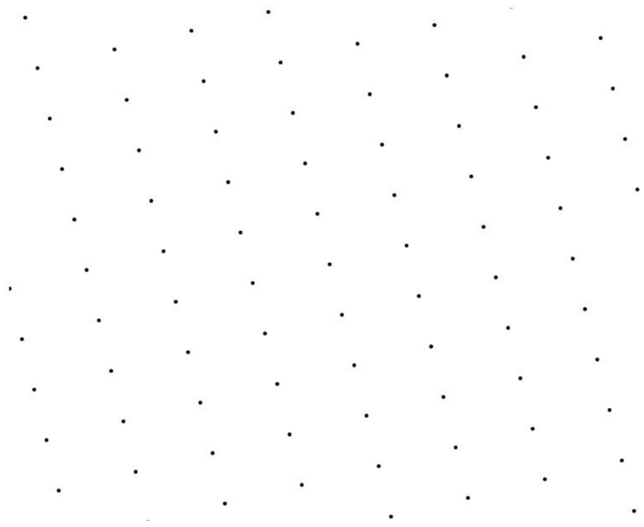
Email:
`nihar.gargava@epfl.ch`

Based on arXiv preprints:
`2107.04844, 2111.03684`

Slides:
`nihargargava.com/cap_2022`

How does it work?:
This presentation and all the animations are written in `html` and `javascript` using reveal.js and d3.js.

Feel free to contact for questions/comments.



Appendix: How to generate random 2-dimensional lattices

To the map $\psi : [\pi/3, 2\pi/3] \times]0, 1] \to \mathbb{H}$ given by $\psi(a, b) = \cos(a) + i \sin(a)/b$ is a measure preserving map!

It maps the rectangle bijectively to a fundamental domain of $\mathbb{H}/SL_2(\mathbb{Z})$.

Using this, the following map randomly generates a lattice.

$$\psi_1 : [0, 2\pi] \times [\pi/3, 2\pi/3] \times]0, 1] \to SL_2(\mathbb{R})$$

$$\psi_1(x, y, z) = \begin{bmatrix} 1 & \cos(y) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \left(\frac{\sin(y)}{z}\right)^{\frac{1}{2}} & 0 \\ 0 & \left(\frac{\sin(y)}{z}\right)^{-\frac{1}{2}} \end{bmatrix} \begin{bmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{bmatrix}$$

This only works for $d = 2$. It is not known how to generalize this to higher dimensions!