Lattices, codes, and sphere packings

Philippe Moustrou, UiT The Arctic University of Norway

$\mathbb{N}^3$ days XIII - November 27, 2020

Contents

Lattices, codes, and sphere packings

Contents

Lattices, codes, and sphere packings

- Global sphere packings in $\mathbb{R}^n$:
  - An overview of the problem: sphere packings vs lattice sphere packings
  - How to construct dense lattices in high dimension from codes?

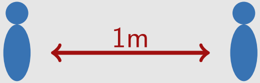
Contents

Lattices, codes, and sphere packings

- Global sphere packings in $\mathbb{R}^n$:
    - An overview of the problem: sphere packings vs lattice sphere packings
    - How to construct dense lattices in high dimension from codes?
- Local sphere packings
    - Various problems: Kissing number, spherical codes...
    - How to show the optimality of some configurations in low dimension?

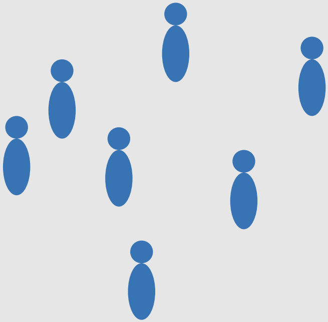
Social distancing and sphere packings

Assume that people should keep one meter distance between themselves...



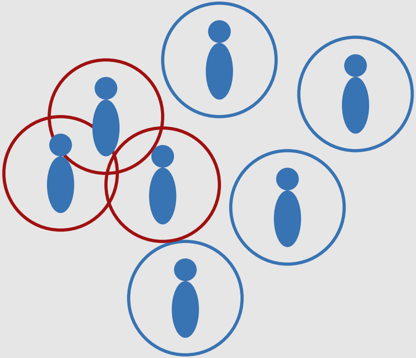
Social distancing and sphere packings

How to deal with a large number of people?



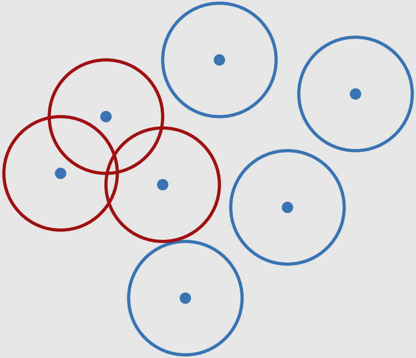
Social distancing and sphere packings

We want non overlapping spheres of radius 0.5m.



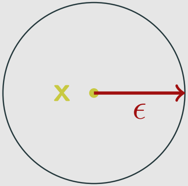
Social distancing and sphere packings

This is the sphere packing problem!



Coding and sphere packings

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 $B(x, \epsilon)$:

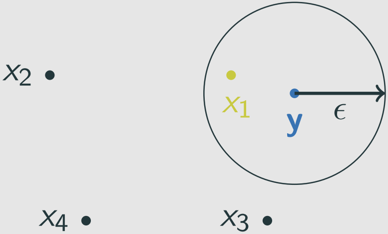


Coding and sphere packings

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

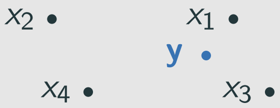
Coding and sphere packings

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



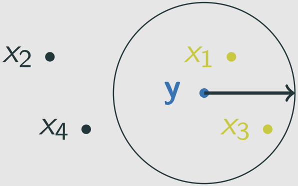
Coding and sphere packings

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



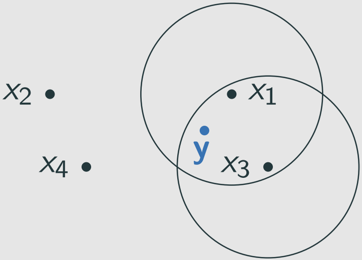
Coding and sphere packings

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



Coding and sphere packings

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



Sphere packings

- 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.

Sphere packings

- 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 again the sphere packing problem!

Sphere packings

- 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 again the sphere packing problem!
- This problem is old, and known to be hard.

Sphere packings

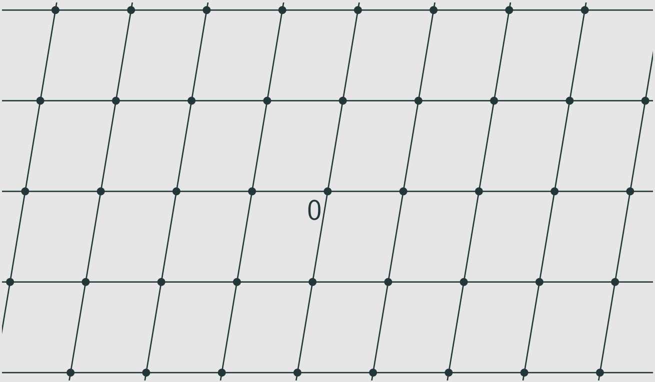
- Finding a good code with respect to this property boils down to finding an arrangement of disjoint spheres having the same radius for which the proportion of space filled is the highest possible.
- This is again the sphere packing problem!
- This problem is old, and known to be hard.
- What if we impose some algebraic structure to the packings, like for linear codes?

Sphere packings

- 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 again the sphere packing problem!
- This problem is old, and known to be hard.
- What if we impose some algebraic structure to the packings, like for linear codes?
- Euclidean lattices provide a way to approach this problem.

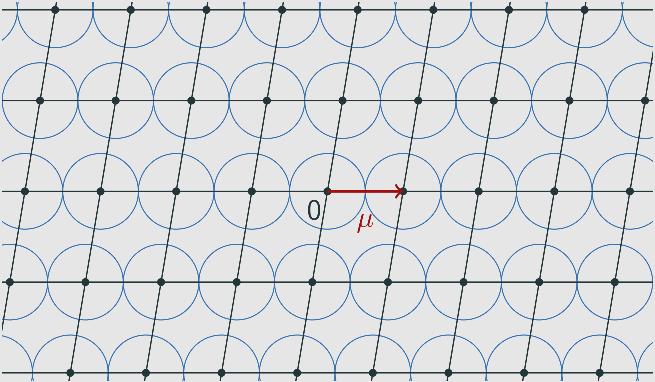
The lattice sphere packing problem

The lattice sphere packing problem consists in finding the biggest proportion of space Δ_n 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

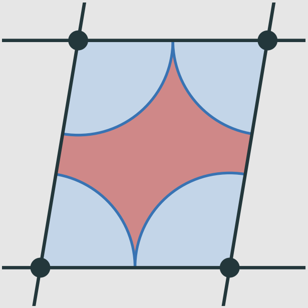
For a given lattice Λ, the best sphere packing associated is given by balls of radius $\mu/2$, where $\mu = \min\{||\lambda||, \lambda \in \Lambda \setminus \{0\}\}$.



The lattice sphere packing problem

The density of this packing is

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



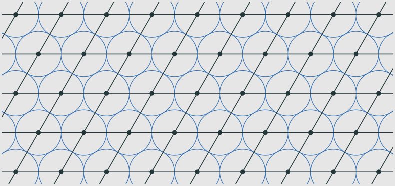
Dimensions 1 and 2

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

Dimensions 1 and 2

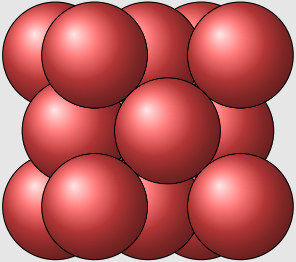
For $n = 1$, the problem is trivial: the best density is 1 !

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).



Dimension 3

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).



Solutions for the lattice sphere packing problem

Then we only know the best lattice packings for dimensions $n \leq 8$ and $n = 24$.

Dimension	Lattice	Proved by
4	D_4	Korkine and Zolotareff, 1877
5	D_5	Korkine and Zolotareff, 1877
6	E_6	Blichfield, 1935
7	E_7	Blichfield, 1935
8	E_8	Blichfield, 1935
24	Λ_{24}	Cohn and Kumar, 2009

Solutions for the lattice sphere packing problem

Then we only know the best lattice packings for dimensions $n \leq 8$ and $n = 24$.

Dimension	Lattice	Proved by
4	D_4	Korkine and Zolotareff, 1877
5	D_5	Korkine and Zolotareff, 1877
6	E_6	Blichfield, 1935
7	E_7	Blichfield, 1935
8	E_8	Blichfield, 1935
24	Λ_{24}	Cohn and Kumar, 2009

In dimensions 8 and 24, E_8 and the Leech lattice provide respectively the unique optimal configurations (Viazovska, 2016).

Solutions for the lattice sphere packing problem

Then we only know the best lattice packings for dimensions $n \leq 8$ and $n = 24$.

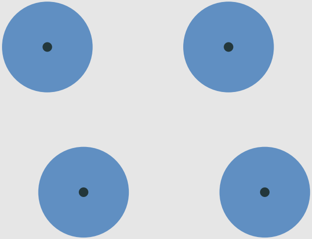
Dimension	Lattice	Proved by
4	D_4	Korkine and Zolotareff, 1877
5	D_5	Korkine and Zolotareff, 1877
6	E_6	Blichfield, 1935
7	E_7	Blichfield, 1935
8	E_8	Blichfield, 1935
24	Λ_{24}	Cohn and Kumar, 2009

In dimensions 8 and 24, E_8 and the Leech lattice provide respectively the unique optimal configurations (Viazovska, 2016).

What about high dimensions?

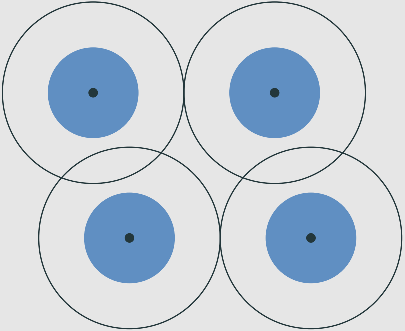
An easy bound for general packings in high dimension

Suppose we have a saturated packing of balls of radius r



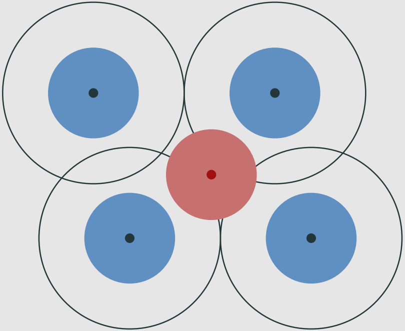
An easy bound for general packings in high dimension

Then, if we double the radius, we cannot have any free point.



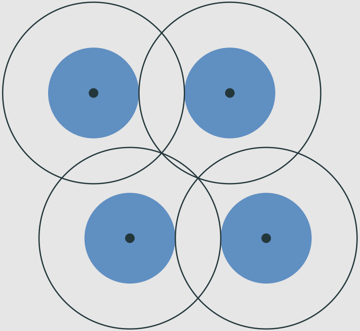
An easy bound for general packings in high dimension

Then, if we double the radius, we cannot have any free point.



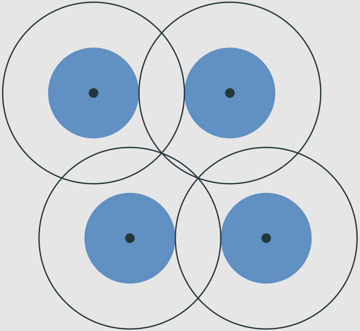
An easy bound for general packings in high dimension

So the balls of radius $2r$ cover the space.



An easy bound for general packings in high dimension

Thus $2^n\Delta \geq 1$, in other words $\Delta \geq \frac{1}{2^n}$.



Lattice packings in higher dimensions

Lattice packings in higher dimensions

Upper bound: $\Delta_n \leq 2^{(-0.5999+o(1))n}$ (Kabatiansky-Levenshtein 1978)

Lattice packings in higher dimensions

Upper bound: $\Delta_n \leq 2^{(-0.5999+o(1))n}$ (Kabatiansky-Levenshtein 1978)

Lower bounds:

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

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

Lattice packings in higher dimensions

Upper bound: $\Delta_n \leq 2^{(-0.5999+o(1))n}$ (Kabatiansky-Levenshtein 1978)

Lower bounds:

- 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).

Lattice packings in higher dimensions

Upper bound: $\Delta_n \leq 2^{(-0.5999+o(1))n}$ (Kabatiansky-Levenshtein 1978)

Lower bounds:

- 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).

Lattice packings in higher dimensions

Upper bound: $\Delta_n \leq 2^{(-0.5999+o(1))n}$ (Kabatiansky-Levenshtein 1978)

Lower bounds:

- 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, $\Delta_n \geq \frac{0.89n\log\log n}{2^n}$.

Lattice packings in higher dimensions

Upper bound: $\Delta_n \leq 2^{(-0.5999+o(1))n}$ (Kabatiansky-Levenshtein 1978)

Lower bounds:

- 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, $\Delta_n \geq \frac{0.89n \log\log n}{2^n}$.

However, these results only provide the existence of good lattices, but are not effective.

Some effective results?

One way to do so is to exhibit finite families of lattices containing a dense lattice.

Some effective results?

One way to do so is to exhibit finite families of lattices containing a dense lattice. The best one can do is to find exponential-sized families:

Some effective results?

One way to do so is to exhibit finite families of lattices containing a dense lattice. 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?

One way to do so is to exhibit finite families of lattices containing a dense lattice. 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 $\exp(11n \log n)$.

Some effective results?

One way to do so is to exhibit finite families of lattices containing a dense lattice. 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 $\exp(11n \log n)$.

Theorem (M., 2017)

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

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

with $\exp(1.5n \log n(1 + o(1)))$ 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

- 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

- 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
  $$\Delta(\Lambda) \geq \frac{\mathrm{Vol}(B(r))}{2^n \mathrm{Vol}(\Lambda)}.$$

A proof of Minkowski-Hlawka theorem

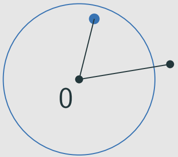
- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.
  If $|B(r) \cap \Lambda \setminus \{0\}| < 1$, then $\mu(\Lambda) \geq r$, thus
  $$\Delta(\Lambda) \geq \frac{\mathrm{Vol}(B(r))}{2^n \,\mathrm{Vol}(\Lambda)}.$$

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

A proof of Minkowski-Hlawka theorem

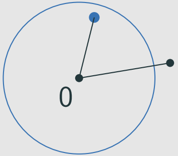
- Basic idea: Let Λ be a lattice in $\mathbb{R}^n$ and $r > 0$.
  If $|B(r) \cap \Lambda \setminus \{0\}| < 1$, then $\mu(\Lambda) \geq r$, thus
  $$\Delta(\Lambda) \geq \frac{\mathrm{Vol}(B(r))}{2^n \mathrm{Vol}(\Lambda)}.$$

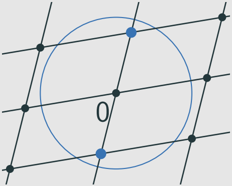
- Since Λ is a lattice, if v is in $B(r) \cap \Lambda \setminus \{0\}$,



- 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
  $$\Delta(\Lambda) \geq \frac{\mathrm{Vol}(B(r))}{2^n \, \mathrm{Vol}(\Lambda)}.$$

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



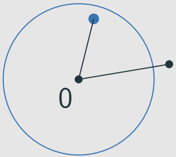


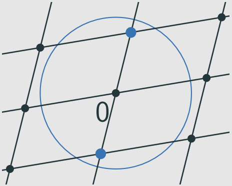
then so does $-v$!

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
  $$\Delta(\Lambda) \geq \frac{\mathrm{Vol}(B(r))}{2^n \mathrm{Vol}(\Lambda)}.$$

- 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 $\Delta(\Lambda) \geq \frac{\mathrm{Vol}(B(r))}{2^n \mathrm{Vol}(\Lambda)}$.

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.

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

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

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 $r > 0$,

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

- So, when $\mathrm{Vol}(B(r)) < 2$, there is a lattice Λ such that $\Delta(\Lambda) \geq \frac{\mathrm{Vol}(B(r))}{2^n}$. 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 $r > 0$,

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

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

- 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.
- Considering lattices having a module structure over the Hurwitz integers, Vance refined Roger's method and got an improvement in the constant in its result.

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.
- Considering lattices having a module structure over the Hurwitz integers, Vance refined Roger's method and got an improvement in the constant in its result.
- 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.
- Considering lattices having a module structure over the Hurwitz integers, Vance refined Roger's method and got an improvement in the constant in its result.
- 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 $2\phi(m)$.

(Nordic) Number theory ~~Network~~ Lattices

- Let $K/\mathbb{Q}$ be a number field of degree n.

(Nordic) Number theory ~~Network~~ Lattices

- Let $K/\mathbb{Q}$ be a number field of degree n.
- Following the real and complex embeddings of $K \to \mathbb{C}$, we can write $n = r_1 + 2r_2$, and there is a natural embedding ι of K into K_R, where $K_R = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n \simeq K \otimes_{\mathbb{Q}} \mathbb{R}$:

$$\begin{array}{cccc} \iota & : & K & \to & K_{\mathbb{R}} \\ & & x & \mapsto & (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)) \end{array}.$$

(Nordic) Number theory ~~Network~~ Lattices

- Let $K/\mathbb{Q}$ be a number field of degree n.
- Following the real and complex embeddings of $K \to \mathbb{C}$, we can write $n = r_1 + 2r_2$, and there is a natural embedding ι of K into K_R, where $K_R = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n \simeq K \otimes_{\mathbb{Q}} \mathbb{R}$:

$$\begin{array}{cccc} \iota & : & K & \to & K_{\mathbb{R}} \\ & & x & \mapsto & (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)) \end{array}.$$

- The map

$$\begin{array}{cccc} \beta & : & K \times K & \to & \mathbb{R} \\ & & (x, y) & \mapsto & \mathrm{tr}(x\bar{y}) \end{array}$$

is a positive-definite symmetric bilinear form, which induces a scalar product $\langle \cdot, \cdot \rangle$ on $K_{\mathbb{R}}$.

(Nordic) Number theory ~~Network~~ Lattices

- Let $K/\mathbb{Q}$ be a number field of degree n.
- Following the real and complex embeddings of $K \to \mathbb{C}$, we can write $n = r_1 + 2r_2$, and there is a natural embedding ι of K into K_R, where $K_R = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n \simeq K \otimes_{\mathbb{Q}} \mathbb{R}$:

$$\begin{array}{cccc} \iota & : & K & \to & K_{\mathbb{R}} \\ & & x & \mapsto & (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)) \end{array}.$$

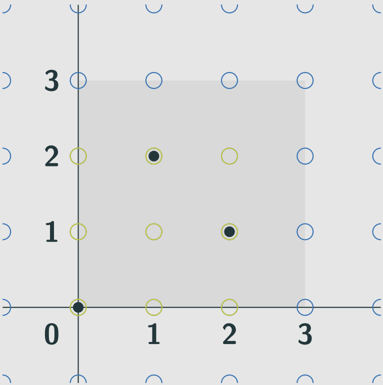
- The map

$$\begin{array}{ccccc} \beta & : & K \times K & \to & \mathbb{R} \\ & & (x, y) & \mapsto & \mathrm{tr}(x\bar{y}) \end{array}$$

  is a positive-definite symmetric bilinear form, which induces a scalar product $\langle \cdot, \cdot \rangle$ on $K_{\mathbb{R}}$.
- The ring of integers $\mathcal{O}_K$, and more generally every fractional ideal $\mathfrak{A}$ of K are free $\mathbb{Z}$-modules of rank n, and thus define lattices in $K_{\mathbb{R}}$.

Lattices from codes: Construction A

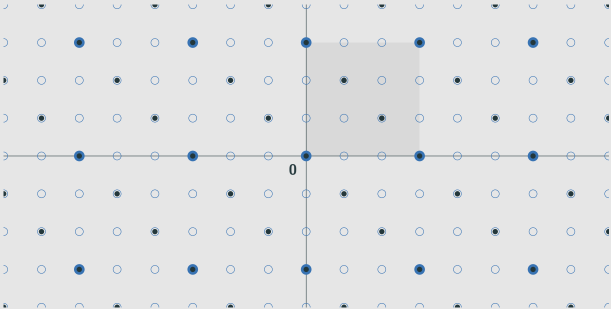
Let p be a prime number, $\pi : \mathbb{Z}^n \to \mathbb{F}_p^n$ the canonical projection, and $C \subset \mathbb{F}_p^n$ a k-dimensional code.



Lattices from codes: Construction A

We define $\Lambda_C = \pi^{-1}(C)$. Then we have $p\mathbb{Z}^n \subset \Lambda_C \subset \mathbb{Z}^n$ and

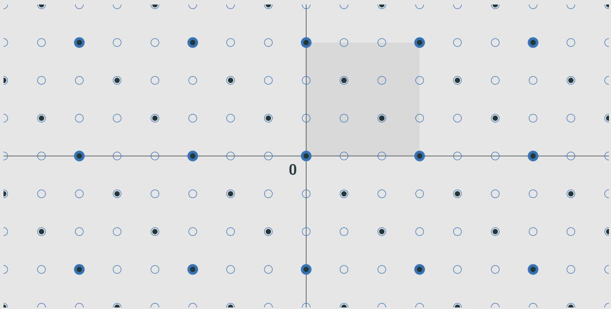
$$Vol(\Lambda_C) = p^{n-k}$$



Lattices from codes: Construction A

We define $\Lambda_C = \pi^{-1}(C)$. Then we have $p\mathbb{Z}^n \subset \Lambda_C \subset \mathbb{Z}^n$ and

$$Vol(\Lambda_C) = p^{n-k}$$



Examples: The famous lattices E_8 and the Leech Lattice Λ_{24} can be obtained via this construction.

Outline of the proof

Theorem (M., 2017)

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 $\exp(1.5 n \log n(1 + o(1)))$ binary operations.

Outline of the proof

Theorem (M., 2017)

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 $\exp(1.5 n \log n (1 + o(1)))$ binary operations.

- Let $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$, $\Lambda_0 = \mathcal{O}_K^2 \subset K_{\mathbb{R}}^2$.

Outline of the proof

Theorem (M., 2017)

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 $\exp(1.5 n \log n (1 + o(1)))$ binary operations.

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

Outline of the proof

Theorem (M., 2017)

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 $\exp(1.5 n \log n(1 + o(1)))$ binary operations.

- Let $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$, $\Lambda_0 = \mathcal{O}_K^2 \subset K_{\mathbb{R}}^2$.
- $\mathfrak{P} \subset \mathcal{O}_K$ prime ideal, $F = \mathcal{O}_K/\mathfrak{P} \simeq \mathbb{F}_q$.
- Adapt Construction A to $\pi : \Lambda_0 \to \Lambda_0/\mathfrak{P}\Lambda_0 \simeq F^2$.

Outline of the proof

Theorem (M., 2017)

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 $\exp(1.5 n \log n (1 + o(1)))$ binary operations.

- Let $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$, $\Lambda_0 = \mathcal{O}_K^2 \subset K_{\mathbb{R}}^2$.
- $\mathfrak{P} \subset \mathcal{O}_K$ prime ideal, $F = \mathcal{O}_K / \mathfrak{P} \simeq \mathbb{F}_q$.
- Adapt Construction A to $\pi : \Lambda_0 \to \Lambda_0 / \mathfrak{P}\Lambda_0 \simeq F^2$.
- Take $\mathcal{L}$ the family of lattices obtained from all the $q+1$ F-lines in F^2.

Outline of the proof

Theorem (M., 2017)

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

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

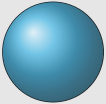
with $\exp(1.5 n \log n(1 + o(1)))$ binary operations.

- Let $K = \mathbb{Q}[\zeta_m] \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\phi(m)}$, $\Lambda_0 = \mathcal{O}_K^2 \subset K_{\mathbb{R}}^2$.
- $\mathfrak{P} \subset \mathcal{O}_K$ prime ideal, $F = \mathcal{O}_K / \mathfrak{P} \simeq \mathbb{F}_q$.
- Adapt Construction A to $\pi : \Lambda_0 \to \Lambda_0 / \mathfrak{P}\Lambda_0 \simeq F^2$.
- Take $\mathcal{L}$ the family of lattices obtained from all the $q + 1$ F-lines in F^2.
- If q is large enough, one gets an analogue of Siegel's mean value theorem.

The kissing number problem

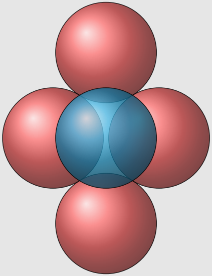
The kissing number problem

How many unit spheres can simultaneously touch a central unit sphere without overlapping?



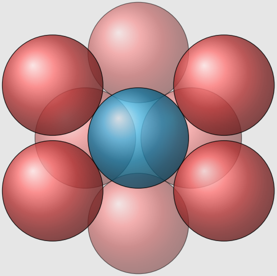
The kissing number problem

How many unit spheres can simultaneously touch a central unit sphere without overlapping?



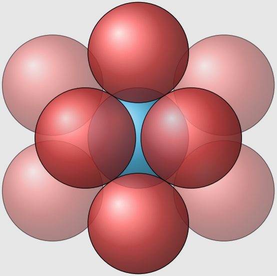
The kissing number problem

How many unit spheres can simultaneously touch a central unit sphere without overlapping?



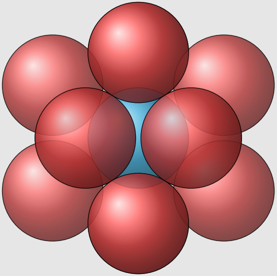
The kissing number problem

How many unit spheres can simultaneously touch a central unit sphere without overlapping?



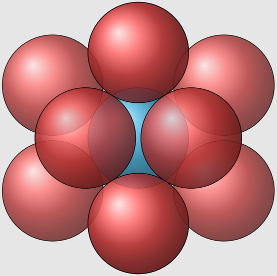
The kissing number problem

How many unit spheres can simultaneously touch a central unit sphere without overlapping?



The kissing number problem

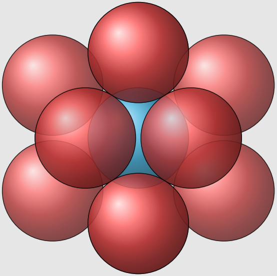
How many unit spheres can simultaneously touch a central unit sphere without overlapping?



Known for $n \in \{1, 2, 3, 4, 8, 24\}$.

The kissing number problem

How many unit spheres can simultaneously touch a central unit sphere without overlapping?



Known for $n \in \{1, 2, 3, 4, 8, 24\}$.

The lattice kissing number problem: what is the maximal number of shortest vectors achieved by a lattice?

Exponential growth

Let τ_n be the kissing number in dimension n. It is known, from various approaches (Chabauty 1953, Shannon 1959, Wyner 1965) that

$$\frac{\log_2 \tau_n}{n} \geq \log_2 \frac{2}{\sqrt{3}} \simeq 0.2075...$$

Exponential growth

Let τ_n be the kissing number in dimension n. It is known, from various approaches (Chabauty 1953, Shannon 1959, Wyner 1965) that

$$\frac{\log_2 \tau_n}{n} \geq \log_2 \frac{2}{\sqrt{3}} \simeq 0.2075...$$

What about the lattice kissing number τ_n^ℓ?

Exponential growth

Let τ_n be the kissing number in dimension n. It is known, from various approaches (Chabauty 1953, Shannon 1959, Wyner 1965) that

$$\frac{\log_2 \tau_n}{n} \geq \log_2 \frac{2}{\sqrt{3}} \simeq 0.2075...$$

What about the lattice kissing number τ_n^ℓ?

Recently (2019), Vlăduț showed that there exist lattices with exponentially large kissing numbers.

Exponential growth

Let τ_n be the kissing number in dimension n. It is known, from various approaches (Chabauty 1953, Shannon 1959, Wyner 1965) that

$$\frac{\log_2 \tau_n}{n} \geq \log_2 \frac{2}{\sqrt{3}} \simeq 0.2075...$$

What about the lattice kissing number τ_n^ℓ?

Recently (2019), Vlăduț showed that there exist lattices with exponentially large kissing numbers.

These lattices are constructed...

Exponential growth

Let τ_n be the kissing number in dimension n. It is known, from various approaches (Chabauty 1953, Shannon 1959, Wyner 1965) that

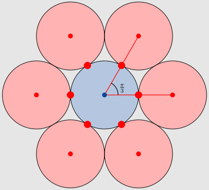
$$\frac{\log_2 \tau_n}{n} \geq \log_2 \frac{2}{\sqrt{3}} \simeq 0.2075...$$

What about the lattice kissing number τ_n^ℓ?

Recently (2019), Vlăduț showed that there exist lattices with exponentially large kissing numbers.

These lattices are constructed...

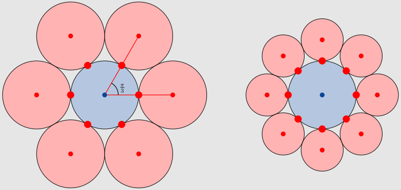
From codes! They come from algebraic geometric codes with exponentially many minimal codewords.



Kissing number:

$$\max\{|C|, \quad C \subset S^{n-1}, \quad x \cdot y \leq 1/2 \text{ for all } x \neq y \in C\}$$

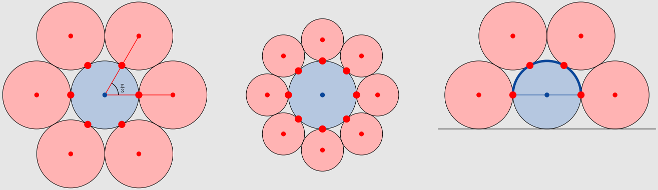
Formulation and generalizations



Spherical codes:

$$\max\{|C|, \quad C \subset S^{n-1}, \quad x \cdot y \leq \cos\theta \text{ for all } x \neq y \in C\}$$

Formulation and generalizations



Kissing number of the hemisphere:

$$\max\{|C|, \quad C \subset \mathrm{H}^{n-1}, \quad x \cdot y \leq 1/2 \text{ for all } x \neq y \in C\}$$

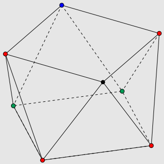
Goal and results

We are interested in special rigid structures, like:

Goal and results

We are interested in special rigid structures, like:

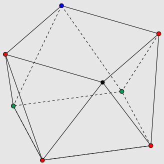
- The square antiprism, the unique optimal θ-spherical code in dimension 3 with $\cos\theta = (2\sqrt{2}-1)/7$ (Schütte-van der Waerden 1951, Danzer 1986).



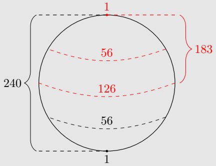
Goal and results

We are interested in special rigid structures, like:

- The square antiprism, the unique optimal θ-spherical code in dimension 3 with $\cos\theta = (2\sqrt{2}-1)/7$ (Schütte-van der Waerden 1951, Danzer 1986).



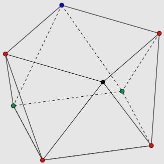
- For the Hemisphere in dimension 8: the E_8 lattice provides an optimal configuration (Bachoc-Vallentin, 2008). What about uniqueness?



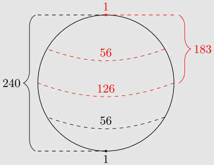
Goal and results

We are interested in special rigid structures, like:

- The square antiprism, the unique optimal θ-spherical code in dimension 3 with $\cos\theta = (2\sqrt{2}-1)/7$ (Schütte-van der Waerden 1951, Danzer 1986).



- For the Hemisphere in dimension 8: the E_8 lattice provides an optimal configuration (Bachoc-Vallentin, 2008). What about uniqueness?



- [Dostert, De Laat, M., 2020]: A general framework to prove optimality and uniqueness of such configurations.

Techniques in low dimensions

Techniques in low dimensions

- Lower bounds:

  Algebraic constructions, very often structures with many symmetries.

Techniques in low dimensions

- Lower bounds:

  Algebraic constructions, very often structures with many symmetries.

- Upper bounds:

Techniques in low dimensions

- Lower bounds:

  Algebraic constructions, very often structures with many symmetries.

- Upper bounds:
  - 2-point bound (Delsarte-Goethals-Seidel 1977)

    $\rightarrow$ linear programming bound

Techniques in low dimensions

- Lower bounds:

  Algebraic constructions, very often structures with many symmetries.

- Upper bounds:
  - 2-point bound (Delsarte-Goethals-Seidel 1977)
    $\rightarrow$ linear programming bound
  - 3-point bound (Bachoc-Vallentin 2008)
    $\rightarrow$ semidefinite programming bound

Techniques in low dimensions

- Lower bounds:

  Algebraic constructions, very often structures with many symmetries.

- Upper bounds:
  - 2-point bound (Delsarte-Goethals-Seidel 1977)
    $\rightarrow$ linear programming bound
  - 3-point bound (Bachoc-Vallentin 2008)
    $\rightarrow$ semidefinite programming bound

  These bounds are related to the hierarchies of semidefinite upper bounds used to give upper bounds on the independence number of finite graphs. (Lovász-Schrijver 1991, Lasserre 2001, Laurent 2007)

Solving an SDP: Rage against the machine precision

Solving an SDP: Rage against the machine precision

- Assume we know a configuration C with $|C| = N$. Any upper bound $< N + 1$ is enough to prove that C is optimal.

Solving an SDP: Rage against the machine precision

- Assume we know a configuration C with $|C| = N$. Any upper bound $< N + 1$ is enough to prove that C is optimal.
- However, sharp bounds provide additional information on optimal configurations, leading to uniqueness proofs.

Solving an SDP: Rage against the machine precision

- Assume we know a configuration C with $|C| = N$. Any upper bound $< N + 1$ is enough to prove that C is optimal.
- However, sharp bounds provide additional information on optimal configurations, leading to uniqueness proofs.
- There are many examples of exact sharp LP bounds...

Solving an SDP: Rage against the machine precision

- Assume we know a configuration C with $|C| = N$. Any upper bound $< N + 1$ is enough to prove that C is optimal.
- However, sharp bounds provide additional information on optimal configurations, leading to uniqueness proofs.
- There are many examples of exact sharp LP bounds...but very few cases in which SDP bound is proven to be sharp while LP is not.

Solving an SDP: Rage against the machine precision

- Assume we know a configuration C with $|C| = N$. Any upper bound $< N + 1$ is enough to prove that C is optimal.
- However, sharp bounds provide additional information on optimal configurations, leading to uniqueness proofs.
- There are many examples of exact sharp LP bounds...but very few cases in which SDP bound is proven to be sharp while LP is not.
- For large problems, SDP solvers only provide approximate solutions in floating point in polynomial time.

Solving an SDP: Rage against the machine precision

- Assume we know a configuration C with $|C| = N$. Any upper bound $< N + 1$ is enough to prove that C is optimal.
- However, sharp bounds provide additional information on optimal configurations, leading to uniqueness proofs.
- There are many examples of exact sharp LP bounds...but very few cases in which SDP bound is proven to be sharp while LP is not.
- For large problems, SDP solvers only provide approximate solutions in floating point in polynomial time.
- Turning an approximate solution into a rigorous proof is hard!

Results

Together with David de Laat and Maria Dostert, based on LLL, we give a procedure turning an approximate solution to an exact solution over $\mathbb{Q}$ or $\mathbb{Q}[\sqrt{d}]$, when it exists. We can prove:

Results

Together with David de Laat and Maria Dostert, based on LLL, we give a procedure turning an approximate solution to an exact solution over $\mathbb{Q}$ or $\mathbb{Q}[\sqrt{d}]$, when it exists. We can prove:

- The Petersen code is the unique optimal $1/6$-code in dimension 4 (Bachoc-Vallentin 2009, Dostert-de Laat-M. 2020).

Results

Together with David de Laat and Maria Dostert, based on LLL, we give a procedure turning an approximate solution to an exact solution over $\mathbb{Q}$ or $\mathbb{Q}[\sqrt{d}]$, when it exists. We can prove:

- The Petersen code is the unique optimal $1/6$-code in dimension 4 (Bachoc-Vallentin 2009, Dostert-de Laat-M. 2020).
- Numerically sharp for the square antiprism (Bachoc-Vallentin 2009) $\rightarrow$ Rigorous proof (Dostert-de Laat-M. 2020)

Results

Together with David de Laat and Maria Dostert, based on LLL, we give a procedure turning an approximate solution to an exact solution over $\mathbb{Q}$ or $\mathbb{Q}[\sqrt{d}]$, when it exists. We can prove:

- The Petersen code is the unique optimal $1/6$-code in dimension 4 (Bachoc-Vallentin 2009, Dostert-de Laat-M. 2020).
- Numerically sharp for the square antiprism (Bachoc-Vallentin 2009) $\rightarrow$ Rigorous proof (Dostert-de Laat-M. 2020)
- E_8 gives an optimal configuration on the hemisphere in dimension 8 (Bachoc-Vallentin 2009)
  $\rightarrow$ Uniqueness (Dostert-de Laat-M. 2020)

Results

Together with David de Laat and Maria Dostert, based on LLL, we give a procedure turning an approximate solution to an exact solution over $\mathbb{Q}$ or $\mathbb{Q}[\sqrt{d}]$, when it exists. We can prove:

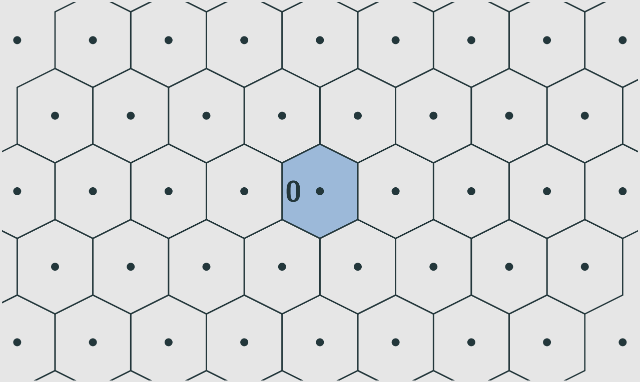
- The Petersen code is the unique optimal $1/6$-code in dimension 4 (Bachoc-Vallentin 2009, Dostert-de Laat-M. 2020).
- Numerically sharp for the square antiprism (Bachoc-Vallentin 2009) $\rightarrow$ Rigorous proof (Dostert-de Laat-M. 2020)
- E_8 gives an optimal configuration on the hemisphere in dimension 8 (Bachoc-Vallentin 2009) $\rightarrow$ Uniqueness (Dostert-de Laat-M. 2020)

Besides spherical codes, we could apply our method for packing spheres in spheres.

Thank you!

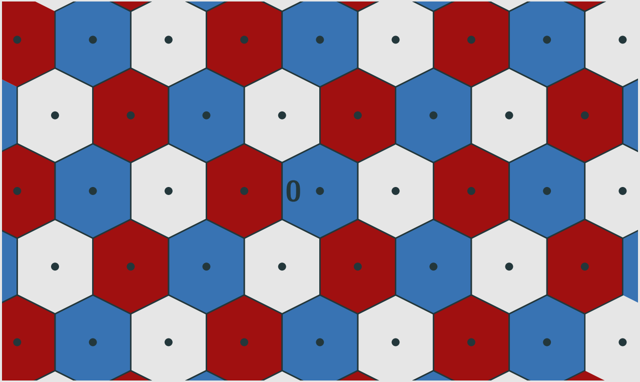
Bonus: Coloring the Voronoi tessellation of a lattice

Recall the Voronoi tesselation of a lattice Λ.



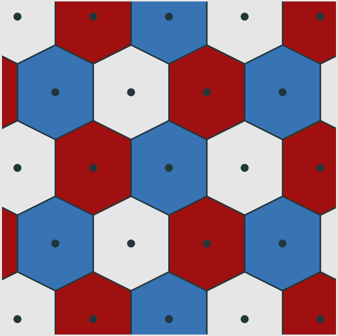
Bonus: Coloring the Voronoi tessellation of a lattice

We want to color this tessellation in such a way that two cells sharing a facet do not receive the same color.



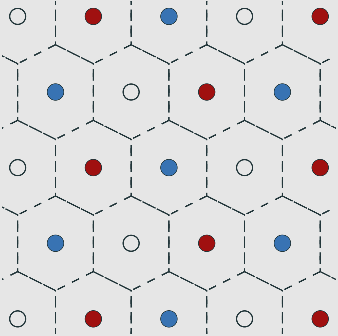
Bonus: Coloring the Voronoi tessellation of a lattice

We are colouring a geometric graph G_Λ.



Bonus: Coloring the Voronoi tessellation of a lattice

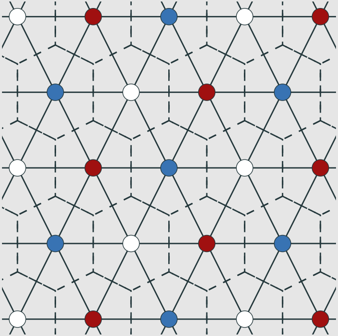
We are colouring a geometric graph G_Λ.



- The vertices: $V = \Lambda$,

Bonus: Coloring the Voronoi tessellation of a lattice

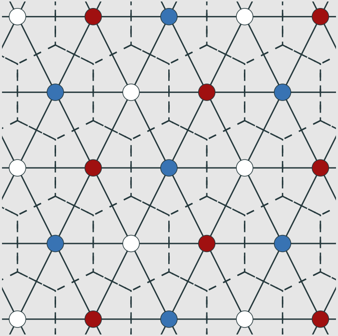
We are colouring a geometric graph G_Λ.



- The vertices: $V = \Lambda$,
- The edges: $\{u, v\} \in E$ if $w = u - v$ is a Voronoi vector of Λ, that is $\mathcal{V}_\Lambda \cap (w + \mathcal{V}_\Lambda)$ is an $(n-1)$-dimensional facet of $\mathcal{V}_\Lambda$.

Bonus: Coloring the Voronoi tessellation of a lattice

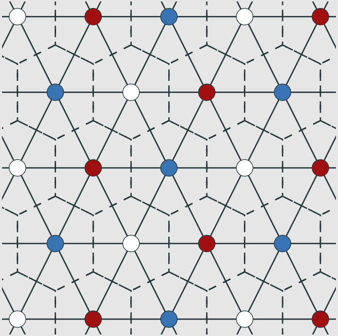
We are colouring a geometric graph G_Λ.



What is the chromatic number $\chi(\Lambda)$ of G_Λ? [Dutour-Sikirić, Madore, M., Vallentin]

Bonus: Coloring the Voronoi tessellation of a lattice

We are colouring a geometric graph G_Λ.



What is the behavior of $\chi(\Lambda)$ with the dimension n ?

- $\chi(\Lambda) \leq 2^n$,
- Expected value: $\chi(\Lambda) \geq 2^{0.099n}$.

What is the chromatic number of the most famous lattices?