SPHERE PACKING LOWER BOUNDS: NEW DEVELOPMENTS

Vlad Serban (joint with N. Gargava), EPFL

Friday, 15 July 2022

Coding Theory and Cryptography: A Conference in Honor of Joachim Rosenthal's 60th Birthday (Uni Zürich).

INTRODUCTION: SPHERE PACKING

The sphere packing problem in $\mathbb{R}^n$ concerns maximizing the proportion of space (packing density) covered by balls of equal radius with disjoint interiors.

The sphere packing problem in $\mathbb{R}^n$ concerns maximizing the proportion of space (packing density) covered by balls of equal radius with disjoint interiors. For lattice packings, this means maximizing the density given by

$$\Delta(\Lambda) := \frac{\mathrm{Vol}(\mathbb{B}_n(\lambda_1(\Lambda)))}{2^n \mathrm{Vol}(\Lambda)},$$

where $\lambda_1(\Lambda)$ is the shortest vector length.

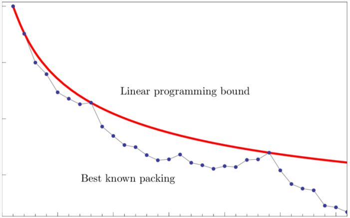
The sphere packing problem in $\mathbb{R}^n$ concerns maximizing the proportion of space (packing density) covered by balls of equal radius with disjoint interiors. For lattice packings, this means maximizing the density given by

$$\Delta(\Lambda) := \frac{\mathrm{Vol}(\mathbb{B}_n(\lambda_1(\Lambda)))}{2^n \mathrm{Vol}(\Lambda)},$$

where $\lambda_1(\Lambda)$ is the shortest vector length.

The optimal lattice packing density $\boldsymbol{\Delta}_n$ is only known in a handful of dimensions ($n \leq 8, n = 24$).

Figure: SP bounds by dimension (Hartman et al., log-scale)



The sphere packing problem in $\mathbb{R}^n$ concerns maximizing the proportion of space (packing density) covered by balls of equal radius with disjoint interiors. For lattice packings, this means maximizing the density given by

$$\Delta(\Lambda) := \frac{\mathrm{Vol}(\mathbb{B}_n(\lambda_1(\Lambda)))}{2^n \mathrm{Vol}(\Lambda)},$$

where $\lambda_1(\Lambda)$ is the shortest vector length.

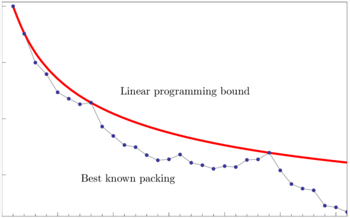
The optimal lattice packing density Δ_n is only known in a handful of dimensions ($n \leq 8, n = 24$).

High-dimensional sphere packings are a fascinating subject (error-correcting codes, mystery,...) but the best known packings achieve exponentially less than upper bounds such as

$$\Delta_n \leq \frac{2^{n \cdot 0.401\ldots}}{2^n}$$

due to Kabatiansky-Levenshtein. We embark on a quest for **structure** (or lack thereof..) !

Figure: SP bounds by dimension (Hartman et al., log-scale)



Lower bounds on the lattice packing density Δ_n in arbitrary dimension n:

Lower bounds

Lower bounds on the lattice packing density Δ_n in arbitrary dimension n:

- The classical Minkowski–Hlawka theorem states that

$$\Delta_n \geq 2\frac{\zeta(n)}{2^n}.$$

Lower bounds

Lower bounds on the lattice packing density Δ_n in arbitrary dimension n:

- The classical Minkowski–Hlawka theorem states that

$$\Delta_n \geq 2\frac{\zeta(n)}{2^n}.$$

- Linear improvement by Rogers to $\Delta_n \geq \frac{cn}{2^n}$, with subsequent sharpenings of c from $2/e$ to 2 (Ball) to $24/e$ when $4 \mid n$ (Vance, Hurwitz integers).

Lower bounds

Lower bounds on the lattice packing density Δ_n in arbitrary dimension n:

- The classical Minkowski–Hlawka theorem states that

$$\Delta_n \geq 2\frac{\zeta(n)}{2^n}.$$

- Linear improvement by Rogers to $\Delta_n \geq \frac{cn}{2^n}$, with subsequent sharpenings of c from $2/e$ to 2 (Ball) to $24/e$ when $4 \mid n$ (Vance, Hurwitz integers).
- Venkatesh obtained using a sequence of cyclotomic fields:

$$\Delta_n \geq \frac{n \log \log n}{2^{n+1}},$$

  for an infinite sequence of dimensions and further improved the linear bound to $c = 65963$ for n large enough.

Lower bounds on the lattice packing density Δ_n in arbitrary dimension n:

- The classical Minkowski–Hlawka theorem states that

$$\Delta_n \geq 2\frac{\zeta(n)}{2^n}.$$

- Linear improvement by Rogers to $\Delta_n \geq \frac{cn}{2^n}$, with subsequent sharpenings of c from $2/e$ to 2 (Ball) to $24/e$ when $4 \mid n$ (Vance, Hurwitz integers).
- Venkatesh obtained using a sequence of cyclotomic fields:

$$\Delta_n \geq \frac{n \log \log n}{2^{n+1}},$$

  for an infinite sequence of dimensions and further improved the linear bound to $c = 65963$ for n large enough.

N.B.: All of these results are **existential/nonconstructive** and most relate to some Siegel Mean Value Theorem: for random lattices in $\mathbb{R}^n$ (fix covolume one) the average lattice sum for a nice function f satisfies

$$\mathbb{E}\left[\sum_{x \in \Lambda \setminus \{0\}} f(x)\right] = \int_{\mathbb{R}^n} f(x)dx.$$

Lower bounds on the lattice packing density Δ_n in arbitrary dimension n:

- The classical Minkowski–Hlawka theorem states that

$$\Delta_n \geq 2\frac{\zeta(n)}{2^n}.$$

- Linear improvement by Rogers to $\Delta_n \geq \frac{cn}{2^n}$, with subsequent sharpenings of c from $2/e$ to 2 (Ball) to $24/e$ when $4 \mid n$ (Vance, Hurwitz integers).
- Venkatesh obtained using a sequence of cyclotomic fields:

$$\Delta_n \geq \frac{n \log \log n}{2^{n+1}},$$

  for an infinite sequence of dimensions and further improved the linear bound to $c = 65963$ for n large enough.

N.B.: All of these results are **existential/nonconstructive** and most relate to some Siegel Mean Value Theorem: for random lattices in $\mathbb{R}^n$ (fix covolume one) the average lattice sum for a nice function f satisfies

$$\mathbb{E}\left[\sum_{x \in \Lambda \setminus \{0\}} f(x)\right] = \int_{\mathbb{R}^n} f(x)dx.$$

Q: What is optimal Δ_n? Explicit constructions?

Effective lower bounds

All explicit families of lattices known (number fields, function fields/algebraic geometry) achieve **exponentially worse** than the Minkowski bound as $n \to \infty$!

All explicit families of lattices known (number fields, function fields/algebraic geometry) achieve **exponentially worse** than the Minkowski bound as $n \to \infty$!

Study effective results instead: work of Rogers, Rush–Sloane, Loeliger, Gaborit–Zémor, Moustrou, Campello.

Effective lower bounds

All explicit families of lattices known (number fields, function fields/algebraic geometry) achieve **exponentially worse** than the Minkowski bound as $n \to \infty$!

Study effective results instead: work of Rogers, Rush–Sloane, Loeliger, Gaborit–Zémor, Moustrou, Campello. Connects random codes and results such as the Gilbert-Varshamov bound to random lattices and Minkowski bound. Applications to e.g. AWGN channels.

All explicit families of lattices known (number fields, function fields/algebraic geometry) achieve **exponentially worse** than the Minkowski bound as $n \to \infty$!

Study effective results instead: work of Rogers, Rush–Sloane, Loeliger, Gaborit–Zémor, Moustrou, Campello. Connects random codes and results such as the Gilbert-Varshamov bound to random lattices and Minkowski bound. Applications to e.g. AWGN channels.

Construction A-style: consider sets of pre-images of codes via reduction maps like:

$$\phi_p : \mathbb{Z}^t \to \mathbb{F}_p^t$$

and show that these pre-images behave like random lattices as $p \to \infty$.

Effective lower bounds

All explicit families of lattices known (number fields, function fields/algebraic geometry) achieve **exponentially worse** than the Minkowski bound as $n \to \infty$!

Study effective results instead: work of Rogers, Rush–Sloane, Loeliger, Gaborit–Zémor, Moustrou, Campello. Connects random codes and results such as the Gilbert-Varshamov bound to random lattices and Minkowski bound. Applications to e.g. AWGN channels.

Construction A-style: consider sets of pre-images of codes via reduction maps like:

$$\phi_p : \mathbb{Z}^t \to \mathbb{F}_p^t$$

and show that these pre-images behave like random lattices as $p \to \infty$.

One can then often show that the existential lower bounds on $\mathbf{\Delta}_n$ are approached (up to arbitrary precision) by a lattice in a finite set (alas exp. size in n) of pre-images $\phi_p^{-1}(C)$ of codes C.

DIVISION RINGS AND EFFECTIVE RESULTS

Let us generalize this picture: replace $\mathbb{Z}$ by e.g., $\mathbb{Z}[\zeta_m]$, where $\zeta_m = e^{2\pi i/m}$. Obtain reduction maps modulo prime ideals in this ring.

Let us generalize this picture: replace $\mathbb{Z}$ by e.g., $\mathbb{Z}[\zeta_m]$, where $\zeta_m = e^{2\pi i/m}$. Obtain reduction maps modulo prime ideals in this ring.

Or consider instead of $\mathbb{Q}$ the (non-commutative) quaternion algebra

$$\left(\frac{-1,-1}{\mathbb{Q}}\right) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}, i^2 = j^2 = -1, ij = -ji = k\}$$

and the subring of Hurwitz integers $\mathcal{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ or } \mathbb{Z} + \frac{1}{2}\}$.

Let us generalize this picture: replace $\mathbb{Z}$ by e.g., $\mathbb{Z}[\zeta_m]$, where $\zeta_m = e^{2\pi i/m}$. Obtain reduction maps modulo prime ideals in this ring.

Or consider instead of $\mathbb{Q}$ the (non-commutative) quaternion algebra

$$\left(\frac{-1,-1}{\mathbb{Q}}\right) = \{a + bi + cj + dk : a,b,c,d \in \mathbb{Q}, i^2 = j^2 = -1, ij = -ji = k\}$$

and the subring of Hurwitz integers $\mathcal{H} = \{a + bi + cj + dk : a,b,c,d \in \mathbb{Z} \text{ or } \mathbb{Z} + \frac{1}{2}\}$.

General case: let A a $\mathbb{Q}$-division algebra, central over a number field K. Write $n := [K : \mathbb{Q}]$ and $m := [A : K]$.

Let us generalize this picture: replace $\mathbb{Z}$ by e.g., $\mathbb{Z}[\zeta_m]$, where $\zeta_m = e^{2\pi i/m}$. Obtain reduction maps modulo prime ideals in this ring.

Or consider instead of $\mathbb{Q}$ the (non-commutative) quaternion algebra

$$\left(\frac{-1,-1}{\mathbb{Q}}\right) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}, i^2 = j^2 = -1, ij = -ji = k\}$$

and the subring of Hurwitz integers $\mathcal{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ or } \mathbb{Z} + \frac{1}{2}\}$.

General case: let A a $\mathbb{Q}$-division algebra, central over a number field K. Write $n := [K : \mathbb{Q}]$ and $m := [A : K]$. We consider $\mathcal{O}_K$-orders $\mathcal{O}$ (maximal) in A viewed as lattices in Euclidean space via $i : A \hookrightarrow A \otimes_{\mathbb{R}} \mathbb{Q}$ and have a notion of prime ideal $\mathfrak{P}$ sitting above $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$ of residue field $\mathbb{F}_q$.

Let us generalize this picture: replace $\mathbb{Z}$ by e.g., $\mathbb{Z}[\zeta_m]$, where $\zeta_m = e^{2\pi i/m}$. Obtain reduction maps modulo prime ideals in this ring.

Or consider instead of $\mathbb{Q}$ the (non-commutative) quaternion algebra

$$\left(\frac{-1,-1}{\mathbb{Q}}\right) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}, i^2 = j^2 = -1, ij = -ji = k\}$$

and the subring of Hurwitz integers $\mathcal{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ or } \mathbb{Z} + \frac{1}{2}\}$.

General case: let A a $\mathbb{Q}$-division algebra, central over a number field K. Write $n := [K : \mathbb{Q}]$ and $m := [A : K]$. We consider $\mathcal{O}_K$-orders $\mathcal{O}$ (maximal) in A viewed as lattices in Euclidean space via $i : A \hookrightarrow A \otimes_{\mathbb{R}} \mathbb{Q}$ and have a notion of prime ideal $\mathfrak{P}$ sitting above $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$ of residue field $\mathbb{F}_q$. Reducing modulo $\mathfrak{p}$ yields surjections

$$\phi_p : \mathcal{O}^t \to M_n(\mathbb{F}_q)^t$$

above primes p split in A (here we take $t \geq 2$ copies).

Let us generalize this picture: replace $\mathbb{Z}$ by e.g., $\mathbb{Z}[\zeta_m]$, where $\zeta_m = e^{2\pi i/m}$. Obtain reduction maps modulo prime ideals in this ring.

Or consider instead of $\mathbb{Q}$ the (non-commutative) quaternion algebra

$$\left(\frac{-1,-1}{\mathbb{Q}}\right) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}, i^2 = j^2 = -1, ij = -ji = k\}$$

and the subring of Hurwitz integers $\mathcal{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ or } \mathbb{Z} + \frac{1}{2}\}$.

General case: let A a $\mathbb{Q}$-division algebra, central over a number field K. Write $n := [K : \mathbb{Q}]$ and $m := [A : K]$. We consider $\mathcal{O}_K$-orders $\mathcal{O}$ (maximal) in A viewed as lattices in Euclidean space via $i : A \hookrightarrow A \otimes_{\mathbb{R}} \mathbb{Q}$ and have a notion of prime ideal $\mathfrak{P}$ sitting above $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$ of residue field $\mathbb{F}_q$. Reducing modulo $\mathfrak{p}$ yields surjections

$$\phi_p : \mathcal{O}^t \to M_n(\mathbb{F}_q)^t$$

above primes p split in A (here we take $t \geq 2$ copies).

We consider subsets of the sets of codes:

$$\mathcal{C}_{k,p} = \{C \subset M_n(\mathbb{F}_q)^t : C \cong \mathbb{F}_q^{nk} \text{ as } \mathbb{F}_q - \text{modules}\}.$$

Let us generalize this picture: replace $\mathbb{Z}$ by e.g., $\mathbb{Z}[\zeta_m]$, where $\zeta_m = e^{2\pi i/m}$. Obtain reduction maps modulo prime ideals in this ring.

Or consider instead of $\mathbb{Q}$ the (non-commutative) quaternion algebra

$$\left(\frac{-1,-1}{\mathbb{Q}}\right) = \{a+bi+cj+dk : a,b,c,d \in \mathbb{Q}, i^2 = j^2 = -1, ij = -ji = k\}$$

and the subring of Hurwitz integers $\mathcal{H} = \{a+bi+cj+dk : a,b,c,d \in \mathbb{Z} \text{ or } \mathbb{Z}+\frac{1}{2}\}$.

General case: let A a $\mathbb{Q}$-division algebra, central over a number field K. Write $n := [K:\mathbb{Q}]$ and $m := [A:K]$. We consider $\mathcal{O}_K$-orders $\mathcal{O}$ (maximal) in A viewed as lattices in Euclidean space via $i : A \hookrightarrow A \otimes_{\mathbb{R}} \mathbb{Q}$ and have a notion of prime ideal $\mathfrak{P}$ sitting above $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$ of residue field $\mathbb{F}_q$. Reducing modulo $\mathfrak{p}$ yields surjections

$$\phi_p : \mathcal{O}^t \to M_n(\mathbb{F}_q)^t$$

above primes p split in A (here we take $t \geq 2$ copies).

We consider subsets of the sets of codes:

$$\mathcal{C}_{k,p} = \{C \subset M_n(\mathbb{F}_q)^t : C \cong \mathbb{F}_q^{nk} \text{ as } \mathbb{F}_q - \text{modules}\}.$$

The preimages via ϕ_p of $C \in \mathcal{C}_{k,p}$ are sublattices of $\mathcal{O}^t$. We consider the rescaled set:

$$\mathbb{L}_p = \{\beta_p \phi_p^{-1}(C) \mid C \in \mathcal{C}_{k,p}\} \text{ for } \beta_p = q^{\frac{nk-n^2t}{n^2mt}}.$$

Main technical result:

Theorem (Gargava, S.)
Let $f : \mathbb{R}^{n^2 mt} \to \mathbb{R}$ *be a nice (integrable, rapid decay) function. With the notations as above, provided* $(n-1)t < k < nt$*, we have that*

$$\lim_{p\to\infty} \mathbb{E}_{\mathbb{L}_{k,p}} \left(\sum_{x \in (\beta_p \phi_p^{-1}(C))'} f(i(x)) \right) \leq (\zeta(n^2 mt) \cdot \mathrm{Vol}(\mathcal{O}^t))^{-1} \cdot \int_{\mathbb{R}^{n^2 mt}} f(x) dx.$$

Main technical result:

Theorem (Gargava, S.)
Let $f : \mathbb{R}^{n^2mt} \to \mathbb{R}$ be a nice (integrable, rapid decay) function. With the notations as above, provided $(n-1)t < k < nt$, we have that

$$\lim_{p\to\infty} \mathbb{E}_{\mathbb{L}_{k,p}} \left(\sum_{x \in (\beta_p \phi_p^{-1}(C))'} f(i(x)) \right) \leq (\zeta(n^2mt) \cdot \mathrm{Vol}(\mathcal{O}^t))^{-1} \cdot \int_{\mathbb{R}^{n^2mt}} f(x)dx.$$

To prove this, partition $M_n(\mathbb{F}_q)^t$ into good/balanced and bad sets. Lifts of the latter should escape the support of f as $p \to \infty$ (say if f has compact support).

Main technical result:

Theorem (Gargava, S.)
Let $f : \mathbb{R}^{n^2 mt} \to \mathbb{R}$ be a nice (integrable, rapid decay) function. With the notations as above, provided $(n-1)t < k < nt$, we have that

$$\lim_{p \to \infty} \mathbb{E}_{\mathbb{L}_{k,p}} \left(\sum_{x \in (\beta_p \phi_p^{-1}(C))'} f(i(x)) \right) \leq (\zeta(n^2 mt) \cdot \mathrm{Vol}(\mathcal{O}^t))^{-1} \cdot \int_{\mathbb{R}^{n^2 mt}} f(x) dx.$$

To prove this, partition $M_n(\mathbb{F}_q)^t$ into good/balanced and bad sets. Lifts of the latter should escape the support of f as $p \to \infty$ (say if f has compact support).

We take as codes k copies of the simple $M_n(\mathbb{F}_q)$-modules $\mathbb{F}_q^n$ and as bad set $B_p \subset M_n(\mathbb{F}_q)^t$ the points with at least one coordinate non-invertible in $M_n(\mathbb{F}_q)$.

Q: How do we obtain good sphere packings from this?

Deducing lower bounds

Q: How do we obtain good sphere packings from this?

- We use the fact that units $\mathcal{O}^\times$ act (diagonally) on our $\mathcal{O}$-lattices.

Deducing lower bounds

Q: How do we obtain good sphere packings from this?

- We use the fact that units $\mathcal{O}^\times$ act (diagonally) on our $\mathcal{O}$-lattices.
- We can average out the quadratic form to ensure $\|\cdot\|$ is invariant under finite order units G_0.

Q: How do we obtain good sphere packings from this?

- We use the fact that units $\mathcal{O}^\times$ act (diagonally) on our $\mathcal{O}$-lattices.
- We can average out the quadratic form to ensure $\|\cdot\|$ is invariant under finite order units G_0.
- Now apply the theorem to $f = \mathbf{1}_{\mathbb{B}(r)}$ and $\forall \varepsilon > 0$ choose r so that

$$\mathrm{Vol}(\mathbb{B}(r)) = (1-\varepsilon)|G_0|\zeta(mn^2t)\mathrm{Vol}(\mathcal{O}^t).$$

Q: How do we obtain good sphere packings from this?

- We use the fact that units $\mathcal{O}^\times$ act (diagonally) on our $\mathcal{O}$-lattices.
- We can average out the quadratic form to ensure $\|\cdot\|$ is invariant under finite order units G_0.
- Now apply the theorem to $f = \mathbf{1}_{\mathbb{B}(r)}$ and $\forall\varepsilon > 0$ choose r so that

$$\mathrm{Vol}(\mathbb{B}(r)) = (1-\varepsilon)|G_0|\zeta(mn^2t)\mathrm{Vol}(\mathcal{O}^t).$$

- It follows by the MVT that for p large enough there exists $\Lambda_\varepsilon \in \mathbb{L}_p$ such that

$$\underbrace{|\mathbb{B}(r) \cap \Lambda_\varepsilon'|}_{\text{multiple of } |G_0|} \leq (1-\varepsilon)|G_0|.$$

Q: How do we obtain good sphere packings from this?

- We use the fact that units $\mathcal{O}^\times$ act (diagonally) on our $\mathcal{O}$-lattices.
- We can average out the quadratic form to ensure $\|\cdot\|$ is invariant under finite order units G_0.
- Now apply the theorem to $f = \mathbf{1}_{\mathbb{B}(r)}$ and $\forall \varepsilon > 0$ choose r so that

$$\mathrm{Vol}(\mathbb{B}(r)) = (1-\varepsilon)|G_0|\zeta(mn^2t)\mathrm{Vol}(\mathcal{O}^t).$$

- It follows by the MVT that for p large enough there exists $\Lambda_\varepsilon \in \mathbb{L}_p$ such that

$$\underbrace{|\mathbb{B}(r) \cap \Lambda'_\varepsilon|}_{\text{multiple of } |G_0|} \leq (1-\varepsilon)|G_0|.$$

So we deduce that $\mathbb{B}(r) \cap \Lambda_\varepsilon = \{0\}$, leading to:

Proposition (Gargava, S.)

There exists $\forall \varepsilon > 0$ a n^2mt-dimensional sub-lattice $\Lambda_\varepsilon \subset \mathcal{O}^t$ with packing density

$$\Delta(\Lambda_\varepsilon) \geq (1-\varepsilon) \cdot \frac{|G_0|\zeta(mn^2t)}{2^{mn^2t}}$$

in the set of scaled pre-images of codes $\mathbb{L}_p$ for p large enough.

Deducing lower bounds

Q: How do we obtain good sphere packings from this?

- We use the fact that units $\mathcal{O}^\times$ act (diagonally) on our $\mathcal{O}$-lattices.
- We can average out the quadratic form to ensure $\|\cdot\|$ is invariant under finite order units G_0.
- Now apply the theorem to $f = \mathbf{1}_{\mathbb{B}(r)}$ and $\forall \varepsilon > 0$ choose r so that

$$\mathrm{Vol}(\mathbb{B}(r)) = (1-\varepsilon)|G_0|\zeta(mn^2t)\mathrm{Vol}(\mathcal{O}^t).$$

- It follows by the MVT that for p large enough there exists $\Lambda_\varepsilon \in \mathbb{L}_p$ such that

$$\underbrace{|\mathbb{B}(r) \cap \Lambda'_\varepsilon|}_{\text{multiple of } |G_0|} \leq (1-\varepsilon)|G_0|.$$

So we deduce that $\mathbb{B}(r) \cap \Lambda_\varepsilon = \{0\}$, leading to:

Proposition (Gargava, S.)

There exists $\forall \varepsilon > 0$ a n^2mt-dimensional sub-lattice $\Lambda_\varepsilon \subset \mathcal{O}^t$ with packing density

$$\Delta(\Lambda_\varepsilon) \geq (1-\varepsilon) \cdot \frac{|G_0|\zeta(mn^2t)}{2^{mn^2t}}$$

in the set of scaled pre-images of codes $\mathbb{L}_p$ for p large enough.

The best bounds are now obtained by maximizing $|G_0|$. Recall:

The best bounds are now obtained by maximizing $|G_0|$. Recall:

- Venkatesh's construction is for $A = K = \mathbb{Q}(\zeta_m)$ and $G_0 = \mathbb{Z}/m\mathbb{Z}$. This yields an improvement of $m/2\varphi(m)$ over linear lower bounds on $\Delta_{2\varphi(m)}$.

The best bounds are now obtained by maximizing $|G_0|$. Recall:

- Venkatesh's construction is for $A = K = \mathbb{Q}(\zeta_m)$ and $G_0 = \mathbb{Z}/m\mathbb{Z}$. This yields an improvement of $m/2\varphi(m)$ over linear lower bounds on $\Delta_{2\varphi(m)}$.
- Vance's construction considers $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and finite units $\mathfrak{T}^* \cong \mathrm{SL}_2(\mathbb{F}_3)$ of the Hurwitz integers (improved constant).

The best bounds are now obtained by maximizing $|G_0|$. Recall:

- Venkatesh's construction is for $A = K = \mathbb{Q}(\zeta_m)$ and $G_0 = \mathbb{Z}/m\mathbb{Z}$. This yields an improvement of $m/2\varphi(m)$ over linear lower bounds on $\Delta_{2\varphi(m)}$.
- Vance's construction considers $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and finite units $\mathfrak{T}^* \cong \mathrm{SL}_2(\mathbb{F}_3)$ of the Hurwitz integers (improved constant).
- Finite subgroups of division rings have been classified by S. Amitsur: limited improvements.

The best bounds are now obtained by maximizing $|G_0|$. Recall:

- Venkatesh's construction is for $A = K = \mathbb{Q}(\zeta_m)$ and $G_0 = \mathbb{Z}/m\mathbb{Z}$. This yields an improvement of $m/2\varphi(m)$ over linear lower bounds on $\Delta_{2\varphi(m)}$.
- Vance's construction considers $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and finite units $\mathfrak{T}^* \cong \mathrm{SL}_2(\mathbb{F}_3)$ of the Hurwitz integers (improved constant).
- Finite subgroups of division rings have been classified by S. Amitsur: limited improvements.
- Can e.g. combine these two ideas: Consider $\mathbb{Q}(\zeta_m) \otimes_{\mathbb{Q}} \left(\frac{-1,-1}{\mathbb{Q}}\right)$. It is a division algebra with center $\mathbb{Q}(\zeta_m)$, maximal $\mathbb{Z}[\zeta_m]$-order $\mathcal{O}$ and with $\mathfrak{T}^* \times \mathbb{Z}/m\mathbb{Z} \subset \mathcal{O}^\times$ if 2 has odd order modulo m.

The best bounds are now obtained by maximizing $|G_0|$. Recall:

- Venkatesh's construction is for $A = K = \mathbb{Q}(\zeta_m)$ and $G_0 = \mathbb{Z}/m\mathbb{Z}$. This yields an improvement of $m/2\varphi(m)$ over linear lower bounds on $\Delta_{2\varphi(m)}$.
- Vance's construction considers $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and finite units $\mathfrak{T}^* \cong \mathrm{SL}_2(\mathbb{F}_3)$ of the Hurwitz integers (improved constant).
- Finite subgroups of division rings have been classified by S. Amitsur: limited improvements.
- Can e.g. combine these two ideas: Consider $\mathbb{Q}(\zeta_m) \otimes_{\mathbb{Q}} \left(\frac{-1,-1}{\mathbb{Q}}\right)$. It is a division algebra with center $\mathbb{Q}(\zeta_m)$, maximal $\mathbb{Z}[\zeta_m]$-order $\mathcal{O}$ and with $\mathfrak{T}^* \times \mathbb{Z}/m\mathbb{Z} \subset \mathcal{O}^\times$ if 2 has odd order modulo m.

Proposition (Gargava, S.)

Let $m_k = \prod_{\substack{p \leq k \text{ prime} \\ 2 \nmid \mathrm{ord}_2 p}} p$ and set $n_k := 8\varphi(m_k)$. Then $\forall \varepsilon > 0$, $\exists$ effective 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

$$\Delta(\Lambda) \geq (1 - e^{-n_k}) \frac{3 \cdot n_k (\log\log n_k)^{7/24}}{2^{n_k}}$$

asymptotically in dimension n_k.

Conclusion

The improved constant means we get the best effective bounds up to dimension $\approx 1.98 \cdot 10^{46}$ roughly. Can also recover a full $n \log \log n$ improvement with non-commutative symmetry.

Conclusion

The improved constant means we get the best effective bounds up to dimension $\approx 1.98 \cdot 10^{46}$ roughly. Can also recover a full $n \log \log n$ improvement with non-commutative symmetry.

Exhaustive searches in these exponential-size finite sets are not tractable, but how does sampling these symmetrized sets $\mathbb{L}_p$ behave vs. just a random lattice?

Conclusion

The improved constant means we get the best effective bounds up to dimension $\approx 1.98 \cdot 10^{46}$ roughly. Can also recover a full $n \log \log n$ improvement with non-commutative symmetry.

Exhaustive searches in these exponential-size finite sets are not tractable, but how does sampling these symmetrized sets $\mathbb{L}_p$ behave vs. just a random lattice?

The improved constant means we get the best effective bounds up to dimension $\approx 1.98 \cdot 10^{46}$ roughly. Can also recover a full $n \log \log n$ improvement with non-commutative symmetry.

Exhaustive searches in these exponential-size finite sets are not tractable, but how does sampling these symmetrized sets $\mathbb{L}_p$ behave vs. just a random lattice?

Thank you!