On the density of cyclotomic lattices constructed from codes

Philippe Moustrou

Université de Bordeaux

Network Coding and Designs
Dubrovnik, 07.04.2016

PhD funded by:

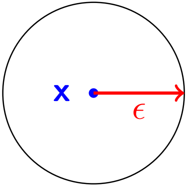
CPU
Numerical certification
& reliability

supervised by:
Christine Bachoc (IMB) and Arnaud Pêcher (LaBRI)

Outline

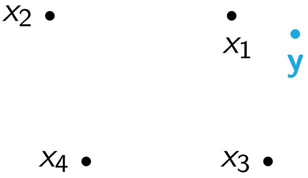
Motivation: Decoding without Ambiguity

Consider a noisy channel over $\mathbb{R}^n$: suppose there exists ϵ such that if $x \in \mathbb{R}^n$ is sent, with high probability, the received vector y is in $B(x, \epsilon)$:



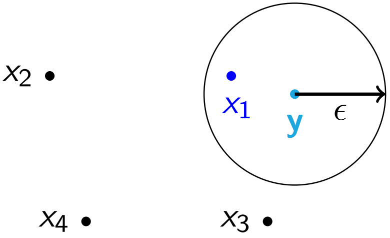
Motivation: Decoding without Ambiguity

If there is only one codeword in the ball of radius ϵ centred in the received vector y,



Motivation: Decoding without Ambiguity

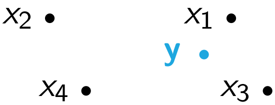
If there is only one codeword in the ball of radius ϵ centred in the received vector y, receiver can decode the message.



Motivation: Decoding without Ambiguity

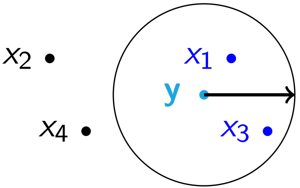
CPU Numerical certification & reliability
université de BORDEAUX

But if there is more than one word in this ball,



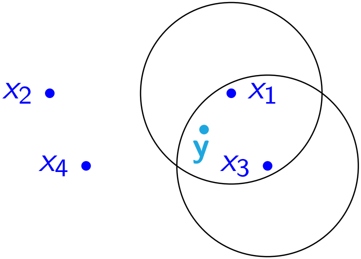
Motivation: Decoding without Ambiguity

But if there is more than one word in this ball, receiver is confused and can not decode !



Motivation: Decoding without Ambiguity

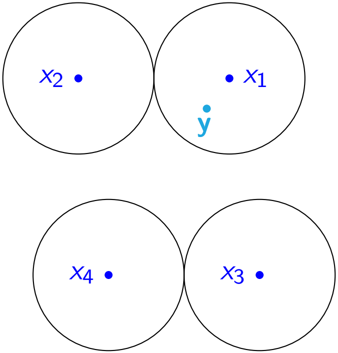
This is equivalent to the fact that the balls of radius ϵ centred in the codewords do not intersect.



Motivation: Decoding without Ambiguity

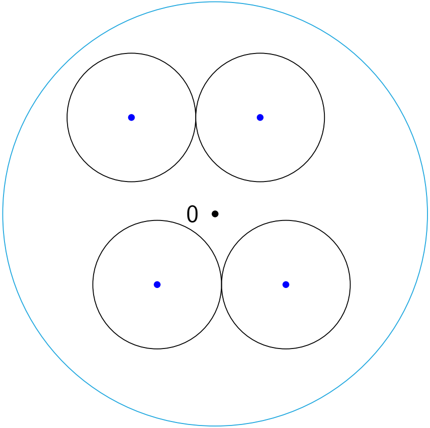
CPU Numerical certification & reliability
université de BORDEAUX

So we would like these balls to be disjoint...



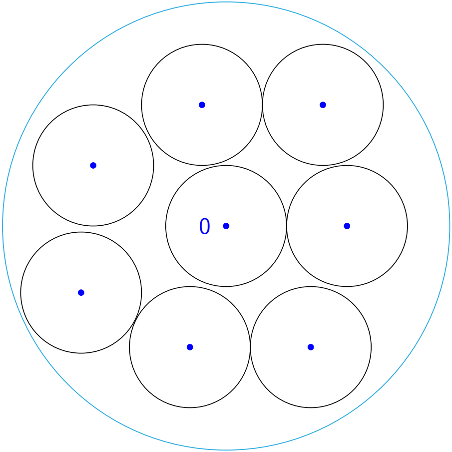
Motivation: Decoding without Ambiguity

...Keeping as many as possible codewords close to 0.



Motivation: Decoding without Ambiguity

...Keeping as many as possible codewords close to 0.



The Sphere Packing Problem

- Finding a good code with respect to this property boils down to finding an arrangement of disjoint spheres having the same radius for which the proportion of space filled is the highest possible.

The Sphere Packing Problem

CPU Numerical certification & reliability · université de BORDEAUX

- Finding a good code with respect to this property boils down to finding an arrangement of disjoint spheres having the same radius for which the proportion of space filled is the highest possible.
- This is the sphere packing problem !

The Sphere Packing Problem

CPU
Numerical certification & reliability
université de BORDEAUX

- Finding a good code with respect to this property boils down to finding an arrangement of disjoint spheres having the same radius for which the proportion of space filled is the highest possible.
- This is the sphere packing problem !
- Sphere packing problem is an old and hard problem of geometry of numbers.

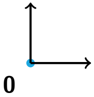
The Sphere Packing Problem

CPU Numerical certification & reliability
université de BORDEAUX

- Finding a good code with respect to this property boils down to finding an arrangement of disjoint spheres having the same radius for which the proportion of space filled is the highest possible.
- This is the sphere packing problem !
- Sphere packing problem is an old and hard problem of geometry of numbers.
- Euclidean lattices provide a way to approach this problem.

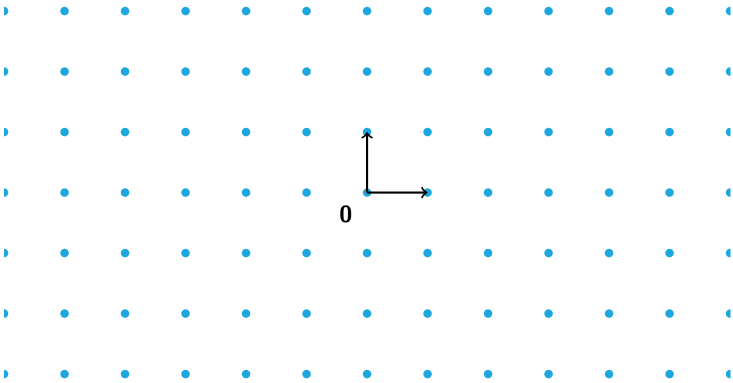
Reminder on Euclidean lattices

A Euclidean lattice Λ in $\mathbb{R}^n$ is the set of all linear combinations with integer coefficients of the elements of a basis B of $\mathbb{R}^n$.



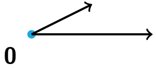
Reminder on Euclidean lattices

A Euclidean lattice Λ in $\mathbb{R}^n$ is the set of all linear combinations with integer coefficients of the elements of a basis B of $\mathbb{R}^n$.



Reminder on Euclidean lattices

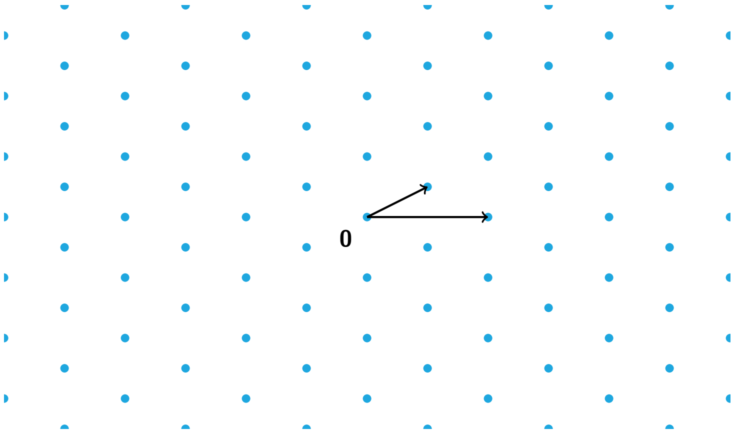
A Euclidean lattice Λ in $\mathbb{R}^n$ is the set of all linear combinations with integer coefficients of the elements of a basis B of $\mathbb{R}^n$.



Reminder on Euclidean lattices

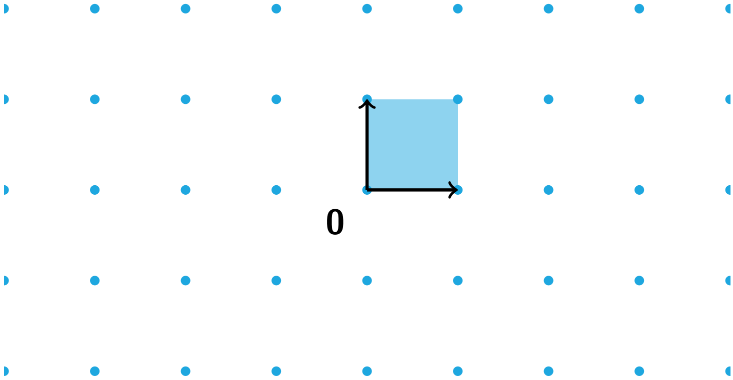
CPU Numerical certification & reliability université de BORDEAUX

A Euclidean lattice Λ in $\mathbb{R}^n$ is the set of all linear combinations with integer coefficients of the elements of a basis B of $\mathbb{R}^n$.



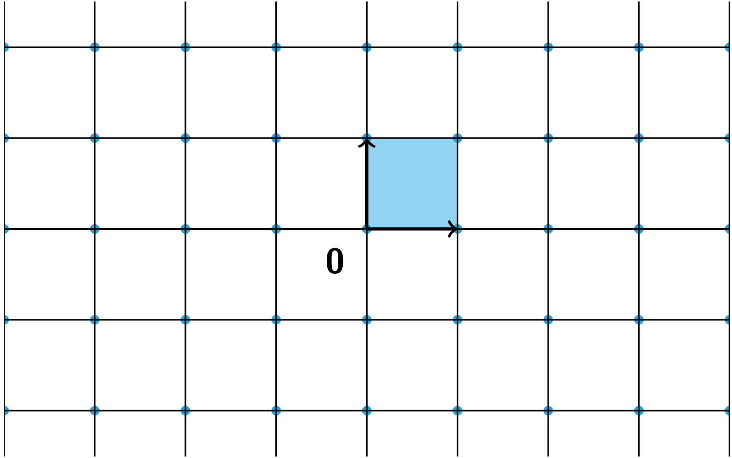
Reminder on Euclidean lattices

Let $\mathcal{P}_B$ the parallelepiped generated by B.



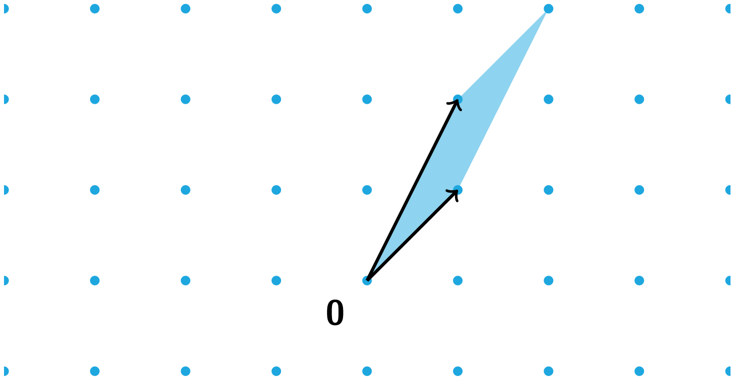
Reminder on Euclidean lattices

Translating $\mathcal{P}_B$ by the points of the lattices, we get a partition of $\mathbb{R}^n$ into equivalent cells . $\mathcal{P}_B$ is called a fundamental region of Λ.



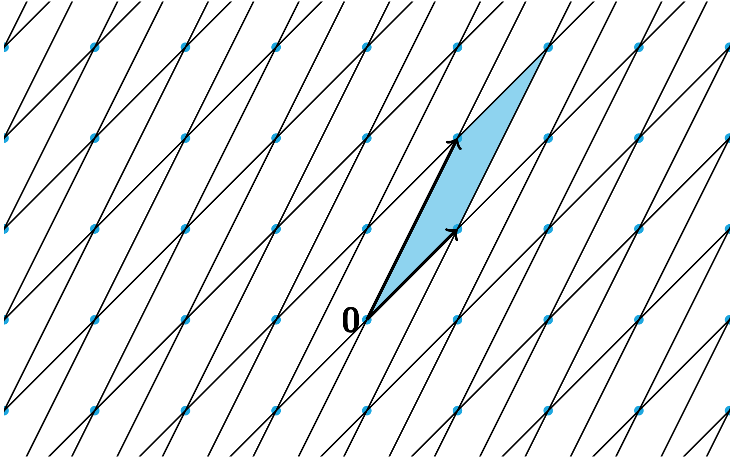
Reminder on Euclidean lattices

This is true for every basis of Λ.



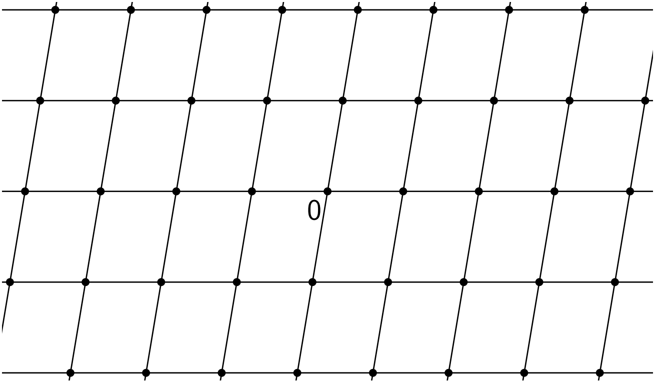
Reminder on Euclidean lattices

Every fundamental region has the same volume. This is the volume of the lattice Λ.



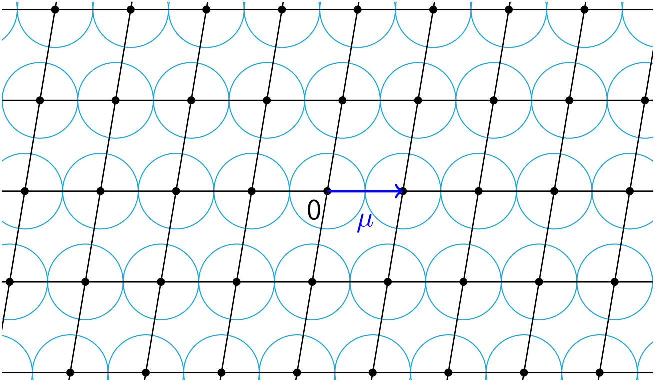
The lattice sphere packing problem

The lattice sphere packing problem consists in finding the biggest proportion of space that can be filled by a collection of disjoint spheres having the same radius, with centers at the points of a lattice Λ.



The lattice sphere packing problem

For a given lattice Λ, the best sphere packing associated is given by balls of radius $\mu/2$, where $\mu = \min\{||\lambda||, \lambda \in \Lambda \setminus \{0\}\}$.

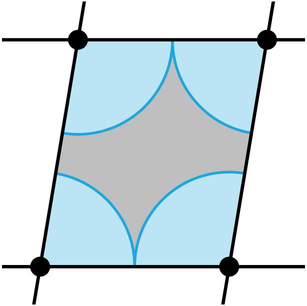


The lattice sphere packing problem

CPU
Numerical certification
& reliability
université de BORDEAUX

The density of this packing is

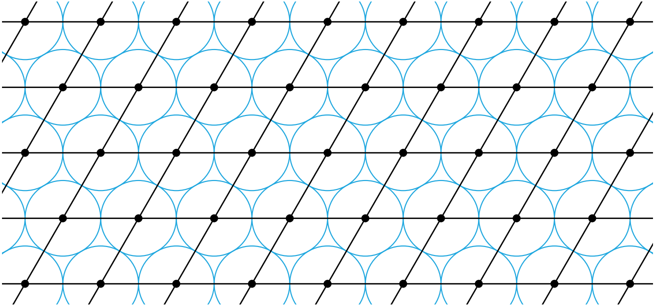
$$\Delta(\Lambda) = \frac{Vol(B(\mu))}{2^n Vol(\Lambda)}$$



Solutions in low dimensions

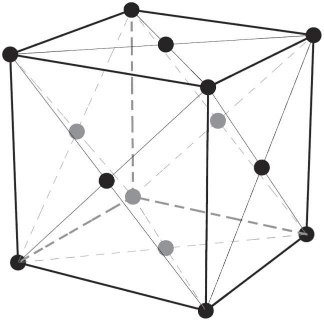
For $n = 1$, the problem is trivial: the best density is 1 !

For $n = 2$, the best packing density is $\frac{\pi\sqrt{3}}{6} \approx 0.9069$, and is given by the hexagonal lattice (Lagrange, 1773, best lattice, Thue, 1892 and Fejes Tóth, 1940, best packing).



Solutions in low dimensions

For $n = 3$, it is the faced-centered cubic lattice which provides the best density $\frac{\pi\sqrt{2}}{6} \approx 0.74048$ (Kepler conjecture, 1611, Gauss, 1832, best lattice, and Hales, 1998, 2014, best packing).



And then ?

And then ?

CPU
Numerical certification & reliability
université de BORDEAUX

- Up to $n = 8$ (Korkine and Zolotaref, Blichfeldt) and for $n = 24$ (Cohn and Kumar), the best lattice packing problem is solved, but it is not known whether it provides the best packing...

And then ?

CPU
Numerical certification & reliability
université de BORDEAUX

- Up to $n = 8$ (Korkine and Zolotaref, Blichfeldt) and for $n = 24$ (Cohn and Kumar), the best lattice packing problem is solved, but it is not known whether it provides the best packing...Not true anymore !

And then ?

CPU Numerical certification & reliability
université de BORDEAUX

- Up to $n = 8$ (Korkine and Zolotaref, Blichfeldt) and for $n = 24$ (Cohn and Kumar), the best lattice packing problem is solved, but it is not known whether it provides the best packing...Not true anymore !
- M. Viazovska just proved that the best lattice packings in dimensions 8 and 24 are optimal.

And then ?

CPU
Numerical certification & reliability
université de BORDEAUX

- Up to $n = 8$ (Korkine and Zolotaref, Blichfeldt) and for $n = 24$ (Cohn and Kumar), the best lattice packing problem is solved, but it is not known whether it provides the best packing...Not true anymore !
- M. Viazovska just proved that the best lattice packings in dimensions 8 and 24 are optimal.
- For other dimensions, the problem is open.

And then ?

- Up to $n = 8$ (Korkine and Zolotaref, Blichfeldt) and for $n = 24$ (Cohn and Kumar), the best lattice packing problem is solved, but it is not known whether it provides the best packing...Not true anymore !
- M. Viazovska just proved that the best lattice packings in dimensions 8 and 24 are optimal.
- For other dimensions, the problem is open.
- Here we are interested in lower bounds for the best packing density Δ_n in dimension n when n goes to infinity.

Summary of results

- Minkowski-Hlawka theorem (stated by Minkowski in 1911, proved by Hlawka in 1943),

$$\Delta_n \geq \frac{2}{2^n}.$$

Summary of results

CPU Numerical certification & reliability
université de BORDEAUX

- Minkowski-Hlawka theorem (stated by Minkowski in 1911, proved by Hlawka in 1943),

$$\Delta_n \geq \frac{2}{2^n}.$$

- Improvement by a linear factor: $\Delta_n \geq \frac{0.73n}{2^n}$ (Rogers,1947).

Summary of results

- Minkowski-Hlawka theorem (stated by Minkowski in 1911, proved by Hlawka in 1943),

$$\Delta_n \geq \frac{2}{2^n}.$$

- Improvement by a linear factor: $\Delta_n \geq \frac{0.73n}{2^n}$ (Rogers,1947).
- Improvements on the constant: $\Delta_n \geq \frac{2n}{2^n}$ (Ball,1992), $\Delta_n \geq \frac{2.2n}{2^n}$ for n divisible by 4 (Vance,2011).

Summary of results

CPU Numerical certification & reliability
université de BORDEAUX

- Minkowski-Hlawka theorem (stated by Minkowski in 1911, proved by Hlawka in 1943),

$$\Delta_n \geq \frac{2}{2^n}.$$

- Improvement by a linear factor: $\Delta_n \geq \frac{0.73n}{2^n}$ (Rogers,1947).
- Improvements on the constant: $\Delta_n \geq \frac{2n}{2^n}$ (Ball,1992), $\Delta_n \geq \frac{2.2n}{2^n}$ for n divisible by 4 (Vance,2011).
- Venkatesh (2013): for all n big enough $\Delta_n \geq \frac{65963n}{2^n}$, and for infinitely many dimensions, $\Delta_n \geq \frac{0.89n \log\log n}{2^n}$.

Some effective results?

CPU
Numerical certification
& reliability
université de BORDEAUX

- An interesting question is to find some effective results about this problem...

Some effective results?

- An interesting question is to find some effective results about this problem...
- ...that is to exhibit finite families of lattices containing a lattice having high density.

Some effective results?

- An interesting question is to find some effective results about this problem...
- ...that is to exhibit finite families of lattices containing a lattice having high density.
- The best one can do is to find exponential-sized families:

Some effective results?

- An interesting question is to find some effective results about this problem...
- ...that is to exhibit finite families of lattices containing a lattice having high density.
- The best one can do is to find exponential-sized families:
- Rush (1989) gave an "effective" proof of Minkowski-Hlawka theorem, with a family having a size of order $\exp(kn \log n)$.

Some effective results?

- An interesting question is to find some effective results about this problem...
- ...that is to exhibit finite families of lattices containing a lattice having high density.
- The best one can do is to find exponential-sized families:
- Rush (1989) gave an "effective" proof of Minkowski-Hlawka theorem, with a family having a size of order $\exp(kn \log n)$.
- Gaborit and Zémor (2006) gave a construction that provides lattices with density higher than $\frac{0.06n}{2^n}$, with a complexity of enumeration of order $\exp(11n \log n)$.

Our result

CPU
Numerical certification & reliability
université de BORDEAUX

We prove an effective version of Venkatesh's theorem:

Theorem

For infinitely many dimension n, one can find a lattice $\Lambda \subset \mathbb{R}^n$ satisfying

$$\Delta(\Lambda) > \frac{0.89 n \log\log n}{2^n}$$

with $\mathcal{O}(\exp(7.8 n \log n))$ binary operations.

A proof of Minkowski-Hlawka theorem

- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.

A proof of Minkowski-Hlawka theorem

CPU Numerical certification & reliability université de BORDEAUX

- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.
  If $|B(r) \cap \Lambda \setminus \{0\}| < 1$, then $\mu(\Lambda) \geq r$,

A proof of Minkowski-Hlawka theorem

CPU
Numerical certification & reliability
université de BORDEAUX

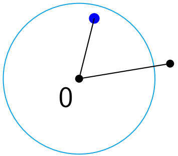
- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.
  If $|B(r) \cap \Lambda \setminus \{0\}| < 1$, then $\mu(\Lambda) \geq r$, thus
  $$\Delta(\Lambda) \geq \frac{Vol(B(r))}{2^n Vol(\Lambda)}.$$

A proof of Minkowski-Hlawka theorem

- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.
  If $|B(r) \cap \Lambda \setminus \{0\}| < 1$, then $\mu(\Lambda) \geq r$, thus
  $$\Delta(\Lambda) \geq \frac{Vol(B(r))}{2^n Vol(\Lambda)}.$$
- Since Λ is a lattice, if v is in $B(r) \cap \Lambda \setminus \{0\}$,

A proof of Minkowski-Hlawka theorem

- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.
  If $|B(r) \cap \Lambda \setminus \{0\}| < 1$, then $\mu(\Lambda) \geq r$, thus
  $$\Delta(\Lambda) \geq \frac{Vol(B(r))}{2^n Vol(\Lambda)}.$$
- Since Λ is a lattice, if v is in $B(r) \cap \Lambda \setminus \{0\}$,



A proof of Minkowski-Hlawka theorem

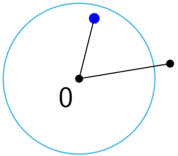
- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.
  If $|B(r) \cap \Lambda \setminus \{0\}| < 1$, then $\mu(\Lambda) \geq r$, thus
  $$\Delta(\Lambda) \geq \frac{Vol(B(r))}{2^n Vol(\Lambda)}.$$
- Since Λ is a lattice, if v is in $B(r) \cap \Lambda \setminus \{0\}$,

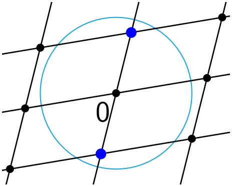
then so does $-v$!

A proof of Minkowski-Hlawka theorem

- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.
  If $|B(r) \cap \Lambda \setminus \{0\}| < 1$, then $\mu(\Lambda) \geq r$, thus
  $$\Delta(\Lambda) \geq \frac{Vol(B(r))}{2^n Vol(\Lambda)}.$$

- Since Λ is a lattice, if v is in $B(r) \cap \Lambda \setminus \{0\}$,





then so does $-v$!

- So the condition $|B(r) \cap \Lambda \setminus \{0\}| < 2$ is sufficient to conclude $\Delta(\Lambda) \geq \frac{Vol(B(r))}{2^n Vol(\Lambda)}$.

A proof of Minkowski-Hlawka theorem

A proof of Minkowski-Hlawka theorem

- Siegel's mean value theorem: Let $\mathcal{L}$ be the set of lattices in $\mathbb{R}^n$ with volume 1.

A proof of Minkowski-Hlawka theorem

- Siegel's mean value theorem: Let $\mathcal{L}$ be the set of lattices in $\mathbb{R}^n$ with volume 1. For $r > 0$,

$$\mathbb{E}_{\mathcal{L}}[|B(r) \cap \Lambda \setminus \{0\}|] = Vol(B(r))$$

A proof of Minkowski-Hlawka theorem

CPU
Numerical certification & reliability
université de BORDEAUX

- Siegel's mean value theorem: Let $\mathcal{L}$ be the set of lattices in $\mathbb{R}^n$ with volume 1. For $r > 0$,

$$\mathbb{E}_{\mathcal{L}}[|B(r) \cap \Lambda \setminus \{0\}|] = Vol(B(r))$$

- So, when $Vol(B(r)) < 2$, there is a lattice Λ such that $\Delta(\Lambda) \geq \frac{Vol(B(r))}{2^n}$. In other words:

A proof of Minkowski-Hlawka theorem

- Siegel's mean value theorem: Let $\mathcal{L}$ be the set of lattices in $\mathbb{R}^n$ with volume 1. For $r > 0$,

$$\mathbb{E}_{\mathcal{L}}[|B(r) \cap \Lambda \setminus \{0\}|] = Vol(B(r))$$

- So, when $Vol(B(r)) < 2$, there is a lattice Λ such that $\Delta(\Lambda) \geq \frac{Vol(B(r))}{2^n}$. In other words:

$$\Delta_n \geq \frac{2}{2^n}$$

How can symmetries be useful?

How can symmetries be useful?

- Idea: If we consider lattices with more symmetries, we can replace the 2-factor in the previous argument by a bigger value, and get a better bound.

How can symmetries be useful?

CPU Numerical certification & reliability université de BORDEAUX

- Idea: If we consider lattices with more symmetries, we can replace the 2-factor in the previous argument by a bigger value, and get a better bound.
- For $n = 2\ell$ with ℓ prime, Gaborit and Zémor considered finite families of lattices invariant under the action of $\mathbb{Z}/\ell\mathbb{Z}$ via (doubly)-cyclic permutation of coordinates.

How can symmetries be useful?

- Idea: If we consider lattices with more symmetries, we can replace the 2-factor in the previous argument by a bigger value, and get a better bound.
- For $n = 2\ell$ with ℓ prime, Gaborit and Zémor considered finite families of lattices invariant under the action of $\mathbb{Z}/\ell\mathbb{Z}$ via (doubly)-cyclic permutation of coordinates.
- For $n = 2\phi(m)$, Venkatesh constructed infinite families of lattices invariant under the action of mth-roots of unity. Taking $m = \prod_{\substack{q \in \mathbb{P} \\ q \leq X}} q$, he optimized the ratio between m and $2\phi(m)$.

Our construction

Our construction

- $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$

Our construction

CPU Numerical certification & reliability
université de BORDEAUX

- $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$
- $\mathfrak{P}$ prime ideal of $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, $F = \mathcal{O}_K/\mathfrak{P} \simeq \mathbb{F}_q$.

Our construction

- $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$
- $\mathfrak{P}$ prime ideal of $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, $F = \mathcal{O}_K / \mathfrak{P} \simeq \mathbb{F}_q$.
- $V = K_\mathbb{R}^2$, $\Lambda_0 = \mathcal{O}_K^2$ and

$$\pi : \Lambda_0 \to \Lambda_0 / \mathfrak{P}\Lambda_0 \simeq F^2$$

Our construction

CPU Numerical certification & reliability
université de BORDEAUX

- $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$
- $\mathfrak{P}$ prime ideal of $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, $F = \mathcal{O}_K/\mathfrak{P} \simeq \mathbb{F}_q$.
- $V = K_{\mathbb{R}}^2$, $\Lambda_0 = \mathcal{O}_K^2$ and

$$\pi : \Lambda_0 \to \Lambda_0/\mathfrak{P}\Lambda_0 \simeq F^2$$

Definition

Let $\mathcal{C}$ be the set of the $q+1$ F-lines of $\Lambda_0/\mathfrak{P}\Lambda_0 = F^2$, and $\mathcal{L}_{\mathcal{C}}$ the associated set of lattices of V: $\mathcal{L}_{\mathcal{C}} = \{\pi^{-1}(C), C \in \mathcal{C}\}$.

Our construction

- $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$
- $\mathfrak{P}$ prime ideal of $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, $F = \mathcal{O}_K/\mathfrak{P} \simeq \mathbb{F}_q$.
- $V = K_{\mathbb{R}}^2$, $\Lambda_0 = \mathcal{O}_K^2$ and

$$\pi : \Lambda_0 \to \Lambda_0/\mathfrak{P}\Lambda_0 \simeq F^2$$

Definition

Let $\mathcal{C}$ be the set of the $q+1$ F-lines of $\Lambda_0/\mathfrak{P}\Lambda_0 = F^2$, and $\mathcal{L}_{\mathcal{C}}$ the associated set of lattices of V: $\mathcal{L}_{\mathcal{C}} = \{\pi^{-1}(C), C \in \mathcal{C}\}$.

- Every lattice in $\mathcal{L}_{\mathcal{C}}$ has volume $qVol(\Lambda_0)$ and is invariant under the action of mth-roots of unity.

Our construction

CPU Numerical certification & reliability
université de BORDEAUX

- $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$
- $\mathfrak{P}$ prime ideal of $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, $F = \mathcal{O}_K / \mathfrak{P} \simeq \mathbb{F}_q$.
- $V = K_{\mathbb{R}}^2$, $\Lambda_0 = \mathcal{O}_K^2$ and

$$\pi : \Lambda_0 \to \Lambda_0 / \mathfrak{P}\Lambda_0 \simeq F^2$$

Definition

Let $\mathcal{C}$ be the set of the $q+1$ F-lines of $\Lambda_0 / \mathfrak{P}\Lambda_0 = F^2$, and $\mathcal{L}_{\mathcal{C}}$ the associated set of lattices of V: $\mathcal{L}_{\mathcal{C}} = \{\pi^{-1}(C), C \in \mathcal{C}\}$.

- Every lattice in $\mathcal{L}_{\mathcal{C}}$ has volume $qVol(\Lambda_0)$ and is invariant under the action of mth-roots of unity.
- The family satisfies, for r and q chosen in a suitable way:

Our construction

- $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$
- $\mathfrak{P}$ prime ideal of $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, $F = \mathcal{O}_K/\mathfrak{P} \simeq \mathbb{F}_q$.
- $V = K_{\mathbb{R}}^2$, $\Lambda_0 = \mathcal{O}_K^2$ and

$$\pi : \Lambda_0 \to \Lambda_0/\mathfrak{P}\Lambda_0 \simeq F^2$$

Definition

Let $\mathcal{C}$ be the set of the $q+1$ F-lines of $\Lambda_0/\mathfrak{P}\Lambda_0 = F^2$, and $\mathcal{L}_{\mathcal{C}}$ the associated set of lattices of V: $\mathcal{L}_{\mathcal{C}} = \{\pi^{-1}(C), C \in \mathcal{C}\}$.

- Every lattice in $\mathcal{L}_{\mathcal{C}}$ has volume $qVol(\Lambda_0)$ and is invariant under the action of mth-roots of unity.
- The family satisfies, for r and q chosen in a suitable way:

$$\mathbb{E}_{\mathcal{L}_{\mathcal{C}}}[|B(r) \cap \Lambda \setminus \{0\}|] \simeq \frac{Vol(B(r))}{qVol(\Lambda_0)}$$

Results

Results

CPU Numerical certification & reliability

université de BORDEAUX

Theorem

For every $1 > \varepsilon > 0$, if $\phi(m)^2 m = o(q_m^{\frac{1}{\phi(m)}})$, then for m big enough, the family of lattices $\mathcal{L}_{\mathcal{C}}$ contains a lattice $\Lambda \subset \mathbb{R}^{2\phi(m)}$ satisfying

$$\Delta(\Lambda) > \frac{(1-\varepsilon)m}{2^{2\phi(m)}}.$$

Results

Theorem

For every $1 > \varepsilon > 0$, if $\phi(m)^2 m = o(q_m^{\frac{1}{\phi(m)}})$, then for m big enough, the family of lattices $\mathcal{L}_{\mathcal{C}}$ contains a lattice $\Lambda \subset \mathbb{R}^{2\phi(m)}$ satisfying

$$\Delta(\Lambda) > \frac{(1-\varepsilon)m}{2^{2\phi(m)}}.$$

- This result is a generalization of Gaborit-Zémor's result: it is valid for a "larger" set of dimensions.

Results

Theorem

For every $1 > \varepsilon > 0$, if $\phi(m)^2 m = o(q_m{}^{\frac{1}{\phi(m)}})$, then for m big enough, the family of lattices $\mathcal{L}_{\mathcal{C}}$ contains a lattice $\Lambda \subset \mathbb{R}^{2\phi(m)}$ satisfying

$$\Delta(\Lambda) > \frac{(1-\varepsilon)m}{2^{2\phi(m)}}.$$

- This result is a generalization of Gaborit-Zémor's result: it is valid for a "larger" set of dimensions.
- The action we consider is free: so we have no loss in the constant (1/2 instead of 0.06).

Results

Results

CPU Numerical certification & reliability
université de BORDEAUX

- For the particular set of dimensions considered by Venkatesh, we obtain the same density...

Corollary

For infinitely many dimensions, $\mathcal{L}_{\mathcal{C}}$ contains a lattice $\Lambda \subset \mathbb{R}^n$ satisfying $\Delta(\Lambda) \geq \frac{0.89 n \log \log n}{2^n}$.

Results

CPU
Numerical certification & reliability
université de BORDEAUX

- For the particular set of dimensions considered by Venkatesh, we obtain the same density...

Corollary

For infinitely many dimensions, $\mathcal{L}_{\mathcal{C}}$ contains a lattice $\Lambda \subset \mathbb{R}^n$ satisfying $\Delta(\Lambda) \geq \frac{0.89 n \log\log n}{2^n}$.

- ... with finite families of lattices !

Complexity of construction

Let $n = 2\phi(m)$. For every $1 > \varepsilon > 0$, the construction of a lattice $\Lambda \subset \mathbb{R}^n$ satisfying $\Delta(\Lambda) > \frac{(1-\varepsilon)m}{2^{2\phi(m)}}$ requires $\mathcal{O}(\exp(7.8 n \log n))$ binary operations.

Concluding comments and perspectives

- The construction can be adapted in such a way that the lattices of $\mathcal{L}_{\mathcal{C}}$ are symplectic.

Concluding comments and perspectives

CPU Numerical certification & reliability

université de BORDEAUX

- The construction can be adapted in such a way that the lattices of $\mathcal{L}_{\mathcal{C}}$ are symplectic.
- Are these families of lattices good with respect to other properties ?

Concluding comments and perspectives

- The construction can be adapted in such a way that the lattices of $\mathcal{L}_{\mathcal{C}}$ are symplectic.
- Are these families of lattices good with respect to other properties ?
- Could we do the same kind of constructions with different groups ?

Concluding comments and perspectives

- The construction can be adapted in such a way that the lattices of $\mathcal{L}_{\mathcal{C}}$ are symplectic.
- Are these families of lattices good with respect to other properties ?
- Could we do the same kind of constructions with different groups ?

Thank you for your attention